CHASE

Cyber/Physical Security and the Internet of Things: Defense Considerations

Robert S. Metzger
Rogers Joseph O'Donnell, P.C.
875 15th Street, N.W., Ste 725
Washington, D.C. 20005
(202) 777-8951
rmetzger@rjo.com www.rjo.com

State of DIB Cyber/Physical Measures

CHASE

IoT Threat

An adversary may exploit cyber-active devices or the means by which these are connected to or managed by infrastructure to deny, disrupt or impair functionality of defense systems.

Question

How well do current DoD initiatives assure that the defense industrial base acts to extend security to address this threat?

Answer

Not well.

Measures taken by DoD focus on contractor protection against counterfeit electronic parts (physical) and protection of information and information systems (cyber) but not on cyber/physical threats.

CHASE

Introduction

Software Attacks with Physical Effects

CHASE

On March 24, 2016, the Department of Justice announced charges against an Iranian hacker who mounted a cyber-physical attack upon the Supervisory Control and Data Acquisition (**SCADA**) systems of the **Bowman Dam**, in Rye, New York. The charges are that the hacker repeatedly obtained information regarding the status and operation of the dam, including information about the water levels and temperature, and the status of the sluice gate, which is responsible for controlling water levels and flow rates. The hacker obtained access that, ordinarily, would have enabled him to remotely operate and manipulate the dam's sluice gate.

An IoT attack upon Industrial Control Systems (**ICS**) might not have the immediacy or threaten physical harm to the safety of Americans as could a SCADA attack upon power grids or flood control infrastructure, but the economic damage and the impairment of defense manufacturing capabilities could be profound. Here too, there is real-world evidence of the power – and danger – of ICS attacks. Once inserted into the ICS that controlled Iran's uranium enrichment facilities, in 2009-10, the "**Stuxnet**" virus produced high rates of failure of centrifuge equipment and crippled Iran's nuclear ambitions. This is an early but cautionary example of how malicious software code can be spread among ICS with devastating industrial effect.

Definitions – and links: IoT ≅ CPS

CHASE

"IDC defines the **IoT** as a network of networks of uniquely identifiable endpoints (or 'things') that communicate without human interaction using IP connectivity. IDC has identified the IoT ecosystem as containing a complex mix of technologies including, but not limited to, modules/devices, connectivity, IoT purpose-built platforms, storage, servers, security, analytics software, IT services, and security. It is important to note that autonomous connectivity is a key attribute within IDC's definition and, at this point, we do not count smartphones, tablets or PCs within our IoT forecast."

IDC Forecast, "Explosive Internet of Things Spending to Reach $1.7 Trillin in 2020, According to IDC," June 2, 2015.

"Cyber-physical systems (**CPS**) are smart systems that include engineered interacting networks of physical and computational components. These highly interconnected and integrated systems provide new functionalities to improve quality of life and enable technological advances in critical areas, such as personalized health care, emergency response, traffic flow management, smart manufacturing, defense and homeland security, and energy supply and use. In addition to CPS, there are many words and phrases (Industrial Internet, Internet of Things (IoT), machine-to-machine (M2M), smart cities, and others that describe similar or related systems and concepts."

NIST, Draft Framework for Cyber-Physical Systems, Release 0.8, Sept. 2015

ICS & the IOT

"The early visionaries of the Internet of Things, IBM's thought leaders among them, foresaw a time when practically any physical object could be equipped with sensors and hooked up to the Internet to translate the physical world into digital information.

They were focusing on factory assembly lines, electrical grids, automobiles, highways, buildings, and the like. The goal was to **gather streams of information from sensors** that could be used to automate processes—such as balancing supply and demand in a power grid—and operate more efficiently.

***

Think of it this way: First-generation IoT technologies gave us nuggets of information that could make a big difference in achieving operational efficiencies. The next generation creates vast communities of devices that share information, which in turn can be interpreted in a larger context and managed by people using cognitive systems. **In the era of Cognitive IoT, no machine is an island**."

Harriet Green, "Cognitive IoT: Making the Internet of Things Deliver for All of Us," Dec. 15, 2015, at http://www.ibm.com/blogs/think/2015/12/15/cognitive-iot-making-the-internet-of-things-deliver-for-all-of-us/ (Emphasis added.)

Industrial Control Systems (ICS): A term used to encompass the many applications and uses of industrial and facility control and automation systems. ISA-99/IEC 62443 is using Industrial Automation and Control Systems (ISA-62443.01.01) with one proposed definition being "a collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process." The following table includes just a few of the ICS-related applications and labels we use.

Types of Industrial/Facility Automation & Control	Uses & Applications	Examples
SCADA & EMS – Supervisory Control & Data Acquisition & Energy Management System	Control and data acquisition over large geographic areas	SCADA & EMS – Supervisory Control & Data Acquisition & Energy Management System
DCS - Distributed Control System	Systems which control, monitor, and manage industrial processes that are disbursed but operated as a coupled system	DCS - Distributed Control System
PCS – Process Control System	Systems which control, monitor, and manage an industrial processes	PCS – Process Control System
Building Automation, BMS -Building Management System	Control systems used to manage security, safety, fire, water, air handling in a building or facility	Building Automation, BMS -Building Management System
I&C - Instrumentation & Control	Electronic devices or assemblies used to monitor, measure, manage or operate equipment in many applications	I&C - Instrumentation & Control
SIS - Safety Instrumented System, safety systems, protection systems	System with the sole function to monitor specific conditions and act to maintain safety of the process	SIS - Safety Instrumented System, safety systems, protection systems

SANS, "An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity," Aug. 2014, available at https://ics.sans.org/media/An-Abbreviated-History-of-Automation-and-ICS-Cybersecurity.pdf.

CHASE

The IoT Poses New Risks to Key Defense Systems and the Defense Industrial Base

IoT Poses New and Different Risks

- Risk: $\int$ **T**(threat) x **V**(vulnerability) x **C**(consequence) $\pm$ Mitigation
- IoT Risks reflect new threats, more vulnerability and broader consequence. Mitigation challenged by scale and diversity.
  - **Threats** may increase: more potential "adversaries" – including commercial rivals – have motivation to attack, with attractive "RoI."
  - **Vulnerability** increases because of proliferated attack surfaces and risk that poor system or device design will easily exploitable.
  - **Consequences** extend beyond traditional data-focused information security objectives to include cyber/physical impacts to safety, system, facility or even enterprise functionality.
  - **Mitigation** is challenging because of the quantity of at-risk devices and absence of methods to rapidly collect, assimilate and respond to events.

Cyber/physical risks extend throughout product lifecycle. Increased use and of reliance upon connected cyber-active devices enable network-directed software attacks to produce widespread hardware effects and collateral damage to dependent systems.

New Threat Dimensions

CHASE

Attack Surfaces

The IoT operates by connection of end-point devices (e.g., sensor networks) to control systems and by communication along the edge as well as to the core. As seen by adversaries, attack surfaces will multiply, to include end-point devices, network interconnections, transport infrastructure and control systems. Authentication, identity management and transaction processing, as may be cloud-delivered, add to exposed surfaces. System-directed attacks may exploit insecure web connections. Attacks could be directed to core (client) functions, such as data analytics, which act upon received sensor data to generate instruction. **IoT implies massive interconnectivity and constant interdependence among devices, communications and control.**

Defense Manufacturing

For illustration, the IoT could enable factory equipment to self-monitor, predict fault, adjust function, balance load and call for maintenance. Such functionality exists today, but its importance will grow. The IoT will facilitate advances in manufacturing, but autonomous communications among machines and "cognitive computing" could be vulnerable to attacks that disable factories.

Defense Logistics

The DIB is likely to employ IoT devices for efficient resource allocation and enhanced functionality. Improved "liquidity" of assets is a promising prospect. IoT devices might be used for defense logistics, e.g., widespread distribution of wireless smart tags to monitor readiness, track availability and inform disposition decisions for physical assets such as pre-positioned military stores.

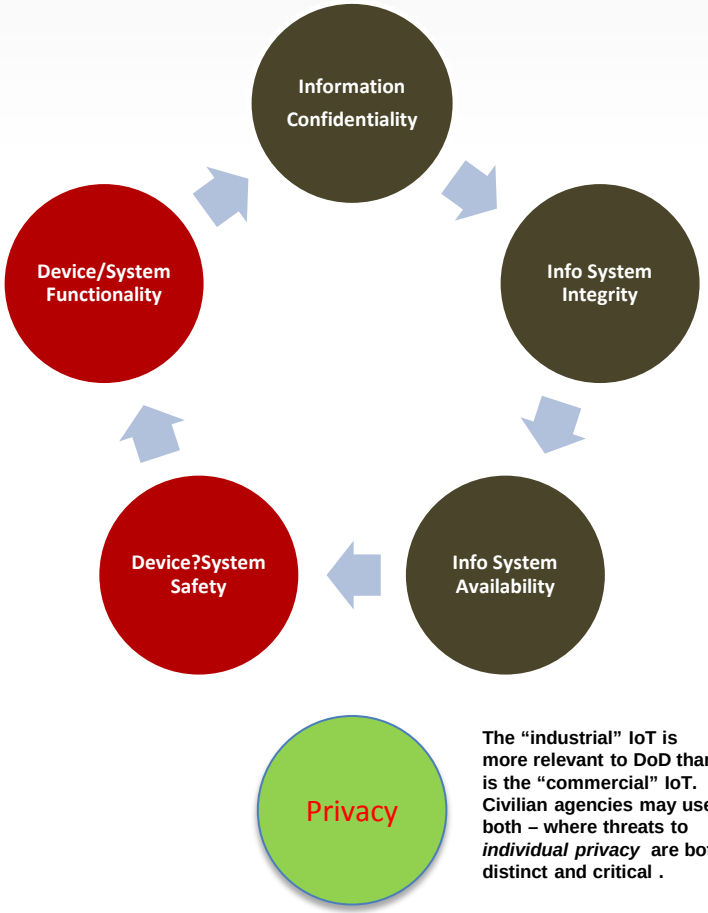
"Attack Once, Impact Many"

Where devices and dependent systems possess common vulnerabilities, single entry point attacks can circulate and impact numerous connected or co-dependent systems. One IoT attack could degrade or disable many power generators across an entire grid. An IoT attack, conceivably, could "poison" the military logistics decision system, leaving commanders without knowledge of equipment availability and readiness. Similar risks are posed to IoT-enabled manufacturing systems.

Cyber/Physical Risks Specific to Defense

- The prevailing cyber threat to information stored on networks is delivered or enabled by software.
  - Compromise to information confidentiality risks loss of DoD technical data and dilutes U.S. technological advantage.
- Cyber/physical threats will operate at the device level and present a panoply or risks, e.g.,
  - To information and information system interests already the subject of FIPS 199 (confidentiality, integrity and availability);
  - To the functionality and safety of devices, units, systems; factories and facilities;
  - To mission fulfillment and leadership confidence (as to critical systems).
- DoD today faces cyber/physical risks in the sustainment of legacy equipment. With the IoT will come new functionality and new risks for ICS.

IoT Threats Expand Beyond FIPS 199:



The "industrial" IoT is more relevant to DoD than is the "commercial" IoT. Civilian agencies may use both – where threats to *individual privacy* are both distinct and critical .

CHASE

Do Federal Measures Protect Key Defense Systems & Infrastructure Against IoT Risks?

Scorecard: Actions Directed to Contractors

CHASE

DoD Action	Import for Cyber/Physical Security
NDAA FY 2011 § 806 Interim & Final Rule: "Supply Chain Risk"	Focuses on sources of potentially corrupted parts or equipment. Limited benefit.
NDAA FY 2012 § 818 and Final Rule: Detection & Avoidance of Counterfeit Parts *Proposed DFAR (Sep. 2015) eliminates ""embedded software or firmware" from definition of "counterfeit electronic part"*	Focuses on counterfeit electronic parts. Limited benefit to avoidance of corrupted or exploitable cyber-active parts.
Proposed FAR: Expanded Reporting of Nonconforming Supplies (June 2014)	Not implemented. If implemented, could promote exploit information exchange.
DFARS: UCTI Rule (2013) and Network Penetration and Reporting Rule (2015)	Focus is on protection of information and information systems. SP 800-171 protects networks but not cyber/physical systems. Reporting required on cyber events but not cyber/physical attacks.
NDAA FY 2016 § 1647: Evaluation of Cyber Vulnerabilities of Major Weapon Systems	DoD required to evaluate cyber vulnerabilities of each major weapon system and to develop risk mitigation strategies.

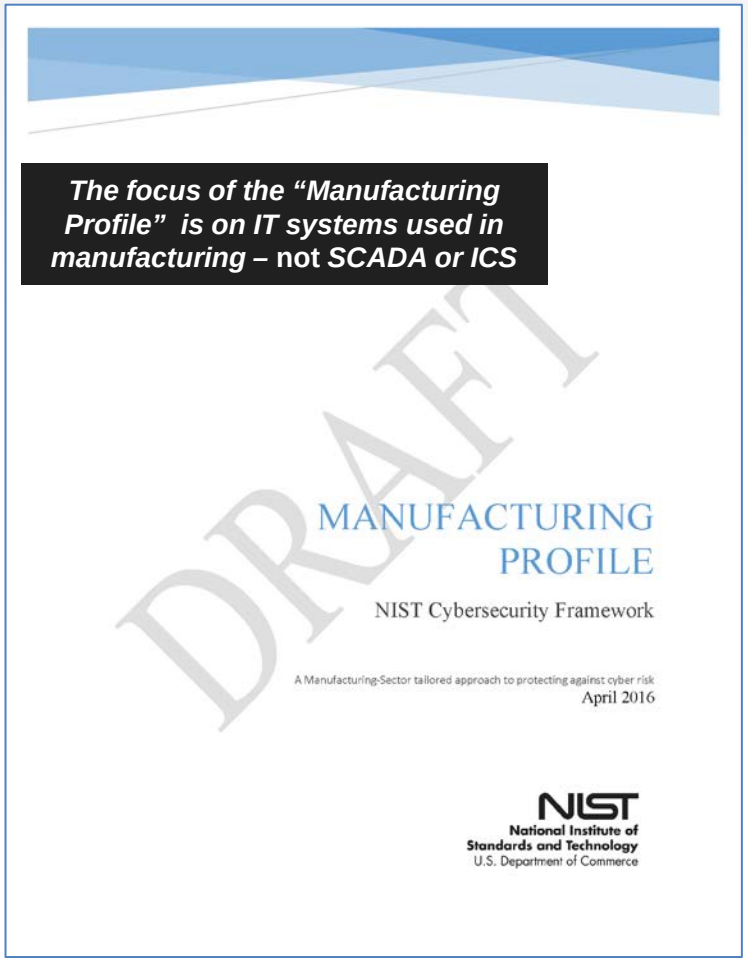
DFARS 252.204-7012 and ICS Threats

CHASE

- "Network Penetration" DFARS (252.204-7012) will have limited benefit to protect DoD interests against IoT threats to ICS.
  - The DFARS protects "Covered Defense Information" against compromise. Contractors may not understand CDI to include sensitive factory data.
  - "Controlled technical information" must be marked per DoDI 5230.24.
  - The focus is protection of information on ICT systems. Contractors may not address cybersecurity of Industrial Control Systems.
  - It relies upon new safeguards established by NIST SP 800-171 which-
    - Seeks to protect only "confidentiality" and not "integrity" or "availability."
    - Does not address functionality or safety or consider ICS (or SCADA) as such.
    - Employs 14 control "families" from FIPS-200 that are ICT-specific and do not consider SCRM subjects such as Secure Systems Engineering.
  - Contractors now have until Dec. 31, 2017 to comply with 800-171.

The "Net Pen" DFARS were promulgated to deal with network-enabled cyber threats distinct from cyber/physical threats presented to ICS and SCADA by IoT functionalities.

Voluntary Measures?



Coming May 10, 2016:
NIST SP 800-160 System Security Engineering

Can the NIST Voluntary Framework serve to protect defense manufacturing?

- Follows Framework: Identify, Protect, Detect, Respond & Recover
- Four "Business/Mission" Objectives
  - Personnel Safety; Environmental Safety; Quality of Production; Production Goals
  - *Compare* to CFAM objectives: Theft or Alternation of Technical Data; Disruption or Denial of Process Control
- 98 "security objectives"- 20 categories

  E.g, (I) Asset Mgmt., (P) Access Control, (D) Anomalies & Events, (R) Communications, (R) Improvements

CHASE

Using Acquisition Authority to Respond to IoT Risks to Key Defense Systems & Infrastructure

Acquisition and Cyber/Physical Threats

CHASE

Premises:

DoD's principal concern is with *industrial* or *enterprise* IoT (not "commercial")

Certain missions, systems and infrastructure will become exposed to IoT threats and must be protected.

Some DIB participants will act to address cyber/physical threats.

Others will promise but not take effective actions.

Many will act only if required. Even a few "gaps" could be disastrous.

Propositions:

Acquisition methods can be used to help address cyber/physical threats posed to DoD systems and capabilities (and critical infrastructure) through the IoT.

Caution is necessary to avoid frustration of IoT promise or separation of DoD from leading commercial-source technologies.

Selective adaptation of existing SCRM and Cyber initiatives can assure DoD that its supply chain will assess and act to reduce exposure to cyber/physical threats.

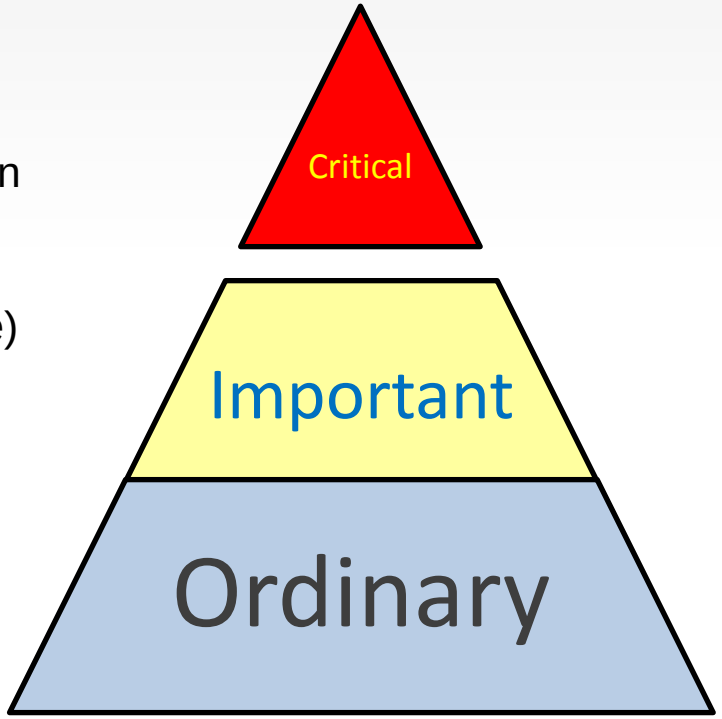
Standards can serve an important role to guide industry outcome.

Potential Acquisition-Based Response

CHASE

For "Critical" IoT-Exposed Systems

- Risk-based analysis (agency)
  - *Threat*: motivation and capability of adversary
  - *Vulnerability*: susceptibility to corruption or subversion
  - *Consequences*: impact of penetration on mission
  - Opportunities for *Mitigation* (to each of T, V & C)
- IoT (C/PS) Risk Management Framework (RMF) (to come)
  - Encourage Contractor assessment against RMF?
  - Direct IoT System Security Report & Plan?
  - Reward/Fund "E2E" System Security Engineering
- Specific Solicitation & Contract Measures (Potential)
  - Restrictions on suspect sources
  - IoT-Specific Security Controls (NIST or Standards)
  - Mandatory Fit/Gap Report vs. Controls
  - Evaluation credit for secure system engineering
  - IoT Security Authorization Process and ATO
  - 3d Party Assessment and external monitoring
  - Require component/sensor deployment database
  - Mandatory event reporting
  - "IoT-CERT" to disseminate events/enable response



For non-critical systems, develop criteria for agencies to identify "at risk" IoT. Develop C/PS RMF for use across multiple industries. Encourage or require contractor use of sector-specific industry standards. Rely upon contractor self-assessment. Require and facilitate event reporting.

Building on Present Accomplishments - I

CHASE

① Encourage DIB participants to self-assess for CPS and ICT vulnerabilities. (Apply Framework Core and Profiles?)

② Promote development of Standards (e.g., ISO/IEC 20243, NIST SP 800-82, SP 800-160) and Best Practices specific to cyber/physical threats and responsive to sectoral specifics.

③ Fund development of technical methods to protect critical IoT systems and for test and inspection to authenticate suspect cyber-active parts.

④ Apply § 1647 results for "triage" to identify at-risk key systems. Create and fund IoT Assurance Center to test and mitigate.

⑤ Compile BoM of active electronic parts for at-risk key systems.

⑥ Expand reporting obligations to include exploits of cyber-active parts and malicious code events.

Building on Present Accomplishments - II

CHASE

⑦ Collect exploit and event information and integrate other threat information. Feed IoT-CERT with CSIA-like info exchange.

⑧ Create and use data analytics and automated decision methods to disseminate device-specific reports to key DoD users.

⑨ Consider regulations requiring DIB primes to adopt systems to anticipate and avoid cyber/physical vulnerabilities, to employ SSE per relevant industry standards and to assure device provenance.

⑩ Consider regulations to obligate DoD contractors to monitor IoT-enabled systems and report on cyber/physical system attacks.

DoD and its principal suppliers should act now to anticipate cyber/physical threats that accompany IoT application to critical defense functions. Answers will be found in end-to-end attention to security throughout product design and lifecycle and recognizing the many vulnerabilities of connected systems with active endpoints. DoD should guide and encourage responsible measures and use acquisition tools only when the risks and responses are better understood.

CHASE

Conclusion:
Thoughts about the Federal Role

IoT Risks Generally: the Federal Role

CHASE

① Promote continuing development of scalable IoT and cyber/physical norms, standards and best practices, while taking care to avoid both prescriptive solutions or the potential chaos of competing and conflicting norms.

② Establish lead authorities for federal oversight; coordinate sector-specific initiatives among multiple federal agencies to address key concerns of security, privacy, functionality, information sharing, recovery.

③ Sponsor sector-specific public-private partnerships to act upon new threats and to disseminate methods to identify, protect, detect, respond and recover.

④ Fund and validate technical methods to reduce IoT vulnerabilities, e.g., secure chips for ID authentication, physical tests to detect device corruption; blockchain, DRM.

⑤ Cause all federal agencies to assess vulnerability of critical systems and infrastructure to cyber/physical threats, and to implement protection plans.

⑥ Assess use of law enforcement, agency and private causes of action to punish offenders and to motivate proactive corporate actions to avoid IoT risks.

⑦ Examine how to employ federal procurement authority (regulations, solicitation requirements, contract clauses, system oversight and contractor administration) to reduce IoT vulnerabilities and recognize, avoid and recover from IoT threats.

About the Presenter

This presentation reflects Mr. Metzger's personal views and should not be attributed to any client of his firm or organization with which he is involved or affiliated.

Robert S. Metzger
Rogers Joseph O'Donnell PC
202-777-8951
Rmetzger@rjo.com

Robert S. Metzger heads the Washington, D.C. office of Rogers Joseph O'Donnell, P.C., a law firm that specializes in public procurement matters. He advises leading U.S. and international companies on key public contract compliance challenges and in strategic business pursuits. Bob is recognized for work on supply chain and cyber security. On these subjects, he has published extensively and has made presentations to many government, industry, legal and technical groups, among them ABA (PCL, S&T, SLD), AIA, ASIS, CALCE, CFAM, DoD, DIB SCC, DoJ, DSB, ERAI, Georgetown Law, Harvard Kennedy School, IPC, National IPR Center, NCMA, NDIA, SAE, SMTA, SSCA and TRANSCOM.

Recently named a 2016 "Federal 100" awardee, Federal Computer Week said of Bob: "In 2015, he was at the forefront of the convergence of the supply chain and cybersecurity, and his work continues to influence the strategies of federal entities and companies alike." Bob is a member of the Defense Science Board Cyber/Supply Chain Task Force. He also is Vice-Chair of the Cyber/Supply Chain Assurance Committee of the IT Alliance for Public Sector (ITAPS), a unit of the Information Technology Industry Council (ITIC), a prominent trade association.

Bob received his B.A. from Middlebury College and his J.D. from Georgetown University Law Center, where he was an Editor of the Georgetown Law Journal. He was a Research Fellow, Center for Science & International Affairs (now "Belfer Center"), Harvard Kennedy School of Government. Bob is a member of the International Institute for Strategic Studies (IISS), London. Academic publications on national security topics include articles in *International Security* and the *Journal of Strategic Studies*.