Information Technology Supply Chain Challenges

7th NASA Supply Chain Quality Assurance Conference

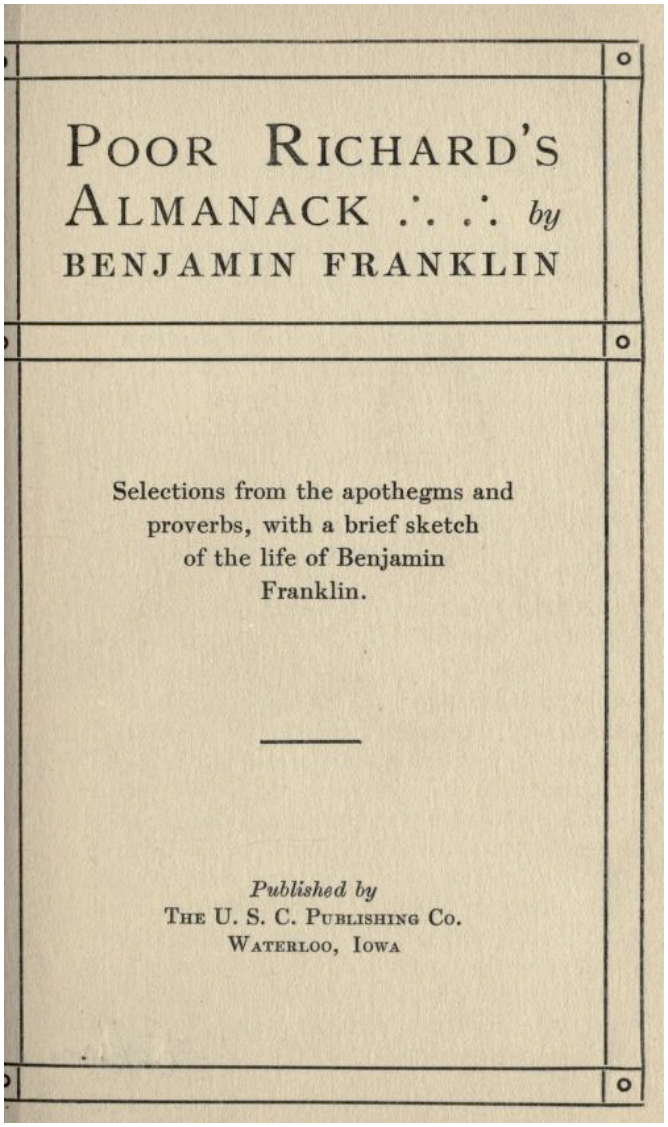
October 22, 2014

Overview

- NASA Enterprise IT Context
- Federal Drivers
- Moving To An Integrated Approach

NASA ENTERPRISE IT CONTEXT

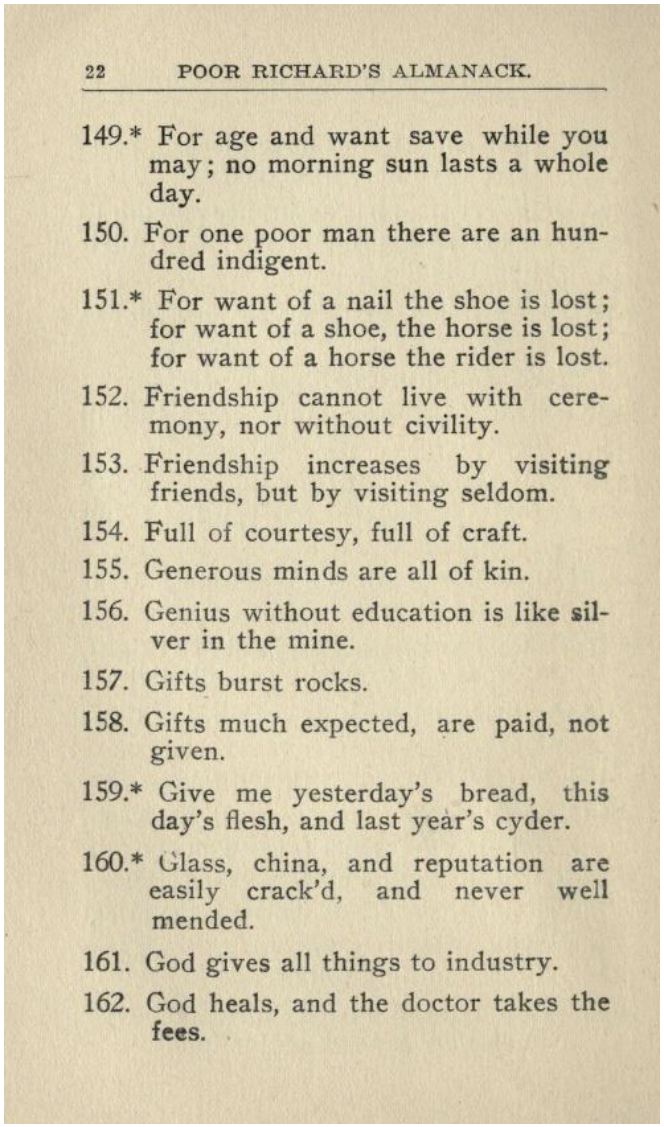
Historical Supply Chain Risk Management (SCRM)



POOR RICHARD'S ALMANACK ∴ ∴ *by* BENJAMIN FRANKLIN

Selections from the apothegms and proverbs, with a brief sketch of the life of Benjamin Franklin.

Published by
THE U. S. C. PUBLISHING CO.
WATERLOO, IOWA



149.* For age and want save while you may; no morning sun lasts a whole day.

150. For one poor man there are an hundred indigent.

151.* For want of a nail the shoe is lost; for want of a shoe, the horse is lost; for want of a horse the rider is lost.

152. Friendship cannot live with ceremony, nor without civility.

153. Friendship increases by visiting friends, but by visiting seldom.

154. Full of courtesy, full of craft.

155. Generous minds are all of kin.

156. Genius without education is like silver in the mine.

157. Gifts burst rocks.

158. Gifts much expected, are paid, not given.

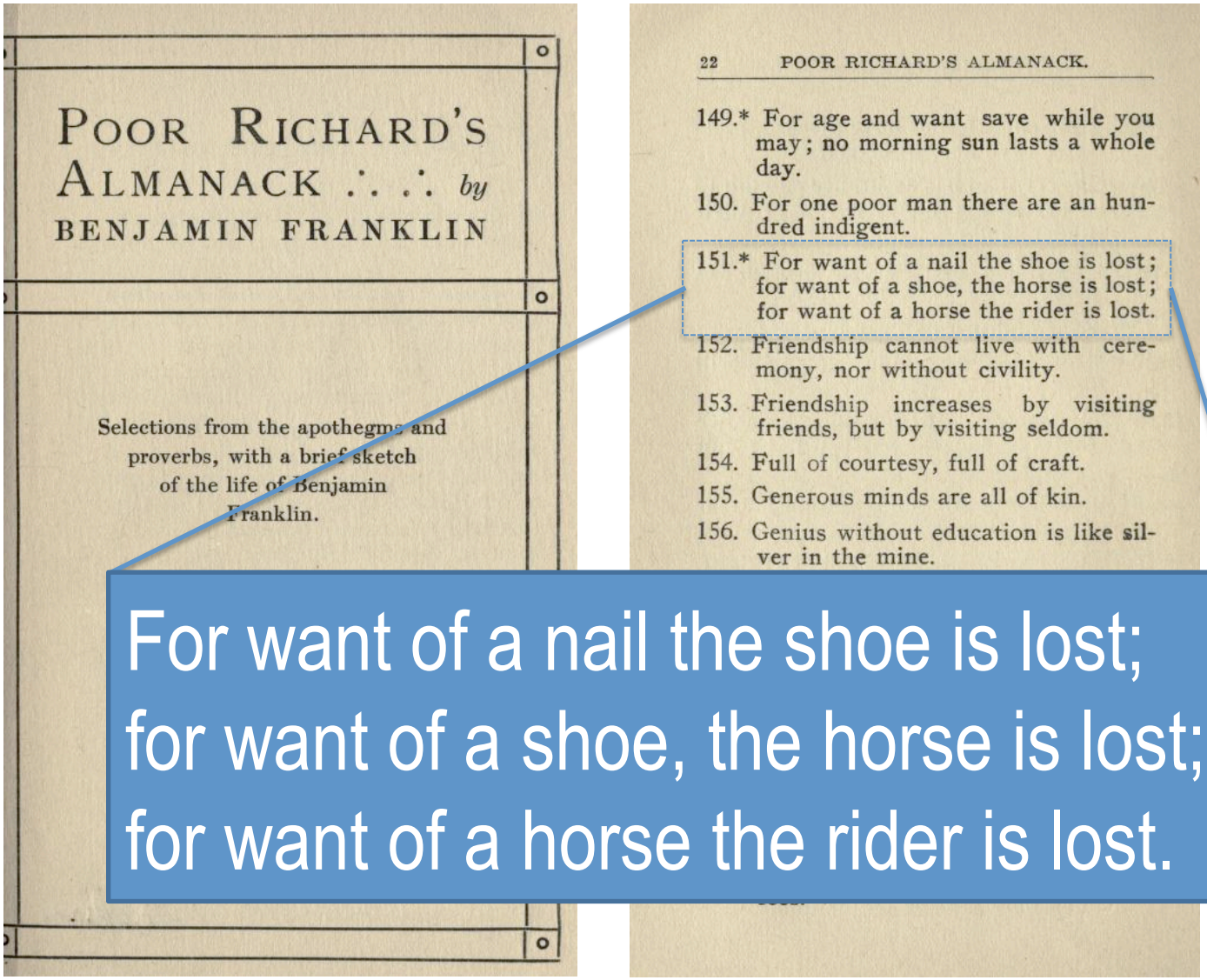
159.* Give me yesterday's bread, this day's flesh, and last year's cyder.

160.* Glass, china, and reputation are easily crack'd, and never well mended.

161. God gives all things to industry.

162. God heals, and the doctor takes the fees.

Historical SCRM



POOR RICHARD'S ALMANACK ∴ ∴ *by* BENJAMIN FRANKLIN

Selections from the apothegms and proverbs, with a brief sketch of the life of Benjamin Franklin.

22 POOR RICHARD'S ALMANACK.

149.* For age and want save while you may; no morning sun lasts a whole day.

150. For one poor man there are an hundred indigent.

151.* For want of a nail the shoe is lost; for want of a shoe, the horse is lost; for want of a horse the rider is lost.

152. Friendship cannot live with ceremony, nor without civility.

153. Friendship increases by visiting friends, but by visiting seldom.

154. Full of courtesy, full of craft.

155. Generous minds are all of kin.

156. Genius without education is like silver in the mine.

For want of a nail the shoe is lost;
for want of a shoe, the horse is lost;
for want of a horse the rider is lost.

NASA Vision, Mission and Principles

2014 NASA Strategic Plan

Goal 1. Expand the frontiers of knowledge, capability and opportunity in space

Goal 2. Advance understanding of Earth and develop technologies to improve the quality of life on our home planet

Goal 3. Serve the American public and accomplish our Mission by effectively managing our people, technical capabilities, and infrastructure

NASA's Objective 3.3:
Provide secure, effective, and affordable information technologies and services that enable NASA's mission.

2014 NASA Information Resources Management (IRM) Strategic Plan

NASA IT Vision
We enable the mission and move with purposeful intent towards improving IT services at NASA.

NASA IT Mission
Provide secure, effective and affordable information technologies and services that enable NASA's mission.

NASA IT Principles
Mission-Enabling. Purposeful. Responsive. Secure. Integrated. Cost-Effective.

NASA Chief Information Officer (CIO) Vision

- To clarify our purpose for existing at NASA. We should enable the mission and move with purposeful intent
- To be a value-added service
- To be customer focused
- To be connected to our many federal initiatives
- Protect our national assets
- Seek out efficiencies and reduce costs to Adopt IT that makes NASA better

NASA CIO Larry Sweet

NASA CIO Priorities

- Enhance NASA's information security posture through implementation of automated security and privacy tools and technologies
- Firm up NASA's policies and position on bring-your-own-device (BYOD) and the concept of Work from anywhere (WFA)
- Make better use of the Cloud
- Develop an IT program that adjusts to the challenging budget environment – moving towards more "services-on-demand"
- Improve IT governance
- Strengthen the NASA CIO Leadership Team

Executive and Legislative Branches

FEDERAL DRIVERS

2008: Comprehensive National Cybersecurity Initiative (NSPD-54/HSPD-23)

The Comprehensive National Cybersecurity Initiative

President Obama has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter. Shortly after taking office, the President therefore ordered a thorough review of federal efforts to defend the U.S. information and communications infrastructure and the development of a comprehensive approach to securing America's digital infrastructure.

In May 2009, the President accepted the recommendations of the resulting Cyberspace Policy Review, including the selection of an Executive Branch Cybersecurity Coordinator who will have regular access to the President. The Executive Branch was also directed to work closely with all key players in U.S. cybersecurity, including state and local governments and the private sector, to ensure an organized and unified response to future cyber incidents; strengthen public/private partnerships to find technology solutions that ensure U.S. security and prosperity; invest in the cutting-edge research and development necessary for the innovation and discovery to meet the digital challenges of our time; and begin a campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms and begin to build the digital workforce of the 21st century. Finally, the President directed that these activities be conducted in a way that is consistent with ensuring the privacy rights and civil liberties guaranteed in the Constitution and cherished by all Americans.

The activities under way to implement the recommendations of the Cyberspace Policy Review build on the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) in January 2008. President Obama determined that the CNCI and its associated activities should evolve to become key elements of a broader, updated national U.S. cybersecurity strategy. These CNCI initiatives will play a key role in supporting the achievement of many of the key recommendations of President Obama's Cyberspace Policy Review.

The CNCI consists of a number of mutually reinforcing initiatives with the following major goals designed to help secure the United States in cyberspace:

- **To establish a front line of defense against today's immediate threats** by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal Government—and ultimately with state, local, and tribal governments and private sector partners—and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions.
- **To defend against the full spectrum of threats** by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies.

* 1 *

- **Initiative #11. Develop a multi-pronged approach for global supply chain risk management.**
  - Globalization of the commercial information and communications technology marketplace provides increased opportunities for those intent on harming the United States by penetrating the supply chain to gain unauthorized access to data, alter data, or interrupt communications. **Risks** stemming from both the domestic and globalized supply chain must be **managed in a strategic and comprehensive way over the entire lifecycle** of products, systems and services. Managing this risk will require a greater **awareness of the threats, vulnerabilities, and consequences** associated with acquisition decisions; the development and employment of tools and resources to technically and operationally mitigate risk across the lifecycle of products (from design through retirement); the development of new acquisition policies and practices that reflect the complex global marketplace; and **partnership with industry** to develop and adopt supply chain and risk management standards and best practices. This initiative will enhance Federal Government skills, policies, and processes to provide departments and agencies with a robust toolset to better manage and mitigate supply chain risk at levels commensurate with the criticality of, and risks to, their systems and networks.

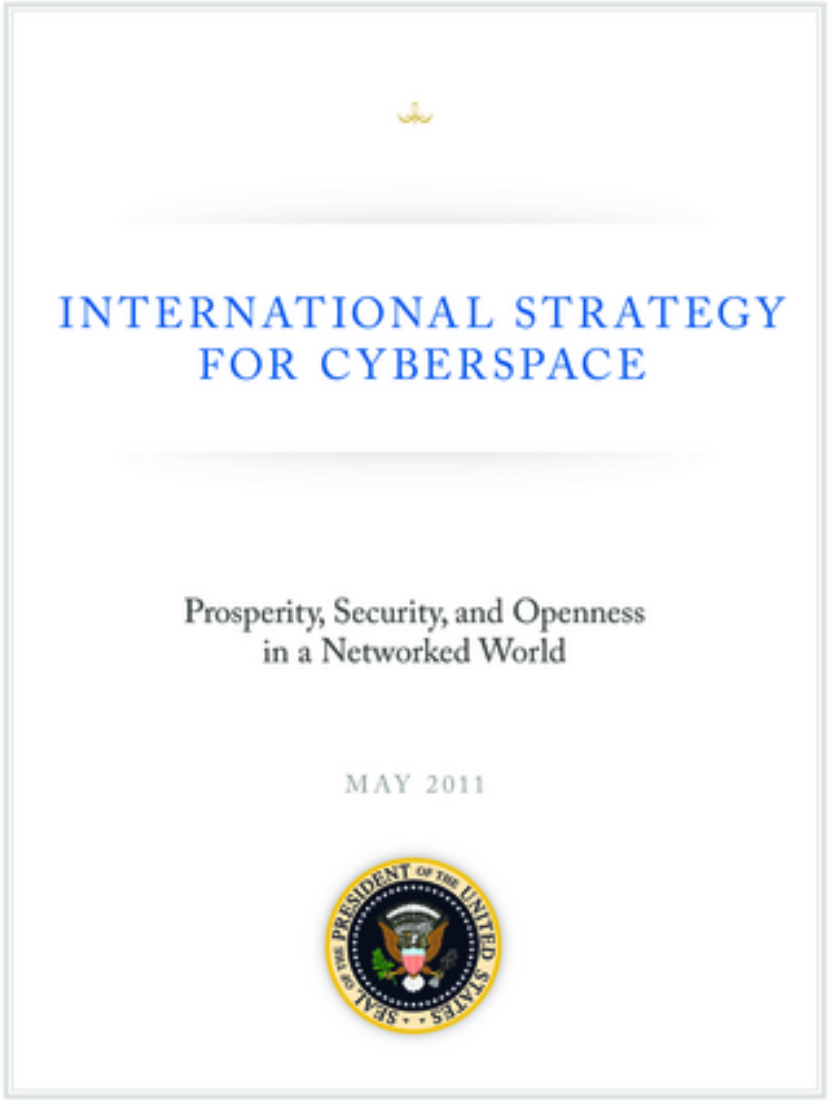
http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

2010: National Space Policy

- **Assurance and Resilience of Mission-Essential Functions**
  - The United States shall:
    - Assure space-enabled mission-essential functions by developing the techniques, measures, relationships, and capabilities necessary to maintain continuity of services;
      - Such efforts may include enhancing the protection and resilience of selected spacecraft and supporting infrastructure;
    - Develop and exercise capabilities and plans for operating in and through a degraded, disrupted, or denied space environment for the purposes of maintaining mission-essential functions; and
    - **Address mission assurance requirements and space system resilience** in the acquisition of future **space capabilities and supporting infrastructure**.

http://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf

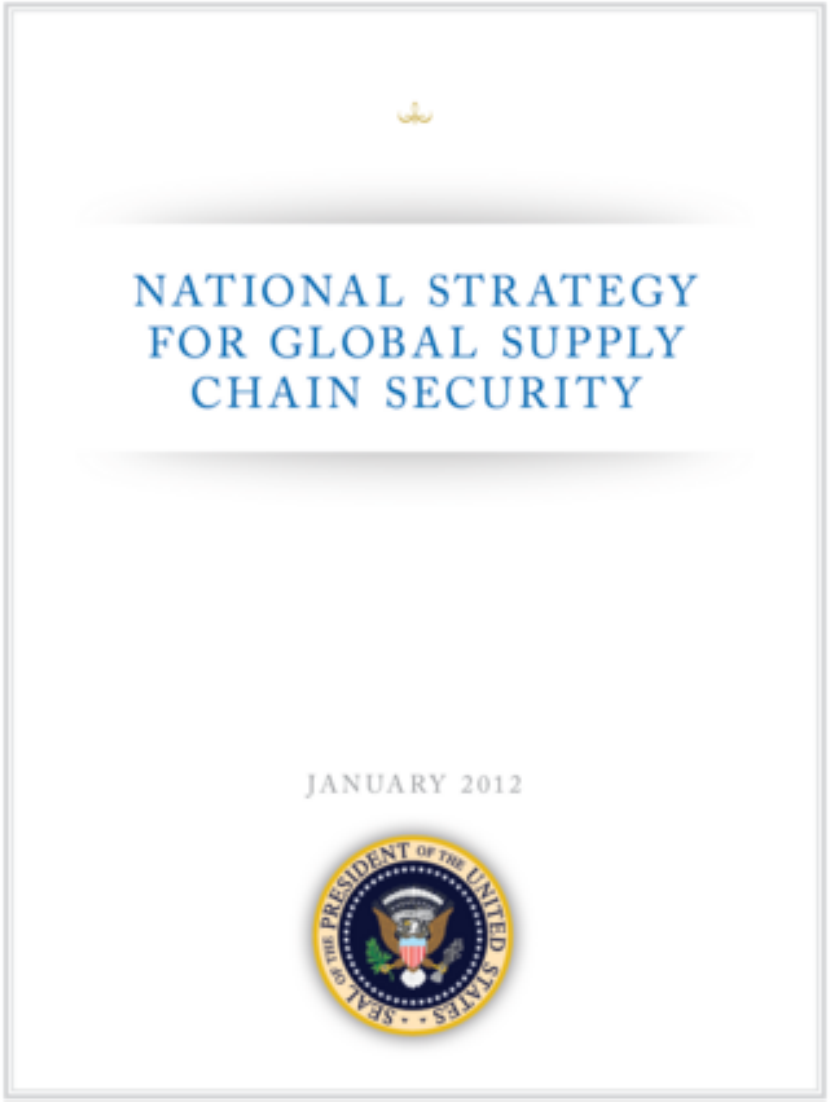
2011: International Strategy for Cyberspace



- **Improve the security of the high-tech supply chain, in consultation with industry.**
  - The operation of critical networks and information infrastructures depends on the assured availability of trustworthy hardware and software. Vulnerabilities in the supply chain can enable attacks on the integrity, availability, or confidentiality of networks and the data they contain. Exploitation of these vulnerabilities impairs economic performance and national security. The United States will work with industry and international partners to **develop best practices** for **protecting the integrity of information systems and critical infrastructure**. In this way, we will greatly enhance the security of the globalized supply chains on which free and open trade depend.

http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

2012: National Strategy for Global Supply Chain Security



- **Goal 2: Foster a Resilient Supply Chain:**
  - Integrated supply chains are fast and cost-efficient but also susceptible to shocks that can rapidly escalate from localized events into broader disruptions. We will seek to develop a global supply chain system that is prepared for and can withstand evolving threats and hazards and can recover rapidly from disruptions Increased resilience and flexible, dynamic capabilities will improve the Nation's ability to absorb shocks, save lives, and reduce the overall impact of a disruption. To accomplish our goal, the United States Government will seek to:
    - **Mitigate systemic vulnerability** to a supply chain disruption prior to a potential event by **using risk management principles** to identify and protect key assets, infrastructure, and support systems; and promoting the implementation of sustainable operational processes and appropriate redundancy for those assets
    - Promote trade resumption policies and practices that will provide for a coordinated restoration of the movement of goods following a potential disruption by developing and implementing national and global guidelines, standards, policies, and programs.

http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf

2013/2014: Legislative Branch Drivers

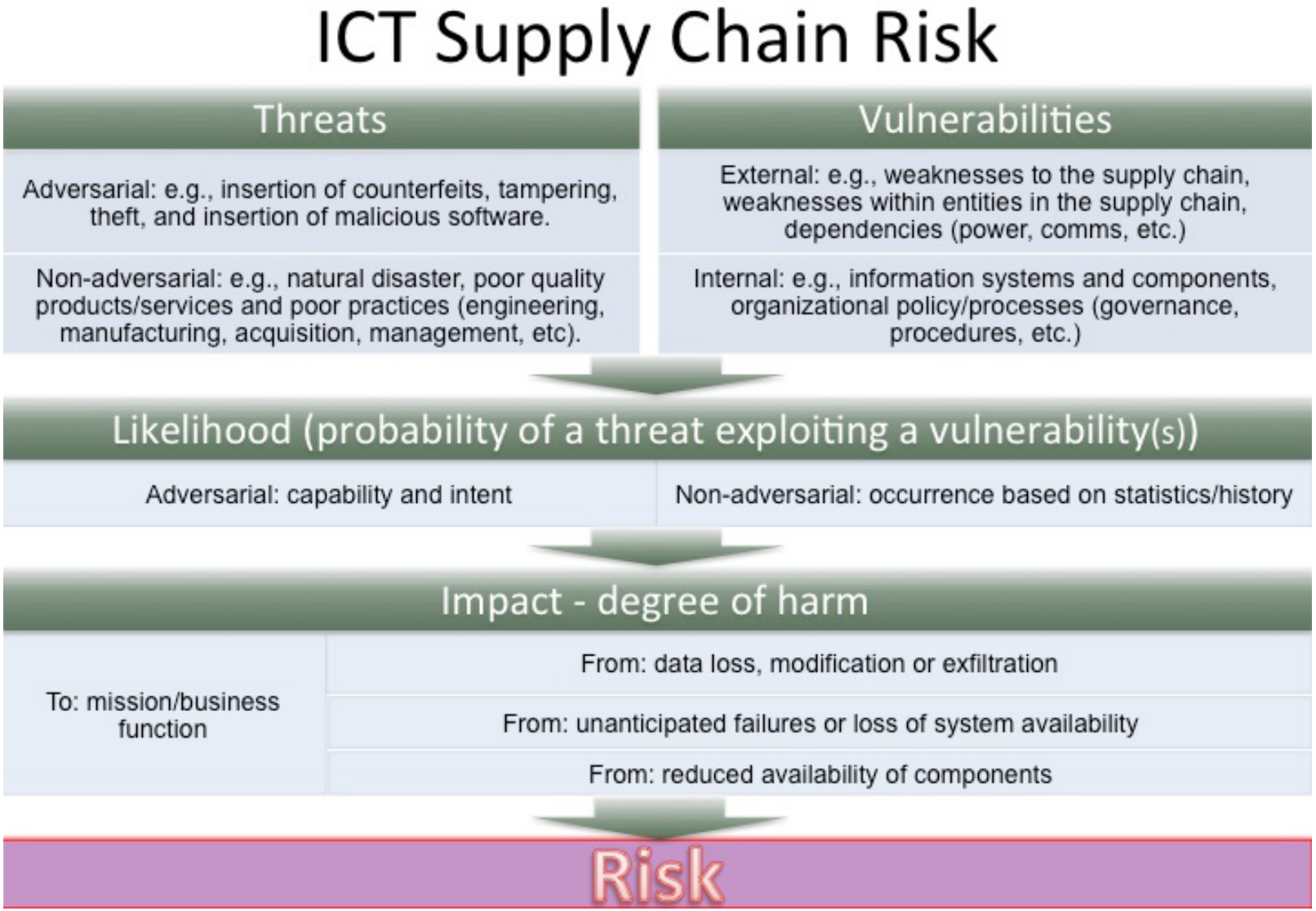
FY2013	FY2014

Section 516 Enacted 2013-03-26
• All information systems
• Assess risk of cyber-espionage or sabotage
• Consult with the FBI
• Peoples Republic of China (PRC) language
  • "produced, manufactured, or assembled"
  • "owned, directed, or subsidized" by the PRC
• National interest declaration
  • With report to the Congress
	Section 515 Enacted 2014-01-07
	• **FIPS199 High & Moderate systems**
	• Assess risk of cyber-espionage or sabotage
	• **Use NIST supply chain criteria**
	• Consult with FBI
	  • **and appropriate agencies**
	• **Any entity posing cyber threat** to the USG
	  • "produced, manufactured, or assembled by **one or more entities**…"
	  • "**including but not limited to**, owned, directed, or subsidized by the PRC"
	• National interest declaration
	  • With report to the Congress
	  • **With mitigation strategy**

NASA Procurement Information Circulars (PICs) applied to contracts:
PIC 13-04: http://www.hq.nasa.gov/office/procurement/regs/pic13-04.html (2013-06-06)
PIC 14-03: http://www.hq.nasa.gov/office/procurement/regs/PIC%2014-03.pdf (2014-04-16)

Supply Chain Risk Management Practices for Federal Information Systems and Organizations

NIST SP800-161 (2nd draft) http://csrc.nist.gov/publications/drafts/800-161/sp800_161_2nd_draft.pdf



MOVING TO AN INTEGRATED APPROACH

Changes in Threats

Undirected or Environmental Threats	Directed or Adversarial Threats
Component Unavailable	Market consolidation (supply denial)
Counterfeit component	Replaced, subverted, components
Sub-standard component	Deliberate production flaws
Infected media, information transfer, processor	Entry point to the enterprise, breach of confidentiality
Latent defect (vulnerability)	Engineered vulnerabilities
Operating environment impacts	Engineered impacts from environmental factors
Failure-intolerant systems	Targeted multi-capability (e.g., cyber-physical) attack on a weakpoint
Outsourced/external service providers	Entry point to the enterprise, insider threats

Modern risk management involves the realization that adaptive human adversaries represent an unconstrained threat source.

Information Security Challenge Areas

- **Engineering disciplines' overlap with IT and the security mindset**
  - Information System Security Engineers: include (early and often) in the system lifecycle – as part of a robust system engineering team
  - Software engineering: extend software assurance efforts with software security assurance
  - System architecture: appropriately de-compose the system and "bake security in", generally moving to a loosely coupled design model designed for resiliency – need the ability to rapidly upgrade system components
  - System operations: significantly reduce "time-to-change" for an identified vulnerability from days/weeks to hours, routinely re-assess existing security preparedness
- **Risk tolerance and resiliency improvements**
  - Migrate from "no change is less risk" to "failure to change is more risk"
  - Migrate from "no single point of failure" to "sustainable operations in spite of adversity"

Today's NASA SCRM

- **Building on excellent capabilities across the risk management, system engineering, and mission assurance disciplines, we have:**
  - Excellent knowledge of spacecraft and instrument component pipelines
  - Improving awareness of ground-side dependencies outside of core mission operations
  - Considerations regarding supply chain while modernizing our IT infrastructure
  - Linked supply chain context into the acquisition process
  - Started building our supply chain analysis capabilities, including partnerships with other Agencies
  - Started integrating supply chain risks into the existing risk management practice
- **The single most impactful practice for NASA is to inform the risk management and system engineering processes**
  - Supply chain risks to inform Likelihood and Consequence for risk decisions

What We Can Do Next

Government	Industry
• Define system impact levels (criticality) • Establish system boundaries and reuse sub-systems where appropriate • Improve integration of performance, security, and supply chain compliance requirements • Integrate SCRM into design and development practices • Conduct oversight, audits, and continual improvement assessments; require certifications? • Engage with industry partners, and share information about supply chain risks and experiences where permitted	• Increase modular architectures, clarify sub-system boundaries and dependencies • Map existing internal and business controls to assurance requirements • Integrate SCRM into design and development practices • Aid oversight, audits, and inform continual improvement assessments; acquire certifications? • Engage with Federal partners, and share information about supply chain experiences with appropriate data sensitivity

We're committed to effective Government and Industry collaboration to mutually assure our supply chains.

BACKUP INFORMATION

NASA PIC 13-04 (2013-06-06)

- **BACKGROUND: Section 516 of the Consolidated and Further Continuing Appropriations Act, 2013, Public Law 113-6, enacted March 26, 2013, provides:**
  - SEC. 516. (a) None of the funds appropriated or otherwise made available under this Act may be used by the Departments of Commerce and Justice, the National Aeronautics and Space Administration, or the National Science Foundation to acquire an information technology system unless the head of the entity involved, in consultation with the Federal Bureau of Investigation or other appropriate Federal entity, has made an assessment of any associated risk of cyber-espionage or sabotage associated with the acquisition of such system, including any risk associated with such system being produced, manufactured or assembled by one or more entities that are owned, directed or subsidized by the People's Republic of China.
  - (b) None of the funds appropriated or otherwise made available under this Act may be used to acquire an information technology system described in an assessment required by subsection (a) and produced, manufactured or assembled by one or more entities that are owned, directed or subsidized by the People's Republic of China unless the head of the assessing entity described in subsection (a) determines, and reports that determination to the Committees on Appropriations of the House of Representatives and the Senate, that the acquisition of such system is in the national interest of the United States.
- **http://www.hq.nasa.gov/office/procurement/regs/pic13-04.html**

NASA PIC 14-03 (2014-04-16) [1]

- **BACKGROUND: Section 515 of the Consolidated and Further Continuing Appropriations Act, 2014, Public Law 113-7, enacted January 7, 2014, provides:**
  - (a) None of the fund appropriated or otherwise made available under this Act may be used by the Departments of Commerce and Justice, the National Aeronautics and Space Administration, or the National Science Foundation to acquire a high-impact or moderate-impact information system, as defined for security categorization in the National Institute of Standards and Technology's (NIST) Federal Information Processing Standard Publication 199, "Standards for Security Categorization of Federal Information and Information Systems" unless the agency has –
    - (1) Reviewed the supply chain risk for the information systems against criteria developed by NIST to inform acquisitions decisions for high-impact and moderate-impact information systems within the Federal Government;
    - (2) Reviewed the supply chain risk from the presumptive awardee against available and relevant threat information provided by the Federal Bureau of Investigation and other appropriate agencies; and
    - (3) In consultation with the Federal Bureau of Investigation or other appropriate Federal entity, conducted an assessment of any risk of cyber-espionage or sabotage associated with the acquisition of such system, including any risk associated with such system being produced, manufactured, or assembled by one or more entities identified by the United States Government as posing a cyber threat, including but not limited to, those that may be owned, directed, or subsidized by the People's Republic of China.

NASA PIC 14-03 (2014-04-16) [2]

- **Section 515, continued:**
  - (b) None of the funds appropriated or otherwise made available under this Act may be used to acquire a high-impact or moderate impact information system reviewed and assessed under subsection (a) unless the head of the assessing entity described in subsection (a) has –
    - (1) Developed, in consultation with NIST and supply chain risk management experts, a mitigation strategy for any identified risks;
    - (2) Determined that the acquisition of such system is in the national interest of the United States; and
    - (3) Reported that determination to the Committees on Appropriations of the House of Representatives and the Senate.
- **http://www.hq.nasa.gov/office/procurement/regs/PIC%2014-03.pdf**

Related NIST Documents

- **Federal Information Processing Standards Publications (FIPS)**
  http://csrc.nist.gov/publications/PubsFIPS.html
  - FIPS 140: Security Requirements for Cryptographic Modules
  - FIPS 199: Standards for Security Categorization of Federal Information and Information Systems
  - FIPS 200: Minimum Security Requirements for Federal Information and Information Systems
- **Special Publications (SP)**
  http://csrc.nist.gov/publications/PubsSPs.html
  - SP 800-30: Guide for Conducting Risk Assessments
  - SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
  - SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations
  - SP 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories
  - SP 800-64: Security Considerations in the System Development Life Cycle
  - SP 800-161: **DRAFT** Supply Chain Risk Management Practices for Federal Information Systems and Organizations (*Second Draft*)

Related ISO Standards Series

- ISO 9000: Quality management systems
- ISO 25000: Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE)
  - Builds from ISOs 9126-1 and 14598-2
- ISO 27000: Information technology — Security techniques — Information security management systems
- ISO 28000: Specification for security management systems for the supply chain
- ISO 31000: Risk management — Principles and guidelines