

ICT Supply Chain Assurance: *An IATAC State-of-the-Art Report*



IATAC

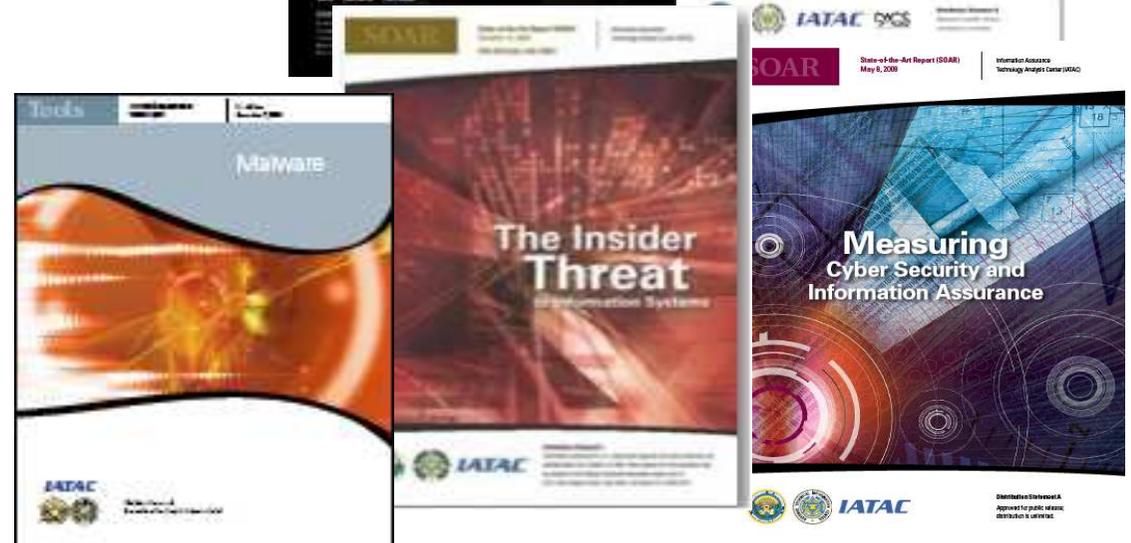


Karen Mercedes Goertzel, CISSP
Booz Allen Hamilton
goertzel_karen@bah.com
703.698.7454

This Presentation: Distribution Statement A - Approved for public release; distribution is unlimited.

IATAC: Proven track record in studying the “hard problems” of cyber security and information assurance (IA)

- Investigate cyber security and information assurance hard problems and groundbreaking developments
 - Depict the problem space
 - Capture breadth and depth of solution landscape
 - Characterize research gaps
- Current state-of-the-art report (SOAR) team includes lead authors of four prior SOARs, and an IA Tools Report:
 - 2005: *DoD IA/Computer Network Defense Common Needs and Capability Gaps*
 - 2007: *Software Security Assurance*
 - 2008: *Insider Threat to Information Systems*
 - 2009: *Measuring Cyber Security and IA*
 - 2009: *Malware* (IA Tools Report)
- Total distribution > 675,000 (and growing!)



2010: ICT Supply Chain Assurance SOAR

- ▶ Defense Technical Information Center (DTIC) tasked its Information Assurance Technology Analysis Center (IATAC) to develop SOAR on information technology (IT) supply chain security
- ▶ Preliminary research/discussions made it clear:
 - Scope needs to expand to include communications technology (IT → ICT)
 - Focus needs to be Supply Chain Assurance
 - “Supply Chain Security”: strong cargo/freight security connotations
 - “Supply Chain Risk Management”: understood to focus on *business* not *security* risk
- ▶ SOAR authors: IATAC system/software assurance subject matter experts (SMEs)
 - Contributions from general supply chain security SMEs
 - Oversight by Office of Director, Defense Research and Engineering (Dr. Steven King), as with previous four SOARs
 - Guidance from Department of Defense Globalization Task Force

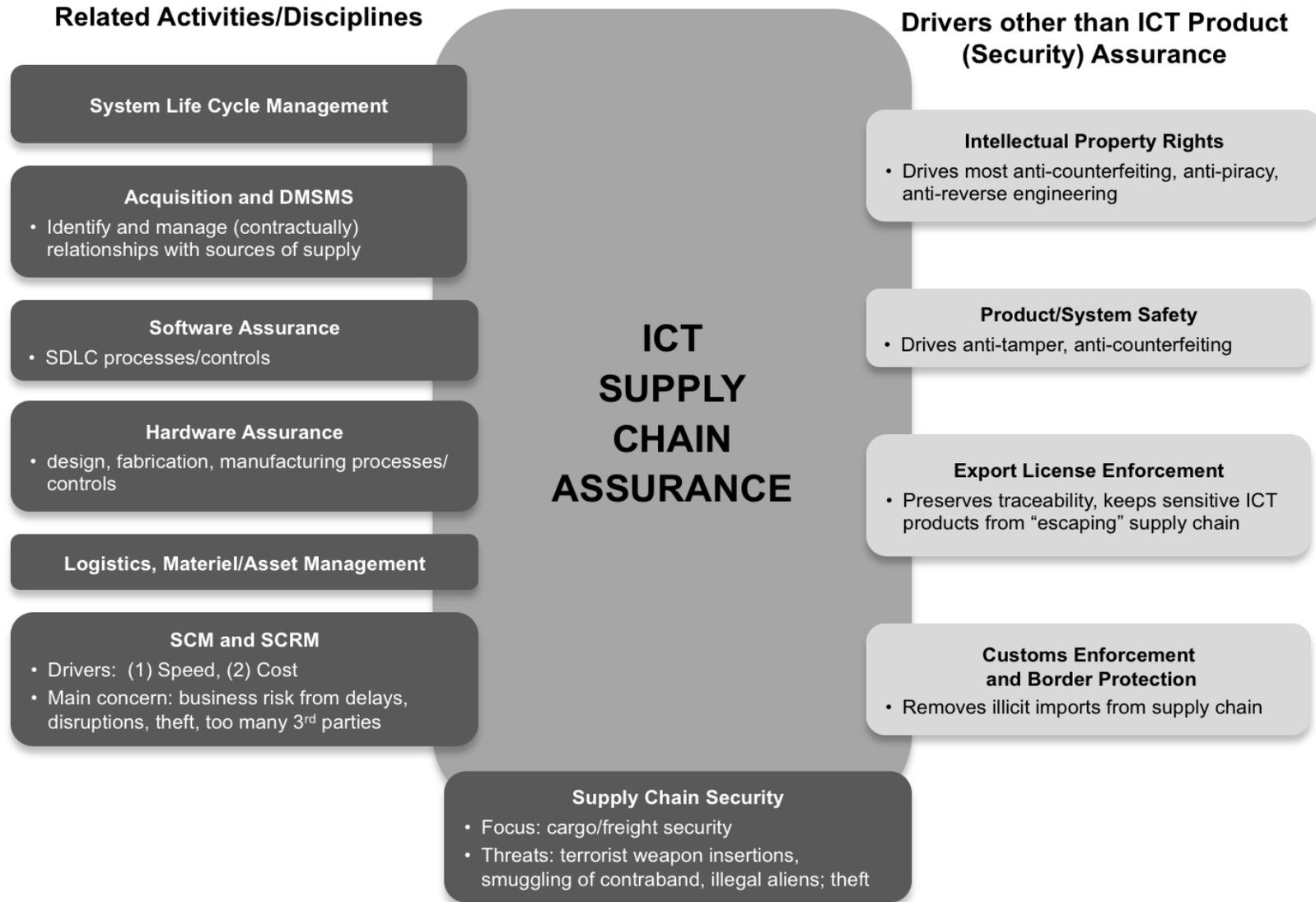
ICT Supply Chain Assurance Scoping the Subject

ASSURANCE



ICT Supply Chain Assurance

Scoping the Subject, *cont'd*



SOAR content

▶ Background

- Defense Science Board and Government Accountability Office Reports
- Dueling definitions: What exactly is a “supply chain”?
- Prerequisites to supply chain assurance
 - quality of supply chain processes
 - software and hardware assurance

▶ Problem Space

- *Threats*
 - to the supply chain itself: threats of disruption
 - from the supply chain to products within it: threats to integrity, trustworthiness, authenticity, availability
- *Vulnerabilities*
 - in the physical supply chain for hardware and software
 - in the electronic supply chain for software

SOAR content, *cont'd*

▶ Solution Space

- *Countermeasures to threats*
 - during acquisition (supplier assurance, acquisition security)
 - during product development and maintenance (software and hardware assurance)
 - before and during distribution and delivery (trusted distribution)
- *Mitigations for vulnerabilities*
 - inadequate supply chain risk management = untrustworthy products
 - security engineering for system assurance
 - assessing risk posed by use of untrustworthy ICT products
 - architectural and reengineering approaches to mitigate risk

SOAR content, *cont'd*

▶ The Supply Chain Assurance Landscape

▪ *Public sector initiatives*

- U.S., international, non-U.S. government activities
- Standards
- Legislation and regulation

▪ *Private sector initiatives*

- U.S., international, non-U.S trade association activities
- Industry standards (mostly anti-counterfeiting)
- Academic education in ICT supply chain assurance

▪ *Science and Technology Research Landscape*

- Research programs (e.g., DARPA TRUST in Integrated Circuits, IARPA STONESOUP)
- Research project matrix (with sponsors identified)

▶ Findings, Observations, Conclusions

SOAR content, *cont'd*

► Appendices

- Compendium of research projects
- DOD Acquisition Security: Critical Program Information protection and Program Protection Planning
- Export controls to prevent sensitive ICT from “escaping” controlled supply chains
- How malicious logic gets into software
- Assuring the "IT-as-a-Service" supply chain: considerations when acquiring public Cloud Infrastructure/Platform/Software/Data-as-a-Service
- IPR enforcement efforts that benefit ICT supply chain assurance

SOAR Schedule

- ▶ Sept. 2009: Work began
- ▶ Oct. 2010: Detailed outline approved
- ▶ 31 Jan. 2010: First draft completed, internal review
- ▶ 28 Feb. 2010: Completion of final draft for invited public comment (2-19 Mar. 2010)
- ▶ 1 Apr. 2010: Final content submitted for editing, graphics, design, layout
- ▶ Jun. 2010: Distribution code/caveat decision, PDF generated, sent to print shop
- ▶ 27 June 2010: SOAR published

Classification and distribution caveats for the SOAR have not yet been determined.

Questions?

