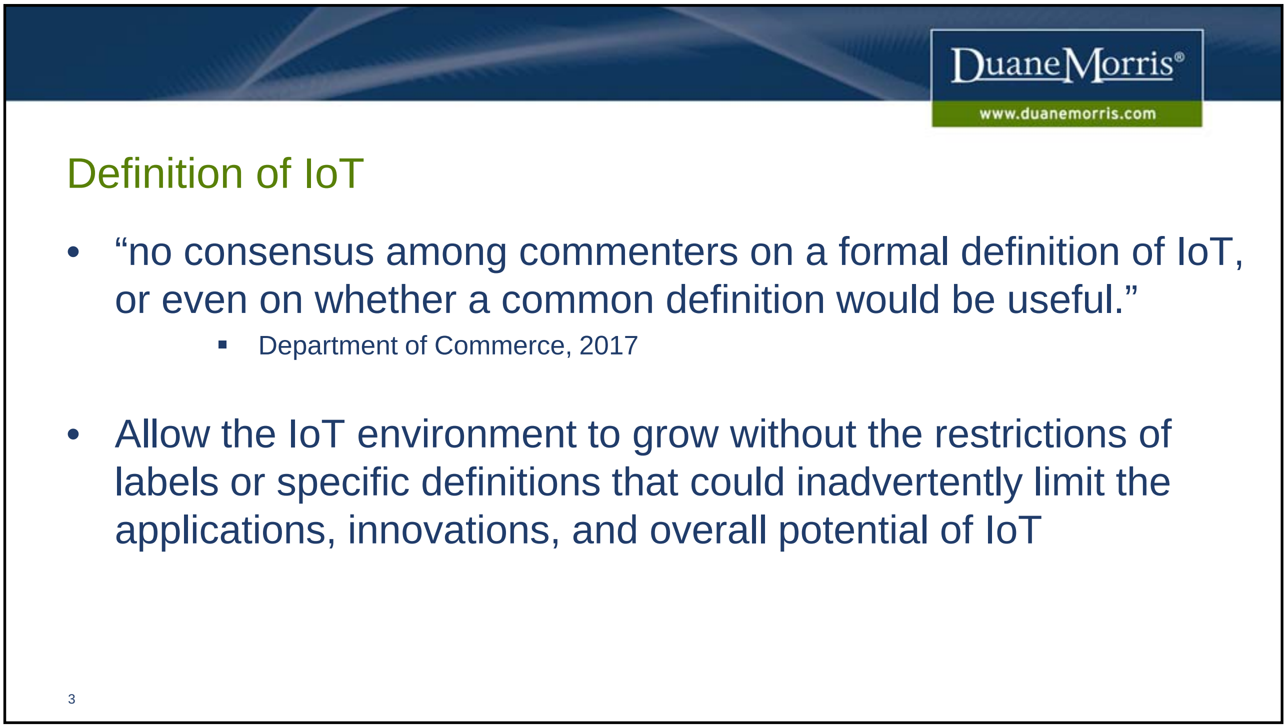
Internet of Things (IoT)
Impact on Privacy and Security

SANDRA A. JESKIE

July 16, 2018

Duane Morris – Firm Offices | New York | London | Singapore | Philadelphia | Chicago | Washington, D.C. | San Francisco | Silicon Valley | San Diego | Los Angeles | Taiwan | Boston | Houston | Austin | Hanoi | Ho Chi Minh City | Shanghai | Atlanta | Baltimore
Wilmington | Miami | Boca Raton | Pittsburgh | Newark | Las Vegas | Cherry Hill | Lake Tahoe | Myanmar | Oman | Duane Morris – Affiliate Offices | Mexico City | Sri Lanka | Duane Morris LLP – A Delaware limited liability partnership

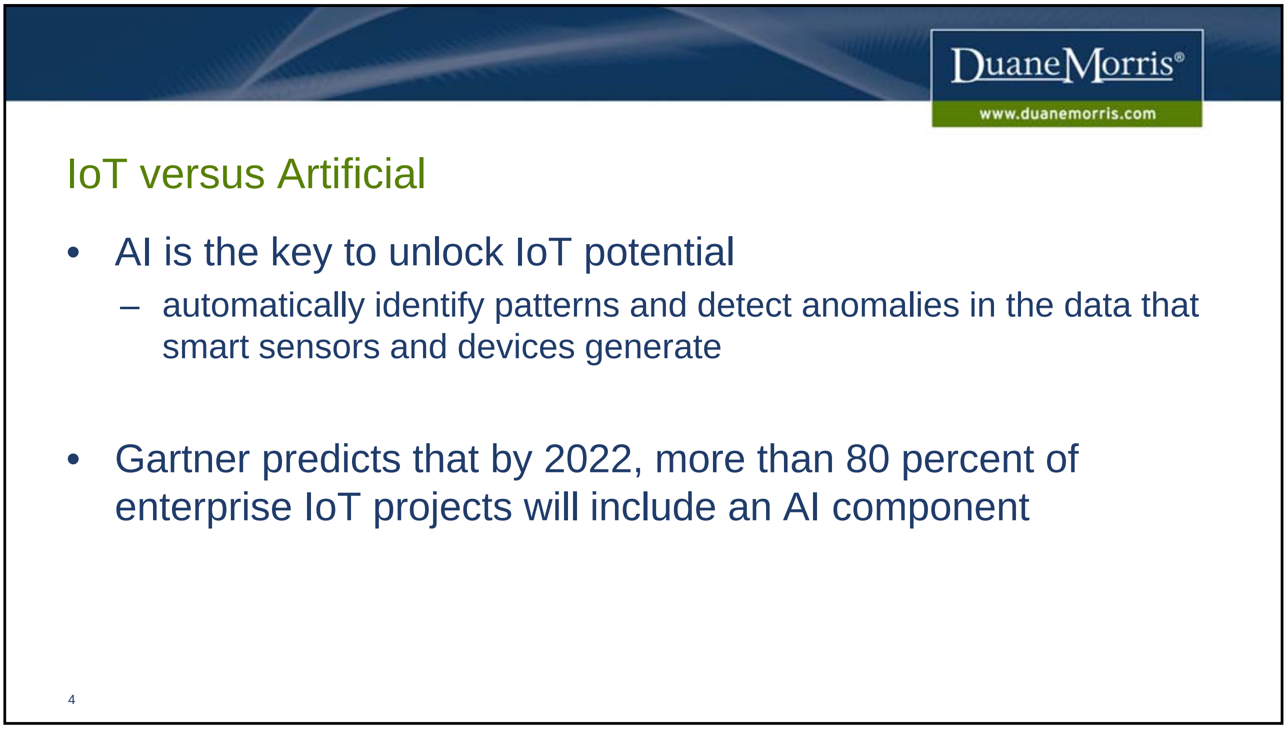
How IOT Will Change The World



Definition of IoT

- “no consensus among commenters on a formal definition of IoT, or even on whether a common definition would be useful.”
  - Department of Commerce, 2017

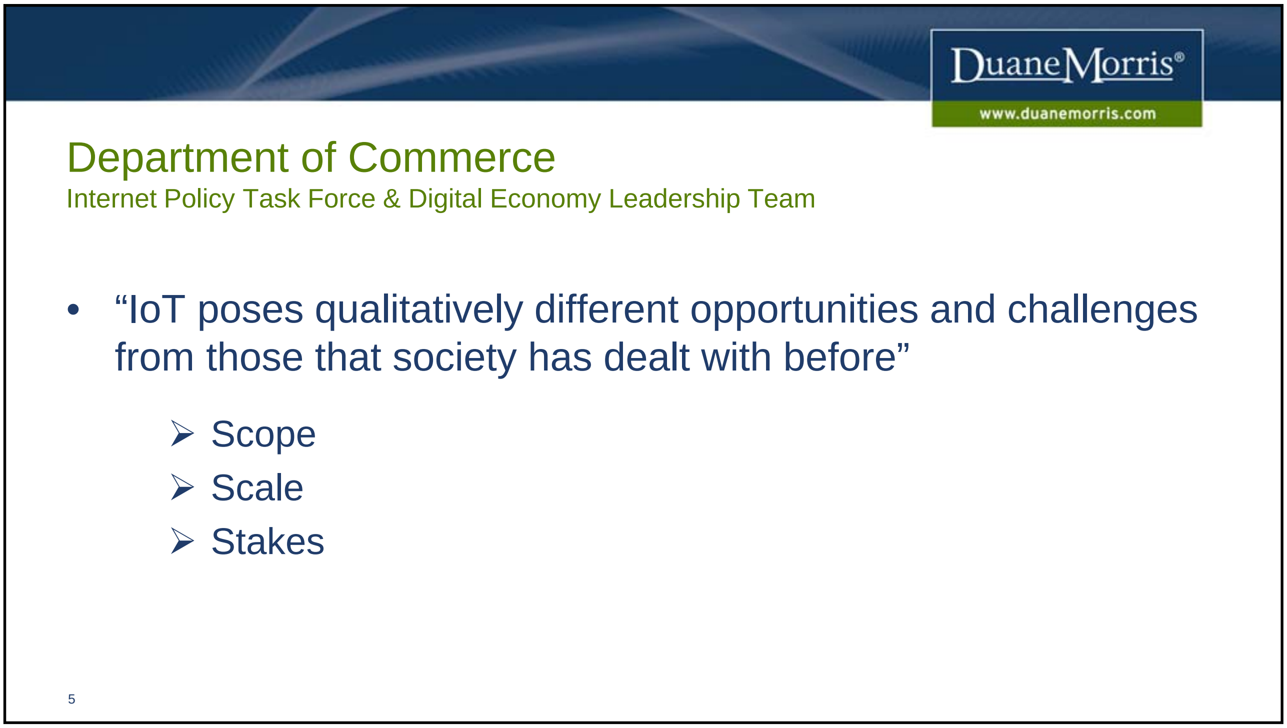
- Allow the IoT environment to grow without the restrictions of labels or specific definitions that could inadvertently limit the applications, innovations, and overall potential of IoT



IoT versus Artificial

- AI is the key to unlock IoT potential
  - automatically identify patterns and detect anomalies in the data that smart sensors and devices generate

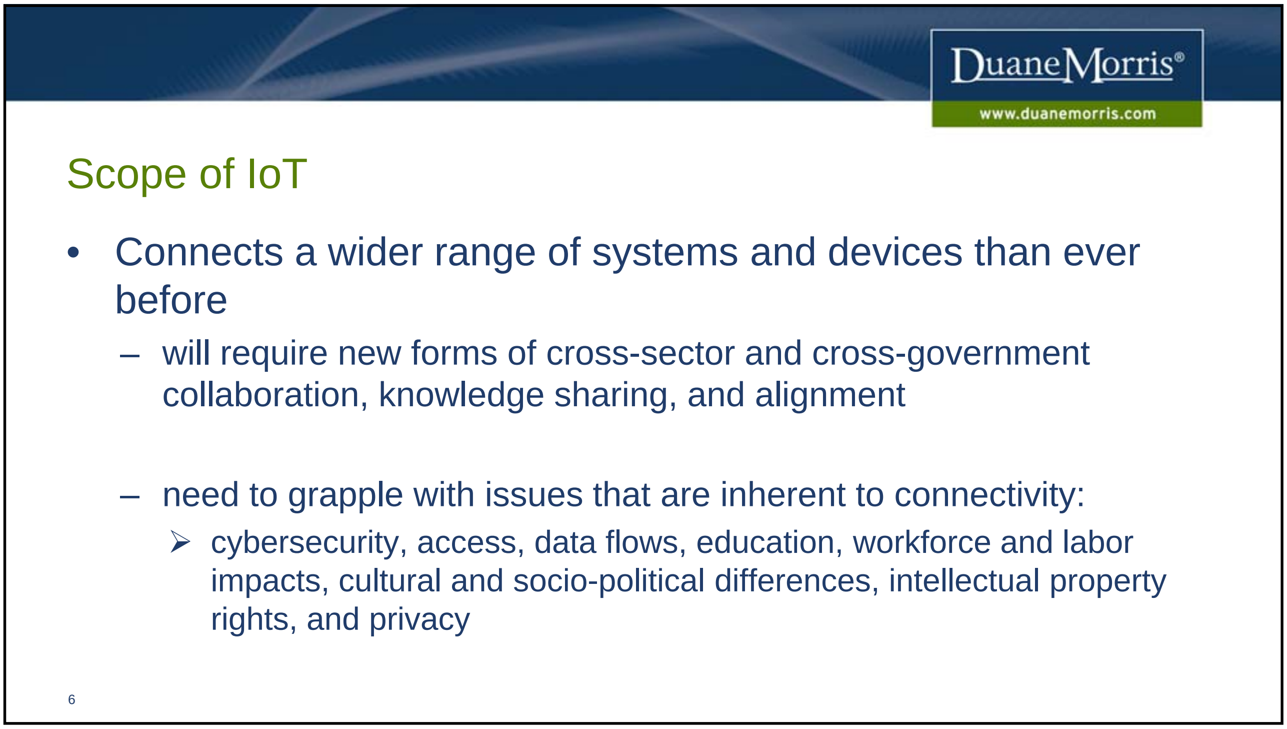
- Gartner predicts that by 2022, more than 80 percent of enterprise IoT projects will include an AI component



Department of Commerce

Internet Policy Task Force & Digital Economy Leadership Team

- "IoT poses qualitatively different opportunities and challenges from those that society has dealt with before"
    - ➢ Scope
    - ➢ Scale
    - ➢ Stakes



Scope of IoT

- Connects a wider range of systems and devices than ever before
    - – will require new forms of cross-sector and cross-government collaboration, knowledge sharing, and alignment
    - – need to grapple with issues that are inherent to connectivity:
        - ➢ cybersecurity, access, data flows, education, workforce and labor impacts, cultural and socio-political differences, intellectual property rights, and privacy

Scale of IoT

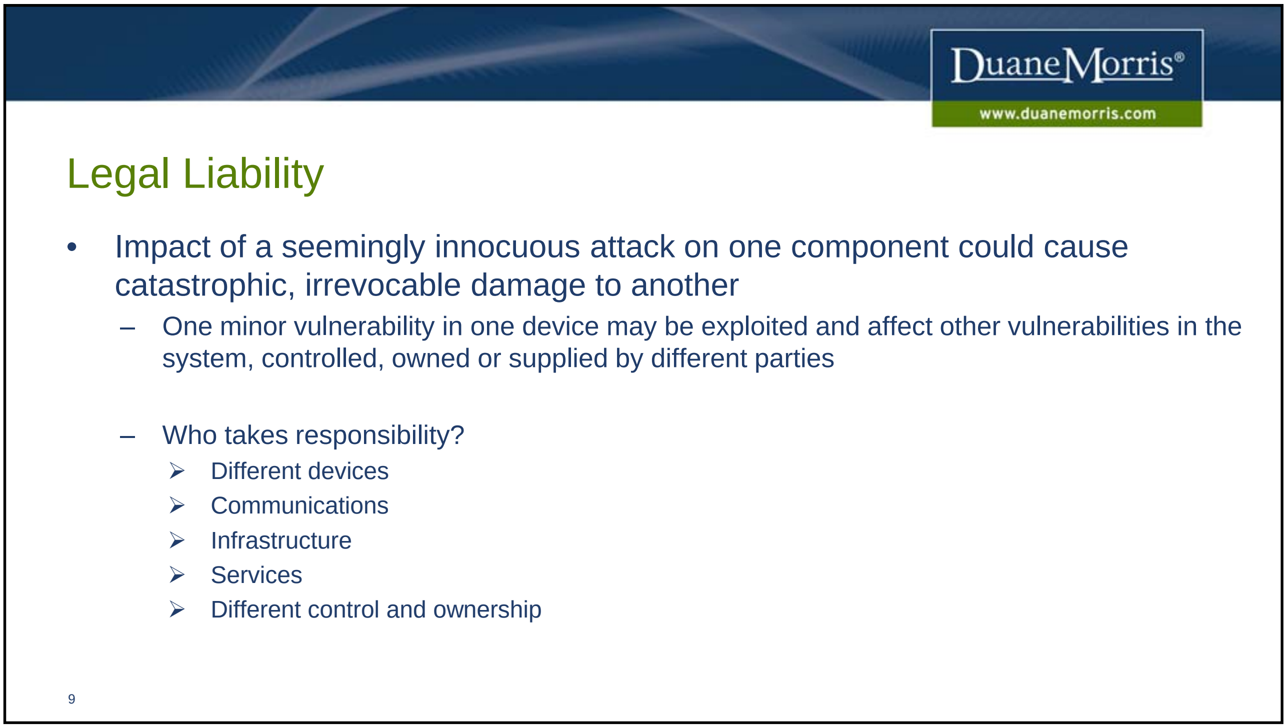
- By 2025, the overall impact of these devices on the global economy will be between $4 trillion and $11 trillion
    - McKinsey Global Institute

- Significant challenges for the current infrastructure, including stability, capacity, resilience, policy and regulatory consistency, and international cooperation

Stakes for IoT

- IoT raises the stakes of a cyberattack
    - events can affect medical devices, supply chain reliability, and cars
    - Risk of physical harm is significant

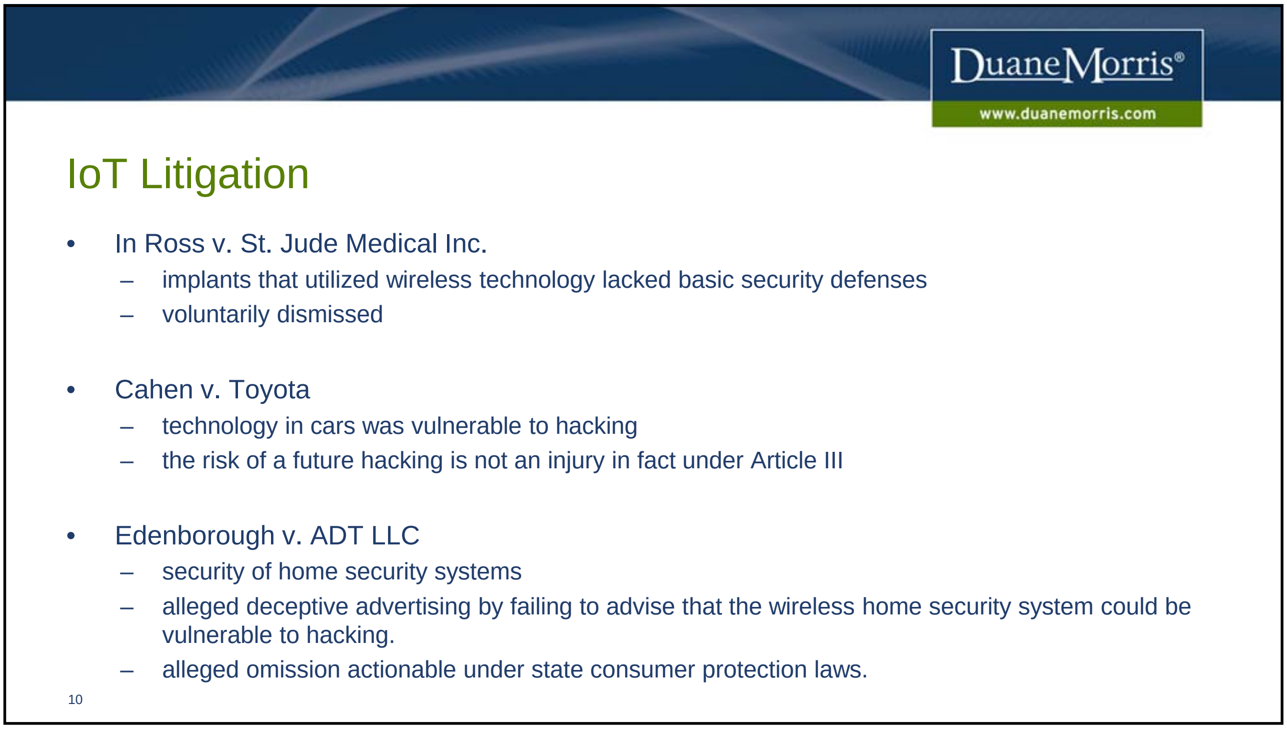
- IoT Hacks
    - Security cameras
    - Smart refrigerator
    - Baby monitors
    - Smart TVs



Legal Liability

- Impact of a seemingly innocuous attack on one component could cause catastrophic, irrevocable damage to another
  - One minor vulnerability in one device may be exploited and affect other vulnerabilities in the system, controlled, owned or supplied by different parties

  - Who takes responsibility?
    - ➢ Different devices
    - ➢ Communications
    - ➢ Infrastructure
    - ➢ Services
    - ➢ Different control and ownership



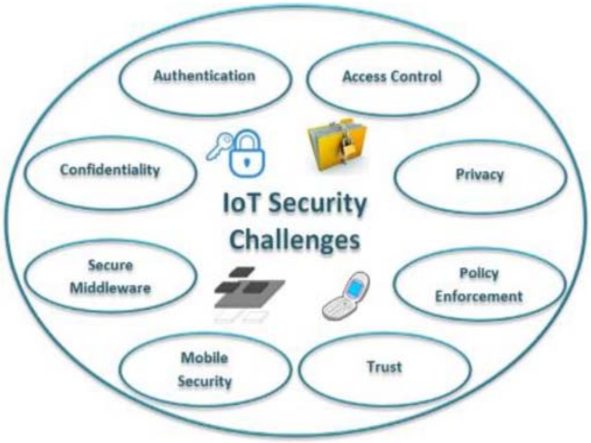
IoT Litigation

- In Ross v. St. Jude Medical Inc.
  - implants that utilized wireless technology lacked basic security defenses
  - voluntarily dismissed

- Cahen v. Toyota
  - technology in cars was vulnerable to hacking
  - the risk of a future hacking is not an injury in fact under Article III

- Edenborough v. ADT LLC
  - security of home security systems
  - alleged deceptive advertising by failing to advise that the wireless home security system could be vulnerable to hacking.
  - alleged omission actionable under state consumer protection laws.

Security and Privacy Challenges



IoT Security Challenges

Authentication

Access Control

Confidentiality

Privacy

Secure Middleware

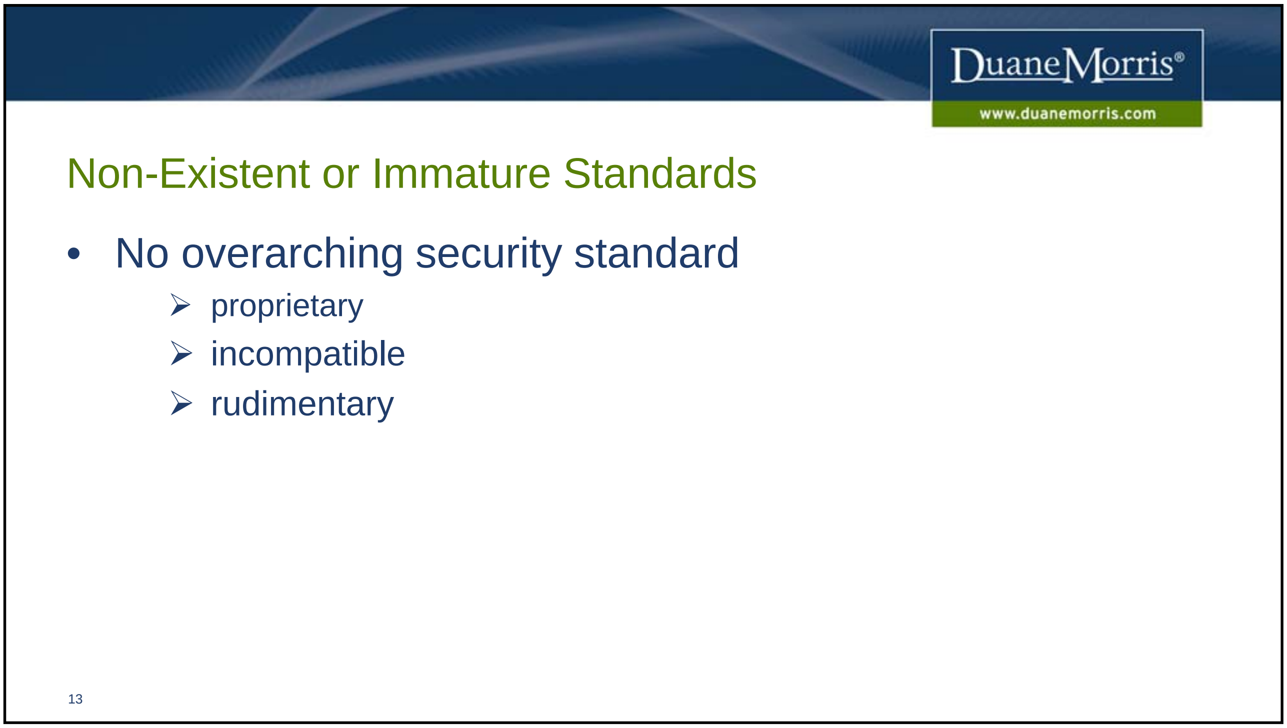
Policy Enforcement

Mobile Security

Trust

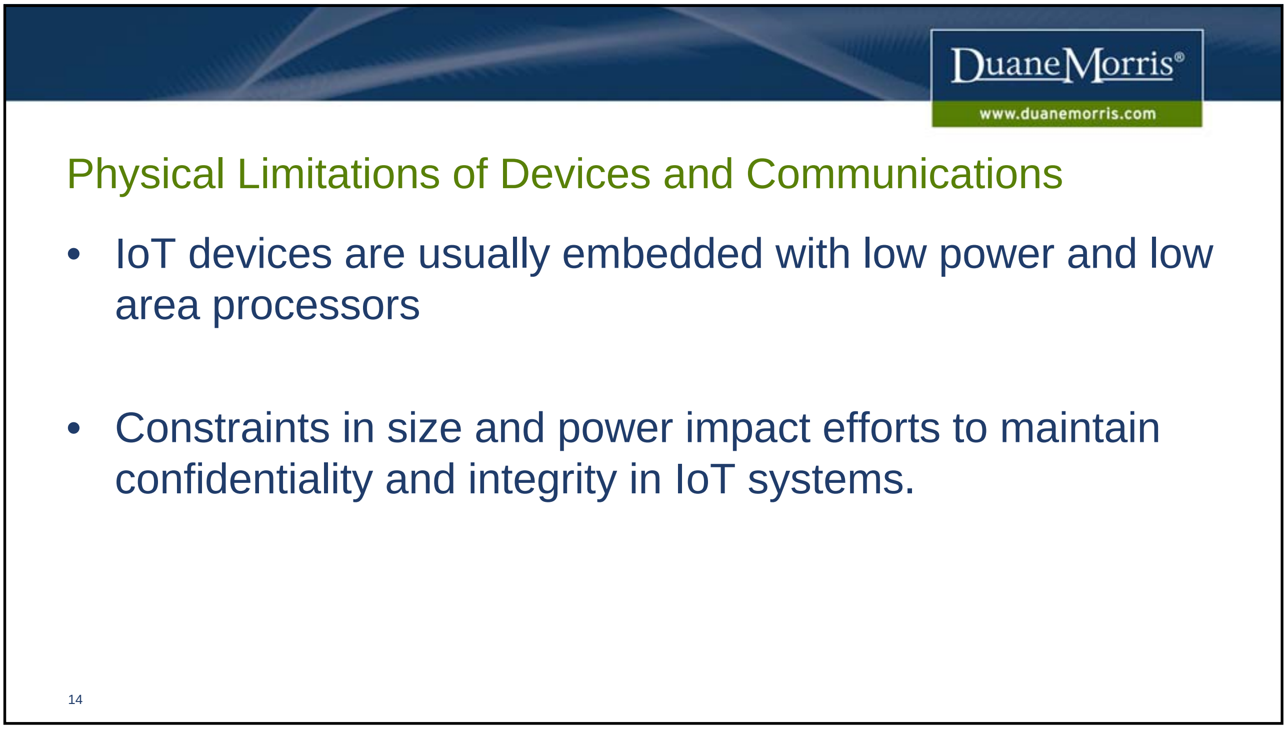
Gaps in Technical Sophistication

- Weakest link determines overall security level!
  - Need end-to-end security solutions
- Who will take the lead?
  - Component suppliers
  - OEMS
  - Integrators



Non-Existent or Immature Standards

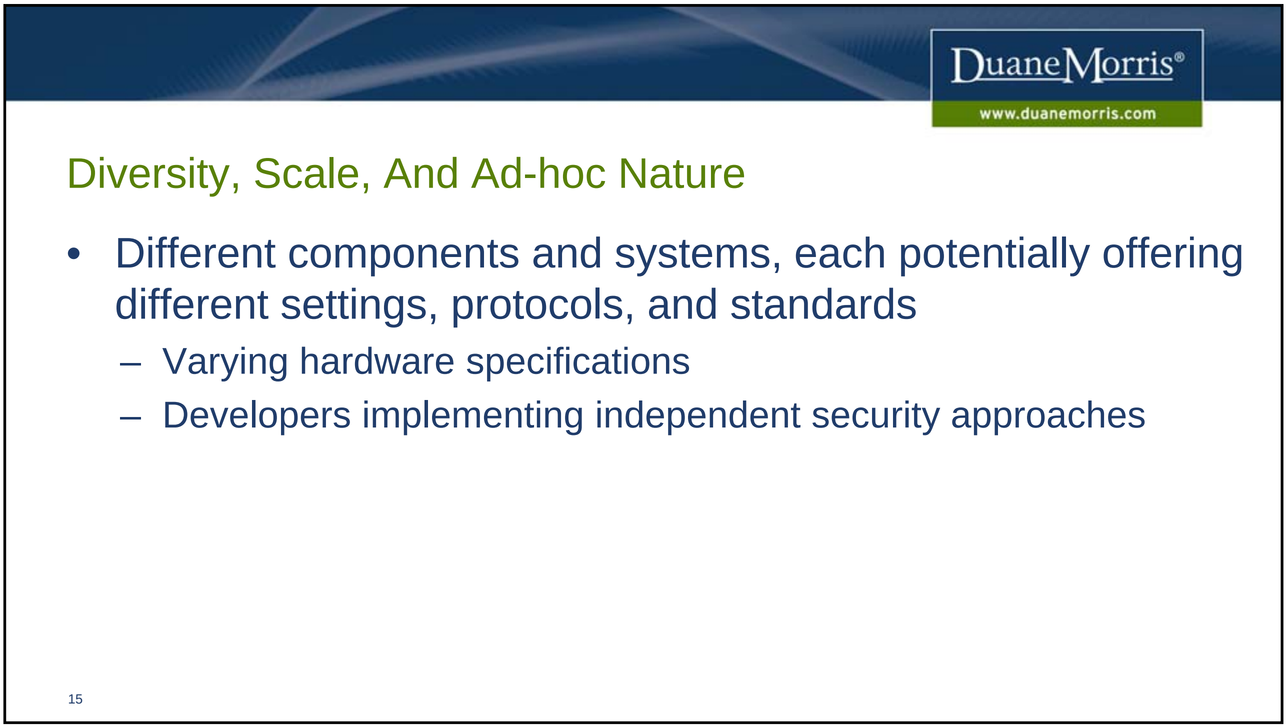
- No overarching security standard
  - proprietary
  - incompatible
  - rudimentary



Physical Limitations of Devices and Communications

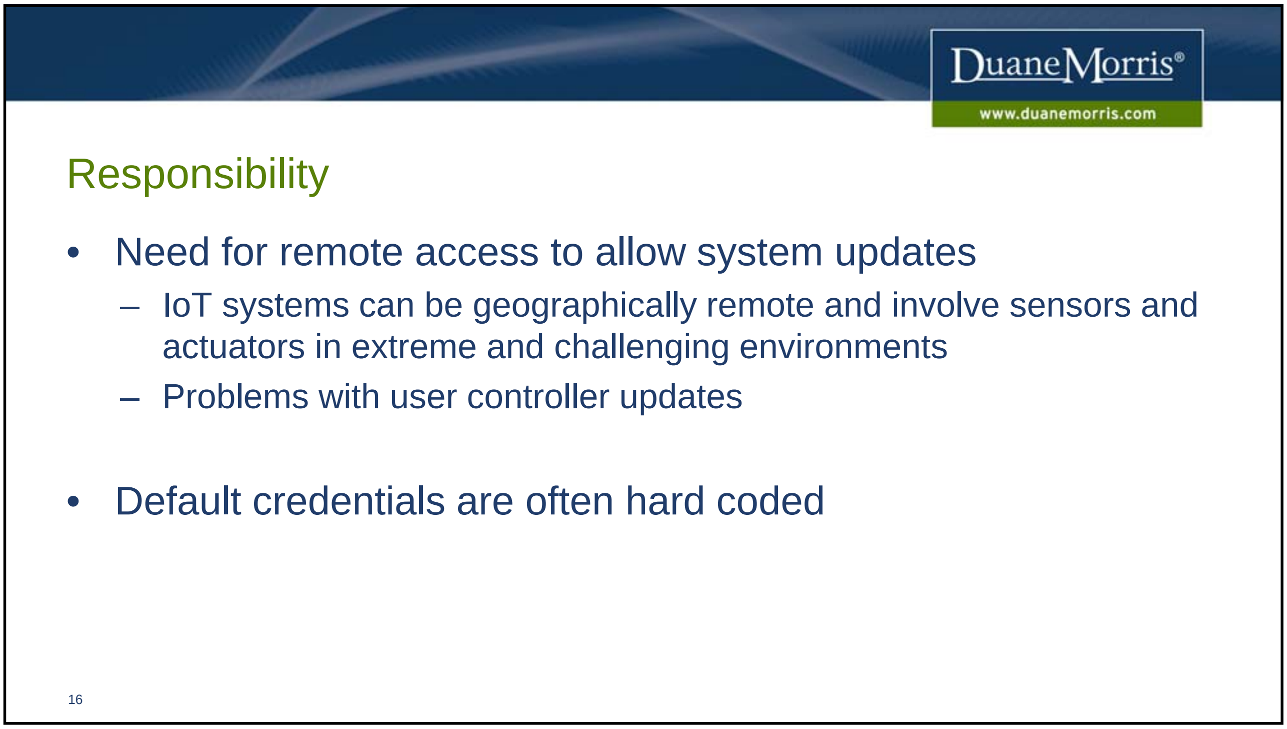
- IoT devices are usually embedded with low power and low area processors

- Constraints in size and power impact efforts to maintain confidentiality and integrity in IoT systems.



Diversity, Scale, And Ad-hoc Nature

- Different components and systems, each potentially offering different settings, protocols, and standards
  - Varying hardware specifications
  - Developers implementing independent security approaches

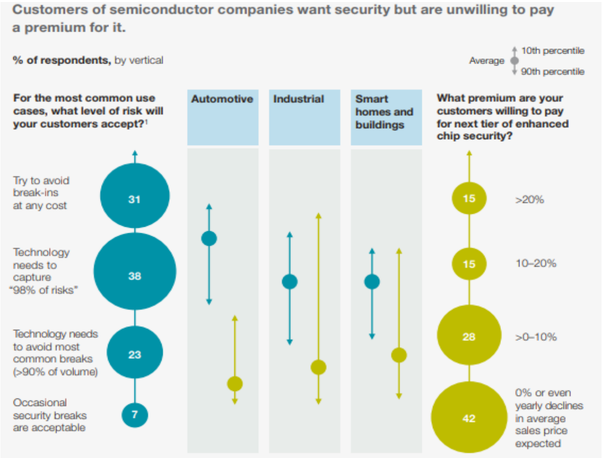


Responsibility

- Need for remote access to allow system updates
  - IoT systems can be geographically remote and involve sensors and actuators in extreme and challenging environments
  - Problems with user controller updates

- Default credentials are often hard coded

End Users View Security as a Commodity



Customers of semiconductor companies want security but are unwilling to pay a premium for it.

McKinsey/GSA Semiconductor Industry Executive Survey

Vast Amounts of Personal Data

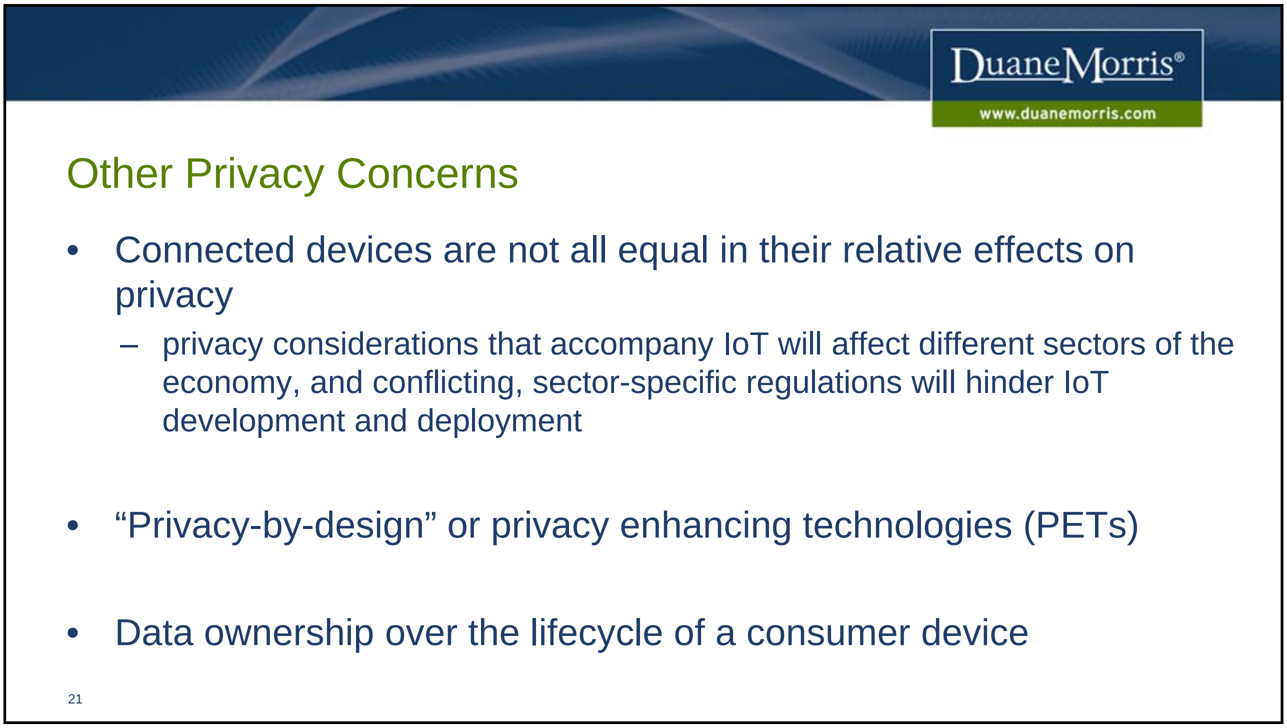
- Scope of personal data collected by connected devices is potentially immense
  - Sensors collect a variety of data
  - Data will be aggregated, analyzed, processed, fused, and mined in order to extract useful information for enabling intelligent and ubiquitous services

Privacy Concerns

- Transparency
  - users cannot determine what the device is doing and whether it is performing unwanted functions
- Visibility
  - devices and sensors, are typically small and unobtrusive
    - ➢ users may not be aware of the devices

Authentication and Identity Management

- Must establish permission to access
  - Authentication of person
    - ➢ IoT systems that feature mobile services will have users passing through different architectures and infrastructures owned by different providers
  - Authentication of service and devices
    - ➢ Must assure the data originated from the intended device, or was received by the intended device.
    - ➢ Must authenticate the service since certain services will have access to certain data

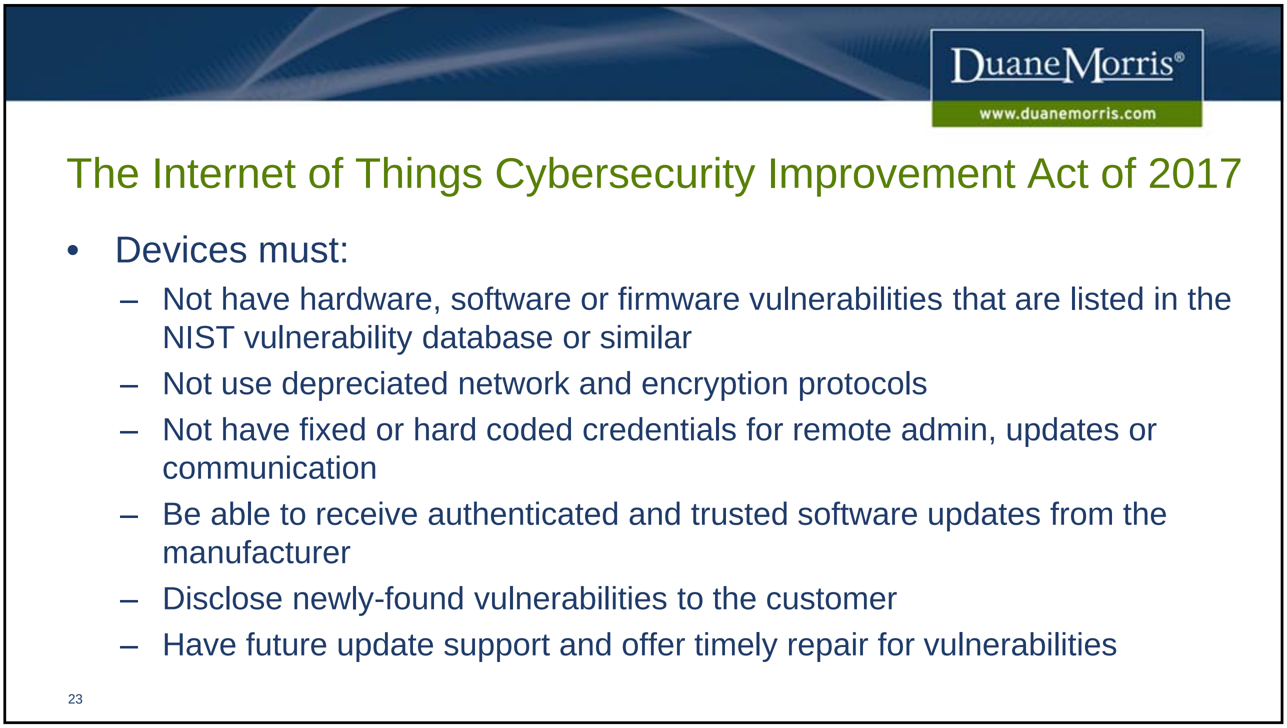


Other Privacy Concerns

- Connected devices are not all equal in their relative effects on privacy
  - privacy considerations that accompany IoT will affect different sectors of the economy, and conflicting, sector-specific regulations will hinder IoT development and deployment
- “Privacy-by-design” or privacy enhancing technologies (PETs)
- Data ownership over the lifecycle of a consumer device

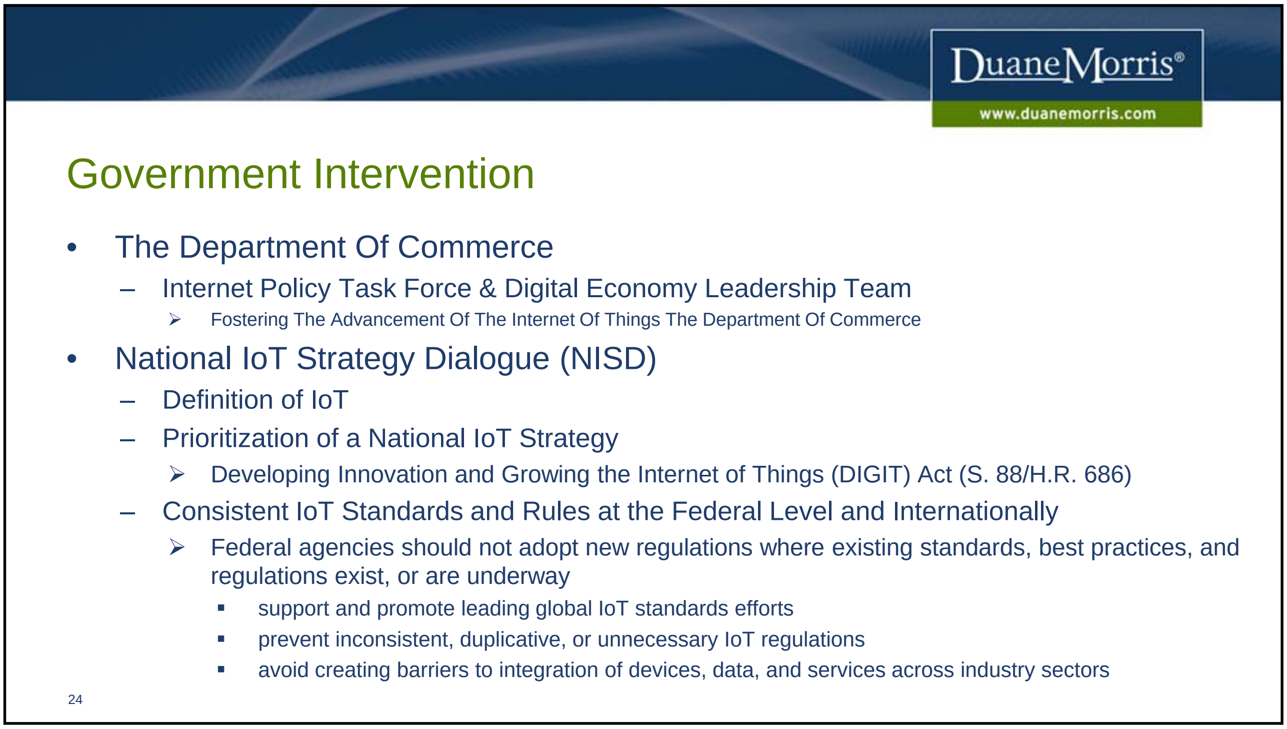
IoT Regulation

- Developing Innovation and Growing the Internet of Things Act (DIGIT) (S. 88/H.R. 686)
  - designed to create a working group of federal stakeholders to provide recommendations to Congress on the following facets of the internet of things: current and future spectrum needs; the regulatory scheme; consumer protection; privacy and security; and the current use of the internet of things by federal agencies
- The Internet of Things Cybersecurity Improvement Act of 2017
  - to establish requirements for vendors who supply the U.S. government with IoT devices



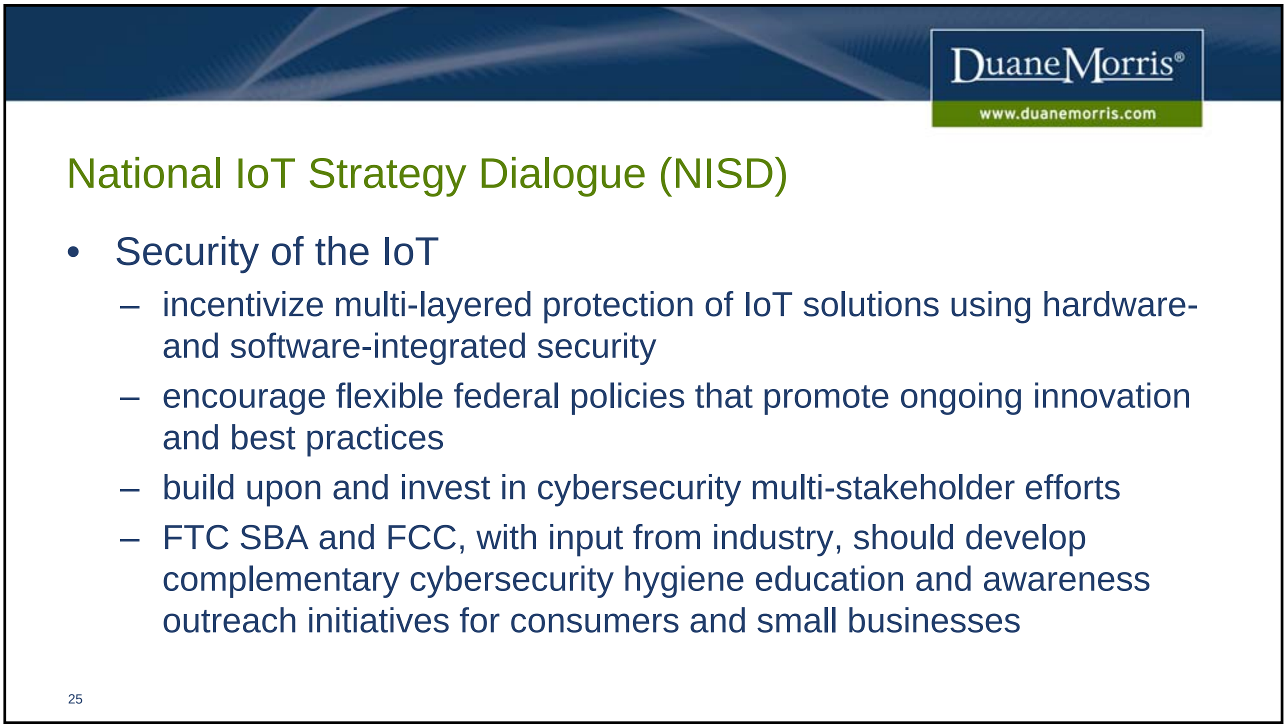
The Internet of Things Cybersecurity Improvement Act of 2017

- Devices must:
  - Not have hardware, software or firmware vulnerabilities that are listed in the NIST vulnerability database or similar
  - Not use depreciated network and encryption protocols
  - Not have fixed or hard coded credentials for remote admin, updates or communication
  - Be able to receive authenticated and trusted software updates from the manufacturer
  - Disclose newly-found vulnerabilities to the customer
  - Have future update support and offer timely repair for vulnerabilities



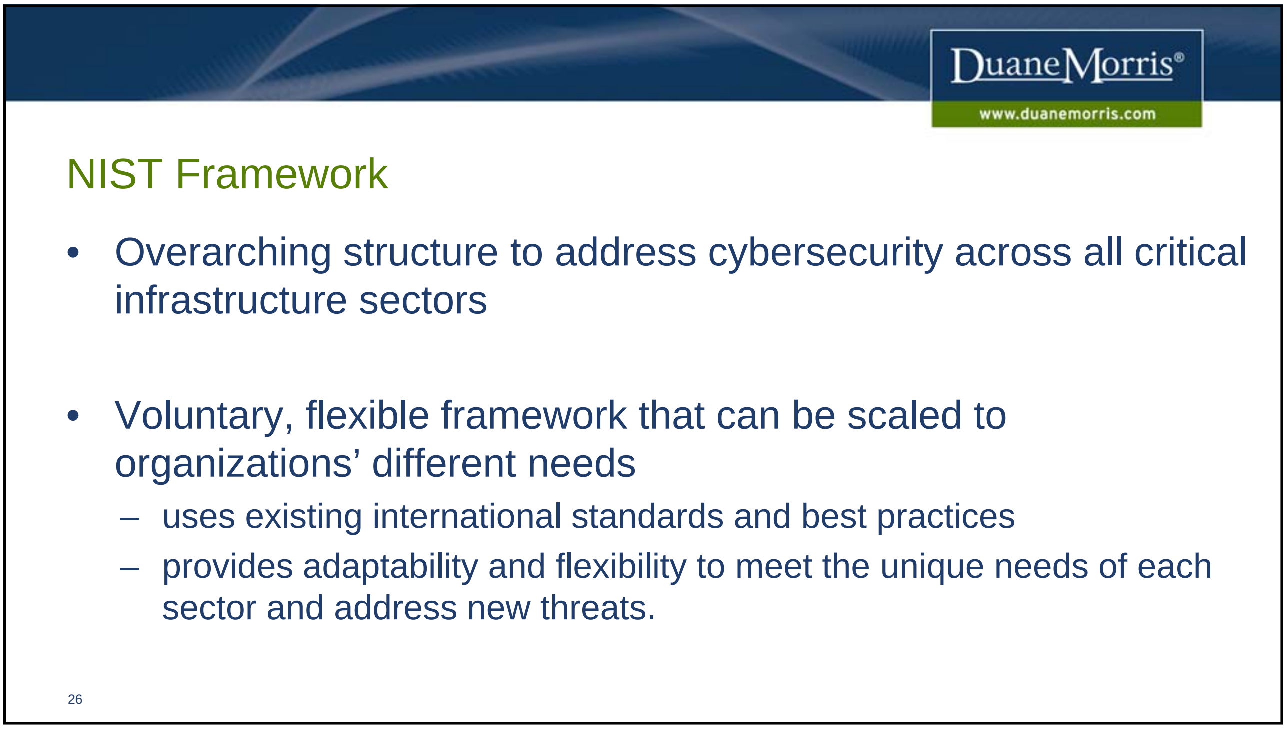
Government Intervention

- The Department Of Commerce
  - Internet Policy Task Force & Digital Economy Leadership Team
    - Fostering The Advancement Of The Internet Of Things The Department Of Commerce
- National IoT Strategy Dialogue (NISD)
  - Definition of IoT
  - Prioritization of a National IoT Strategy
    - Developing Innovation and Growing the Internet of Things (DIGIT) Act (S. 88/H.R. 686)
  - Consistent IoT Standards and Rules at the Federal Level and Internationally
    - Federal agencies should not adopt new regulations where existing standards, best practices, and regulations exist, or are underway
      - support and promote leading global IoT standards efforts
      - prevent inconsistent, duplicative, or unnecessary IoT regulations
      - avoid creating barriers to integration of devices, data, and services across industry sectors



National IoT Strategy Dialogue (NISD)

- Security of the IoT
  - incentivize multi-layered protection of IoT solutions using hardware- and software-integrated security
  - encourage flexible federal policies that promote ongoing innovation and best practices
  - build upon and invest in cybersecurity multi-stakeholder efforts
  - FTC SBA and FCC, with input from industry, should develop complementary cybersecurity hygiene education and awareness outreach initiatives for consumers and small businesses

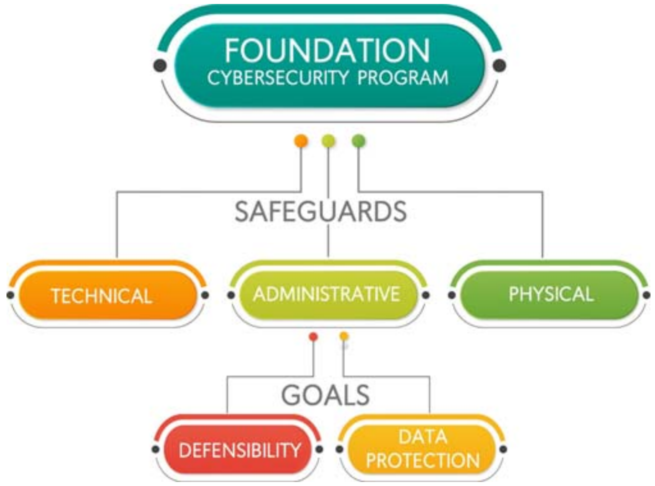


NIST Framework

- Overarching structure to address cybersecurity across all critical infrastructure sectors

- Voluntary, flexible framework that can be scaled to organizations' different needs
  - uses existing international standards and best practices
  - provides adaptability and flexibility to meet the unique needs of each sector and address new threats.

A Cybersecurity Risk Management Map



NIST Cybersecurity Framework

IDENTIFY

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

PROTECT

- Access control
- Awareness and training
- Data security
- Info protection and procedures
- Maintenance
- Protective technology

DETECT

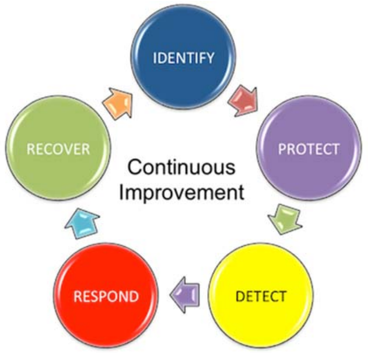
- Anomalies and events
- Security continuous monitoring
- Detection process

RESPOND

- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

- Recover planning
- Improvements
- Communications



DuaneMorris®

www.duanemorris.com

Questions?