Under Scrutiny: Contractors and Cybersecurity

Paul Rosen
Evan Wolff
David Bodenheimer
Michael Gruden
Navigating the Regulatory Seas: Information Security & Privacy Risk

- Navigating Government Contracts Information Security & Privacy Risk
  - Federal & Global Cyber Risks and Regulations

- Navigating IoT Cyber Threats & Risks
  - Where do they start? Or End?

- Navigating “Ordinary” Information Security & Privacy Risk
  - Legal Principles, Information Sharing, and Incident Preparation/Response
Navigating Government Contracts
Information Security & Privacy Risk

Federal & Global Cyber Risks and Regulations
Current Threat Environment

• Data breaches caused by third parties are increasing
• Nearly 50% of breaches are the result of hacking
• Almost 70% of breaches take 30 days or longer to detect
• 73% of breaches conducted by outsiders
• PII, payment, medical and credential data categories are most compromised

Sources: Ponemon and Verizon
DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (OCT 2016)

• Incorporated into all Department of Defense (DoD) contracts to protect sensitive Government information except exclusively off-the-shelf (COTS) items

• 3 Core Requirement of Clause
  (1) Safeguarding Covered Defense Information (CDI)
  (2) Flowdown Clause to Subcontractors
  (3) Cyber Incident Reporting

• December 31, 2017 Implementation Deadline
If Contractor processes, stores or transmits CDI on its information systems, it must implement “adequate security” on those systems to protect CDI.

- Contractor achieves “adequate security” by implementing all 110 controls in NIST SP 800-171
  - Includes System Security Plans (SSPs) and Plans of Action and Milestones (POAMs)
    - DoD may use SSPs and POAMs as Evaluation Factors and consider in Source Selection Decisions
What is Controlled Unclassified Information (CUI)?

- Categorized by the National Archives and Records Administration (NARA) and listed in the CUI Registry
- Common CUI Categories arising in Government Contracting include:
  - Controlled Technical Information
  - Export Control Information
  - Privacy Information such as PII and Health Data
  - Procurement and Acquisition Information
  - Proprietary Business Information
Subcontracting Requirements

- Prime must flowdown the Clause without alteration to subs whose performance requires use of CDI

- Prime must also require subs to:
  (1) Notify Prime when submitting NIST SP 800- 171 variance request to DoD CIO; and
  (2) Provide Prime Contractor with DoD incident report number upon cyber incident occurrence
Cyber Incident Reporting Requirements

- Contractor must report cyber incidents that either
  - “affect” CDI or any information system where CDI resides; OR
  - affect ability to provide operationally critical support
- Contractor must report through DIBNet portal within 72 hours of discovery
- Contractor must preserve and protect images of all information systems and relevant monitoring(packet capture) data known to be affected for 90 days from date of reporting

DFARS Cyber Incident Reporting
Recent DFARS Cyber Developments

• Draft NIST SP 800-171A, “Assessing Security Requirements for Controlled Unclassified Information” (FEB 2018)
  – Provides sample SSPs and POAMs
  – Requests a greater level of detail
  – Encourages organization to document CUI information types processed, stored, or transmitted by a system
  – Directs organization to provide detailed narrative that describes each system component within the system environment
  – Mapping tables and guidance in Appendices
Recent DFARS Cyber Developments

- DoD Updates to DFARS Safeguarding Clause Frequently Asked Questions (FAQs) (APR 2018), highlights include:
  - Unless prohibited by FAR/DFARS, all costs associated with compliance of DFARS 252.204-7012 are allowable.
  - May require contractors to identify and include POAMs for NIST SP 800-171 security controls NOT implemented at the time of award.
  - May require contractor to self-certify compliance with DFARS Clause 252.204-7012, including implementation of NIST SP 800-171.
  - Government may consider SSPs and POAMs when making overall risk management decision concerning contract award.
FAR Cyber Clause & Pending Developments

- FAR 52.204-21 (JUN 2016), Basic Safeguarding of Covered Contractor Information Systems
  - Mandatory in all contracts
  - Requires protection via 17 controls pulled from NIST SP 800-171

- Pending FAR Cybersecurity Clause
  - Pending FAR clause focused on Controlled Unclassified Information
  - Expected to largely mirror DFARS Safeguarding Clause
    - Would have same Safeguarding and Cyber Incident Reporting requirements
  - Expected to be proposed in the next few months
Federal Systems & Federal Information

- **FISMA (2014 revision)**
  - Increased accountability, reporting and oversight for data security and privacy

- **Revised OMB Circular A-130 (July 28, 2016)**
  - Data security and privacy are “crucial elements of a comprehensive, strategic, and continuous risk-based program”
  - Agency contracts must “enable agencies to meet Federal and agency-specific requirements pertaining to the protection of Federal information”

  - Applies to all who work with Privacy Act systems of records and federal PII, with flowdown requirement
  - Specified training requirements include Privacy Act, working with federal PII, incident response, and potential civil and criminal consequences for violations
European Legislation with Extraterritorial Effects

- GDPR will be effective May 25, 2018
- Harmonizes European data protection legislation
- Directly applies to all EU Member States
- Builds on existing legal concepts
- Strengthens rights of individuals
- Fines up to 4% total worldwide annual revenue or €20M ($23.7M currently), whichever is higher
General Data Protection Regulation (GDPR)

• GDPR applies if:
  o Establishment is operating in the EU, or
  o Not based in the EU but **either**
    1. Offering goods or services to EU-based individuals; OR
       ▪ Mere accessibility through website or providing email address or contact details is **NOT** sufficient
       ▪ EU language, payment in Euros **IS sufficient**
    2. Monitoring their behavior
       ▪ e.g., Using cookies to track & create consumer profile (analyzing/predicting preferences, etc.)
Navigating 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
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
“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
“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
“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

Department of Defense – Networks & Military Technology

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-17-668]
IoT Cyber Threats & Risks

Who Regulates? And How?
Who Regulates IoT?

Before IoT: Parallel Regulatory Regimes (Privacy & Cyber)

Patchworks

• **Privacy**
  - HIPAA
  - GLB
  - FERPA
  - Privacy Act

• **Cyber**
  - FISMA
  - FAR
  - DFARS
  - GSA, HHS . . . .

Technology Fusion

• **IoT & Drones**
  - “next trillion files”
  - FAA regulate IoT?

• **IoT + Cloud + AI**
  - FedRamp
  - DFARS
  - Antitrust (DOJ vs. FTC)
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 of Senate & House Hearings
Who Regulates IoT?

Federal Agencies & IoT Oversight

**Federal Agencies**

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

**& More Agencies**

- **DOE**
  - Smart grid
- **DOT**
  - Connected cars
- **DOD**
  - Advanced Tech
- **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]
IoT Cyber Threats & Risks

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**

3. **Build on Proven Security Practices**

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>DOD, DISA, and Department of the Navy</td>
<td>Government / Personal</td>
</tr>
<tr>
<td>Component Policies on Wireless and Personal Portable Electronic Devices 2014 and 2016</td>
<td>DISA</td>
<td>Government</td>
<td>Smart watches / Infra devices</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>Smartphones</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>

---

*Source: GAO analysis of Department of Defense (DOD) information, 1 GAO-17-688*
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 (over 70)
• Agency guidance (e.g., DOT ITS-JPO, FDA, GSA)
• Existing & emerging industry standards (e.g., ISO/IEC, OMG)

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>Cryptographic Techniques</td>
<td>ETSI; IEEE; ISO/IEC JTC 1; ISO TC 68; ISO TC 307; W3C</td>
<td>Standards Available</td>
<td>Standards Available</td>
<td>Some Standards Available</td>
<td>Standards Available</td>
<td>Some Standards Available</td>
</tr>
<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; ODF; 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>
IoT Cyber Threats & Risks
Protecting Yourself on the IoT Frontier

Define IoT
• Enforceable contract terms or security plans?

Tailor your requirements
• No one-size-fits-all (per NIST) – vs. sector-by-sector

Pick your security standard

Perform your risk assessment
• All standards – Bang-for-buck

Know your supply chain
• Market leverage & privity?
• Security savvy?

Wild, Wild West of IoT
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.”

[Geoff Webb, How will billions of devices impact the Privacy of Things? (Dec. 7, 2015)]
Navigating “Ordinary” Information Security & Privacy Risk

Legal Principles, Information Sharing, and Incident Preparation/Response
Managing Ordinary and Government Contract Risk Throughout the Business Lifecycle

• Governance
• Corporate policies and procedures, especially Incident Response Plan
• Vendor management, compliance terms, and flowdown
• Business transactions and privacy and information security due diligence
• Training and awareness
Managing Risk with Effective Incident Response: Prepare, Practice, and Execute

• Legal Principles:
  – Minimizing attack surface – e.g. does IoT need to be connected to myriad of devices or does a single ISP suffice?
  – Spreading risk – not one person owns all the risk
• Incident response plan (IRP)
• Incident response team (IRT), including third party forensics and outside counsel
  – IRT considered a “team sport”
    • Information Technology, Legal, Business, Communications, CEO
• Tabletop exercises
Incident Response

• Focus on IT attacks and prevention
  — Offensive and defensive perspectives
• Incident Response Plan (IRP)
  — Manage external risks
• Investigation triggered by incident report -- Focus on security, mitigation and evidence gathering
• Data breach-related notification requirements
  — Legal, regulatory and contractual compliance
  — Response timelines
  — Methods of notification
• Anticipate and assess litigation risks
Incident Preparation

- Tabletop Exercises
  - Conduct tabletop exercises at multiple levels
    - Ground level/first responders
    - Executive level
    - Enterprise level: don’t overlook middle management
- Vulnerability Assessments
- Pen Tests
- Train to Incident Response Plan:
  - Write to IRP, Train to IRP, Review IRP
Cyber Insurance Coverage

- Cyber insurance encompasses both third-party losses (liability to others) and first-party losses (losses to policyholder’s own business interests).
- Cyber coverage programs are often negotiated based on individual company needs, especially for larger insureds.
- No “standardized” insurance policy forms, so various insurers’ and brokers’ policy forms differ in the scope of coverage provided.

- Type of losses cyber insurance may include:
  - Privacy & Network Security Risk
  - Privacy & Network Security Liability
  - Privacy Regulatory Fines and Penalties
  - Media Liability
  - Dependent Business Interruption/Dependent System Failure
  - Cyber Extortion
  - Digital Asset Restoration
  - PCI Fines and Penalties
  - Breach Event Expenses
  - Network Business Interruption
  - System Failure
Post-Dive Wrap-Up: Managing Information Security & Privacy Risk

- Implement Physical, Technical, and Administrative Controls to address risks, compliance and otherwise
- Establish Appropriate Governance
- Review and Update Policies & Procedures Regularly
- Analyze Internet of Things interconnections
- Prepare for Data Incidents in Advance (Incident Response Plan, Team, Tabletop, Data Breach Toolkit)
- Review Vendor Management Process
- Analyze Audit and Reporting Processes
- Participate in Industry and Government Partnerships
QUESTIONS?

David Bodenheimer  
(202) 624-2713  
dbodenheimer@crowell.com

Michael Gruden  
(202) 624-2545  
mgruden@crowell.com

Paul Rosen  
(213) 443-5577  
prosen@crowell.com

Evan Wolff  
(202) 624-2615  
ewolff@crowell.com