IoT Cybersecurity
Regulating & Securing Infinity

David Z. Bodenheimer
Crowell & Moring LLP
Association of Corporate Counsel
Tysons Corner, VA
April 26, 2018
IoT Cyber Threats & Risks
Where Do They Start? Or End?
Why is IoT a Cyber Target?

• It’s Big!
  • 8.4 Billion Devices (2017)
  • 20.4 Billion Devices (2020)

• It’s Lucrative!
  • $7 Trillion (2020)
  • $11 Trillion (2025)

• It’s Everywhere!
  • Smart-Everything (Cars, Toasters, Pills, Buildings, Phones, Shoes)
IoT Cyber Threat Map

Where the Scary Things Are

**Multiple Sectors**
- Industrial, Health, Retail, Energy, Home . . . .

**Multiple Devices**
- Cars, phones, thermostats, drones, fridge . . . .

**Multiple Networks**
- Satellites, Cellular, Local Wireless, LPWAN

**Multiple Edge Devices**
- SCADA, embedded systems, operating systems

**Hackers, Hackers Everywhere**
- Cyber criminals, nation states, teens in basement . . . .
IoT Threats in the News

Stopping Self-Driving Cars From Becoming Cybersecurity Weapons

How my fridge caused hundreds of websites to crash

Agencies’ approach to IoT security highlights differences in cybersecurity approach

IoT security for healthcare is in critical condition

IoT Gadgets: Exploring the New Sources of Discoverable Evidence

The Internet of Things: The security crisis of 2018?
IoT Cyber Risks: What’s Bugging the Feds?

**Sen. Mark Warner (VA):**
“Additionally, the sheer number of IoT devices – expected to exceed 20 billion devices by 2020 – has enabled bad actors to launch devastating Distributed Denial of Service (DDoS) attacks.” [S. 1691 Fact Sheet]

**Rep. Jerry McNerney (CA):**
“Security vulnerabilities in IoT devices are likely to pose threats to our national security and endanger our nation’s economy.” [comments on H.R. 1324, the Securing IoT Act]

**Government Accountability Office (GAO):**
“For example, in 2016, hundreds of thousands of weakly-secured IoT devices were accessed and hacked, disrupting traffic on the Internet.” [GAO-17-75]

**National Security Telecommunications Advisory Committee (NSTAC):**
“The threat will only increase as the number and type of IoT devices grow and as such devices become more autonomous, capable, and ubiquitous.” [NSATC Report on Internet & Communications Resilience]

**Department of Homeland Security (DHS):**
“IoT security, however, has not kept up with the rapid pace of innovation and deployment, creating substantial safety and economic risks.” [Strategic Principles for Securing the Internet of Things]
**IoT National Security Threats**

**Mission Sabotage**
- Electrical system attack
- Knock out communications

**Equipment Sabotage**
- Insider threat to utilities
- Flood dry dock & sink ship

**Security Breach**
- TV pipeline to devices
- Surveil & steal critical data

**Leadership Targets**
- Hijack Pentagon leader’s car
- Steer car over the cliff

[GAO Report on DOD IoT (GAO-17-668)]
IoT Cyber Regulation
Who Regulates? And How?
Who Regulates IoT?

Before IoT: Parallel Regulatory Regimes (Privacy & Cyber)

<table>
<thead>
<tr>
<th>Patchworks</th>
<th>Integrated Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Privacy Patchwork</td>
<td>• IoT + Drones</td>
</tr>
<tr>
<td>‣ HIPAA (healthcare)</td>
<td>‣ “Next trillion files”</td>
</tr>
<tr>
<td>‣ GLB (financial)</td>
<td>‣ FAA regulate?</td>
</tr>
<tr>
<td>‣ FERPA (educational)</td>
<td>• IoT + Cloud + AI</td>
</tr>
<tr>
<td>‣ Privacy Act (federal)</td>
<td>‣ Big Data = Bigger</td>
</tr>
<tr>
<td>• Cyber Patchwork</td>
<td>‣ AI Cyber Attacks</td>
</tr>
<tr>
<td>‣ FISMA (federal)</td>
<td></td>
</tr>
<tr>
<td>‣ DFARS/HIPAA, etc.</td>
<td></td>
</tr>
</tbody>
</table>
Who Regulates IoT?

Congressional Oversight on the Hill

**Congressional Committees**
- “more than 30 different congressional committees” *Politico* (2015)

**Legislative Actions**
- S.88 - Developing Innovation & Growing the Internet of Things (DIGIT) Act
- S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017
- H.R.3985 - Internet of Medical Things Resilience Partnership Act of 2017

**Congressional Hearings & Reports**
- Lots & Lots & Lots of Senate & House Hearings
### Federal Agencies

- **FCC**
  - Spectrum management
- **DHS**
  - Critical infrastructure
- **FTC**
  - Consumer devices
- **FDA**
  - Medical devices

### And More Agencies

- **DOE**
  - Smart grid
- **DOT**
  - Connected cars
- **DOD**
  - IoT advanced technologies
- **DOJ**
  - Law enforcement
Who Regulates IoT?

Federal & State Enforcement Actions

**Criminal Enforcement (DOJ)**

**Administrative Enforcement (FTC)**
- Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children’s Privacy Law and the FTC Act: Settlement marks the agency’s first children’s privacy and security case involving connected toys (Jan. 18, 2018) [FTC Press Release]

**State Enforcement**
- In Safetech IoT Settlement, New York Attorney General Outlines Reasonable Security Program, iptechblog (June 1, 2017) [NY AG Settlement]
Who Regulates IoT?

Regulating the Undefined

- **NIST Publication**
  
  “However, the current Internet of Things (IoT) landscape presents itself as a mix of jargon, consumer products, and unrealistic predictions. There is no formal, analytic, or even descriptive set of the building blocks that govern the operation, trustworthiness, and lifecycle of IoT. This vacuum between the hype and the science, if a science exists, is evident. Therefore, a composability model and vocabulary that defines principles common to most, if not all networks of things, is needed to address the question: ‘what is the science, if any, underlying IoT?’

  [NIST, Draft NISTIR 8063 (Feb. 2016)]

- **Privacy of Things**
  
  “The Internet of Things (IoT) will create the single largest, most chaotic conversation in the history of language. Imagine every human being on the planet stepping outside and yelling at the top of their lungs everything that comes into their heads, and you still wouldn’t be close to the scale of communications that are going to occur when all those IoT devices really get chattering.”

IoT Cyber Standards

What Standards? And Where?
What are the IoT Cyber Standards?

Department of Homeland Security Guidance

1. Incorporate Security at the Design Phase
2. Advance Security Updates and Vulnerability Management
4. Prioritize Security Measures According to Potential Impact
5. Promote Transparency across IoT
6. Connect Carefully and Deliberately

U.S. Department of Homeland Security

STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT)

Version 1.0
November 15, 2016
What are the IoT Cyber Standards?

Food & Drug Administration – Medical Devices

Varying Security Regimes – Patient Risk

• Pre-Market Considerations
• Post-Market Considerations

NIST Cybersecurity Framework

• 2014 NIST Framework
• Identify, Protect, Detect, Respond, & Recover

Elements for Post-Market Cyber Program

• Identify: maintain safety & ID market data (e.g., complaints & returns)
• Protect/Detect: assess & detect vulnerabilities, risks & threats
• Protect/Respond/Recover: assess security controls
• Mitigate:
  • Assess & mitigate safety risks
  • Preserve essential performance (i.e., efficacy)
What are the IoT Cyber Standards?

Department of Defense – Networks & Military Technology

**GAO Assessments**

**DOD & Intelligence Assessments**
- Multiple DOD/IC Assessments: Defense Science Board, DOD CIO Report, Joint Staff, DNI Threat Assessment . . . .
  
  “DOD has stated that it is entering a rapidly deepening pool of vulnerability.”

**No Unified IoT Oversight or Standards**
- “According to DOD officials, no one specific office or entity is responsible for IoT security.”
- “DOD has policies and guidance for IoT devices, but gaps remain.”
What are the IoT Cyber Standards?

Department of Defense – Networks & Military Technology

Figure 3: Examples of Department of Defense (DOD) Policies and Guidance on Types of Internet of Things (IoT) Devices

<table>
<thead>
<tr>
<th>Policy and guidance</th>
<th>Sponsor</th>
<th>Ownership of device</th>
<th>Type of device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction and Use of Wearable Fitness Devices and Headphones within DOD Accredited Spaces and Facilities April 2016</td>
<td>DOD Chief Information Officer</td>
<td>Personal</td>
<td>Fitness devices</td>
</tr>
<tr>
<td>DODI 8420.01, Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies November 2009</td>
<td>DOD Chief Information Officer</td>
<td>Government Personal</td>
<td>Smart watches and other portable electronic devices</td>
</tr>
<tr>
<td>Component Policies on Wireless and Personal Portable Electronic Devices 2014 and 2016</td>
<td>DIA, DISA, and Department of the Navy</td>
<td>Government</td>
<td>Smartphones</td>
</tr>
<tr>
<td>Security Technical Implementation Guides for specific DOD-issued mobile devices like Apple and Blackberry 2016</td>
<td>DISA</td>
<td>Government</td>
<td>Infrastructure devices</td>
</tr>
<tr>
<td>Unified Facilities Criteria: Cybersecurity of Facility-Related Control Systems September 2016</td>
<td>OSD and Departments of the Army, Navy, and Air Force</td>
<td>Government Vendor</td>
<td>Infrastructure devices</td>
</tr>
</tbody>
</table>

DIA Defense Intelligence Agency
DISA Defense Information Systems Agency
DOD Department of Defense
OSD Office of the Secretary of Defense

Source: GAO analysis of Department of Defense (DOD) information. GAO-17-908
What are the IoT Cyber Standards?

National Institute of Standards & Technology (NIST)

**NISTIR 8200**
- Purpose: survey existing IoT cyber standards

**Multiplicity of Standards**
- Relevant NIST standards
- Agency guidance (e.g., DOT ITS-JPO, FDA, GSA)
- Existing & emerging industry standards (e.g., ISO/IEC)

**Key Findings & Non-Findings**
- IoT Definition: None
- Functional Applications: Connected vehicles, consumer devices, healthcare/medical devices, smart buildings & smart manufacturing
- Cyber Standard: No one-size-fits-all
- Core Areas: 11 core areas for cybersecurity standardization
What are the IoT Cyber Standards?

NISTIR 8200: Status of Cybersecurity Standardization for Several IoT Applications

<table>
<thead>
<tr>
<th>Core Areas of Cybersecurity Standardization</th>
<th>Examples of Relevant SDOs</th>
<th>Connected Vehicles</th>
<th>Consumer IoT</th>
<th>Health IoT &amp; Medical Devices</th>
<th>Smart Buildings</th>
<th>Smart Manufacturing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Incident Management</td>
<td>ETSI; ISO/IEC JTC 1; ITU-T; PCI</td>
<td>Some Standards</td>
<td>Some Standards</td>
<td>Some Standards</td>
<td>Some Standards</td>
<td>Some Standards</td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td>ETSI; FIDO Alliance; IETF; OASIS; OIDF; ISO/IEC JTC 1; ITU-T; W3C</td>
<td>Standards Available</td>
<td>Standards Available</td>
<td>Some Standards</td>
<td>Standards Available</td>
<td>Standards Available</td>
</tr>
</tbody>
</table>
## What are the IoT Cyber Standards?

### NISTIR 8200: Status of Cybersecurity Standardization for Several IoT Applications

<table>
<thead>
<tr>
<th>Core Areas of Cybersecurity Standardization</th>
<th>Examples of Relevant SDOs</th>
<th>Connected Vehicles</th>
<th>Consumer IoT</th>
<th>Health IoT &amp; Medical Devices</th>
<th>Smart Buildings</th>
<th>Smart Manufacturing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Management Systems</td>
<td>ATIS; IEC; ISA; ISO/IEC JTC 1; ISO TC 223; OASIS; The Open Group</td>
<td>Some Standards</td>
<td>Some Standards</td>
<td>Some Standards</td>
<td>Some Standards</td>
<td>Some Standards</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Slow Uptake</td>
<td>Slow Uptake</td>
<td>Slow Uptake</td>
<td>Slow Uptake</td>
<td>Slow Uptake</td>
</tr>
<tr>
<td>IT System Security Evaluation</td>
<td>ISO/IEC JTC 1; The Open Group; UL</td>
<td>Standards Needed</td>
<td>Standards Needed</td>
<td>Standards Needed</td>
<td>Standards Needed</td>
<td>Standards Needed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not Implemented</td>
<td>Not Implemented</td>
<td>Not Implemented</td>
<td>Not Implemented</td>
<td>Not Implemented</td>
</tr>
<tr>
<td>Hardware Assurance</td>
<td>ISO/IEC JTC 1; SAE International</td>
<td>Some Standards</td>
<td>Some Standards</td>
<td>Some Standards</td>
<td>Some Standards</td>
<td>Some Standards</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Slow Uptake</td>
<td>Not Implemented</td>
<td>Slow Uptake</td>
<td>Not Implemented</td>
<td>Not Implemented</td>
</tr>
</tbody>
</table>
Questions?

David Z. Bodenheimer
Crowell & Moring LLP
dbodenheimer@crowell.com
(202) 624-2713
www.crowell.com