UTILITIES TELECOM COUNCIL

ICT Supply Chain Risk Management

Nadya Bartol, CISSP, CGEIT
UTC Senior Cybersecurity Strategist

What is ICT Supply Chain Risk Management?

- Information and Communication Technology (ICT) products are assembled, built, and transported by geographically extensive supply chains of multiple suppliers
- Acquirer does not always know how that happens, even with the primary supplier
- Not all suppliers are ready to articulate their cybersecurity and cyber supply chain practices
- Abundant opportunities exist for malicious actors to tamper with and sabotage products, ultimately compromising system integrity, reliability, and safety

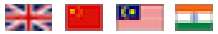
Acquirers need to be able

to understand and manage associated risks

Source: Nadya Bartol, ACSAC Case Study, December 2010

From *The World Is Flat by Thomas Friedman*

Dell Inspiron 600m Notebook: Key Components and Suppliers

Component		Supplier or Potential Suppliers
Intel Microprocessor		US-owned factory in the Philippines, Costa Rica, Malaysia, or China *(Intel)*
Memory		South Korea *(Samsung)*, Taiwan *(Nanya)*, Germany *(Infineon)*, or Japan *(Elpida)*
Graphics Card		China *(Foxconn)*, or Taiwanese-owned factory in China *(MSI)*
Cooling fan		Taiwan *(CCI and Auras)*
Motherboard		Taiwan *(Compal and Wistron)*, Taiwanese-owned factory in China *(Quanta)*, or South Korean-owned factory in China *(Samsung)*
Keyboard		Japanese company in China *(Alps)*, or Taiwanese-owned factory in China *(Sunrex and Darfon)*
LCD		South Korea *(Samsung, LG.Philips LCD)*, Japan *(Toshiba or Sharp)*, or Taiwan *(Chi Mei Optoelectronics, Hannstar Display, or AU Optronics)*
Wireless Card		Taiwan *(Askey or Gemtek)*, American-owned factory in China *(Agere)* or Malaysia *(Arrow)*, or Taiwanese-owned factory in China *(USI)*
Modem		China *(Foxconn)*, or Taiwanese company in China *(Asustek or Liteon)*
Battery		American-owned factory in Malaysia *(Motorola)*, Japanese company in Mexico, Malaysia, or China *(Sanyo)*, or South Korean or Taiwanese factory *(SDI and Simplo)*
Hard Disk Drive		American-owned factory in Singapore *(Seagate)*, Japanese-owned company in Thailand *(Hitachi or Fujitsu)*, or Japanese-owned company in the Philippines *(Toshiba)*
CD/DVD		South Korean company with factories in Indonesia and Philippines *(Samsung)*, Japanese-owned factory in China or Malaysia *(NEC)*, Japanese-owned factory in Indonesia, China, or Malaysia *(Teac)*, or Japanese-owned factory in China *(Sony)*
Notebook Carrying Bag		Irish company in China *(Tenba)*, or American company in China *(Targus, Samsonite, and Pacific Design)*
Power Adapter		Thailand *(Delta)*, or Taiwanese-, South Korean-, or American-owned factory in China *(Liteon, Samsung, and Mobility)*
Power Cord		British company with factories in China, Malaysia, and India *(Volex)*
Removable Memory Stick		Israel *(M-System)*, or American company with factory in Malaysia *(Smart Modular)*

Source: Booz Allen Hamilton and DoD

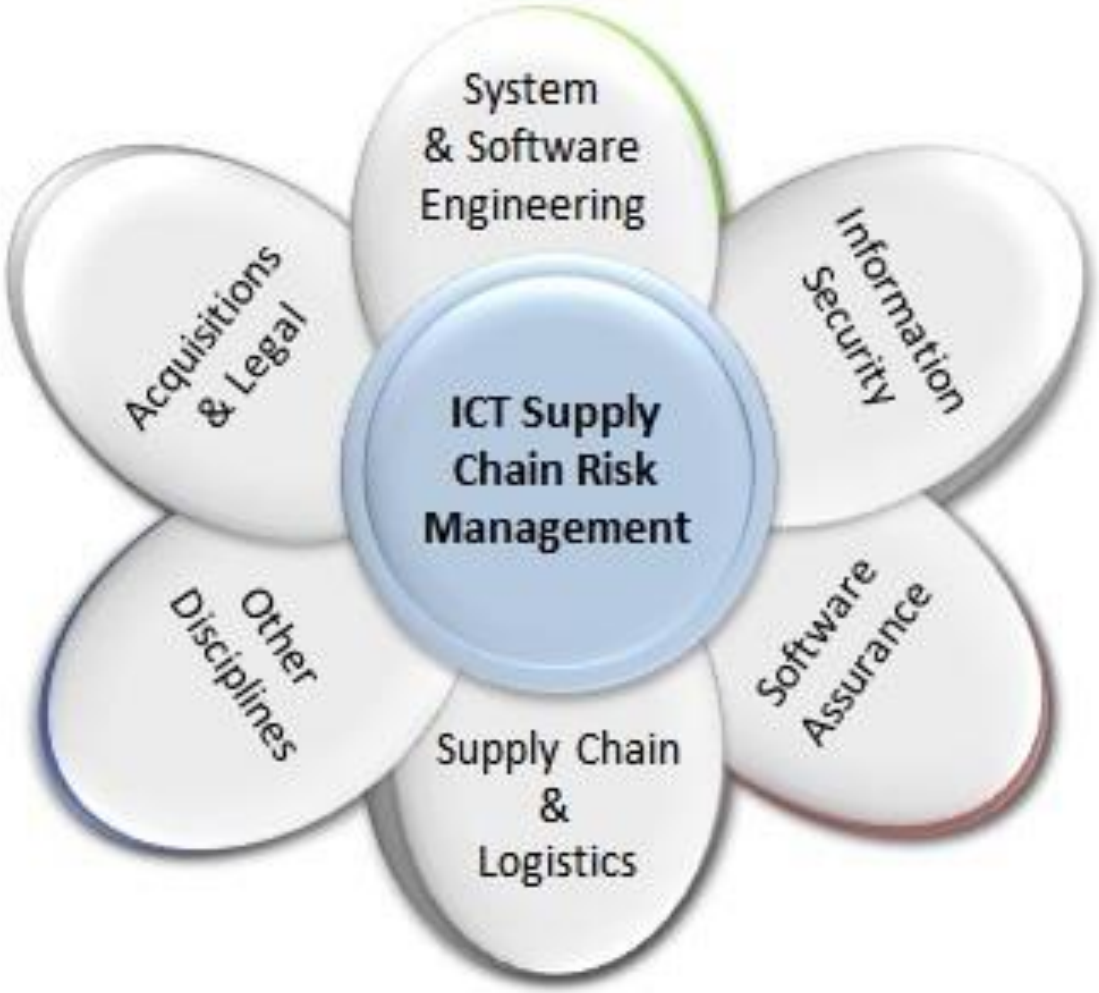
How is ICT SCRM Different from Traditional Supply Chain Risk Management

Traditional Supply Chain Risk Management	ICT SCRM
Will my physical product get to me on time?	Will my product (physical or logical) or get to me as it was shipped and as I ordered?
Is my supply chain resilient and will it continue delivering what I need in case of disaster?	Is my supply chain infiltrated by someone who is inserting extra features into my hardware and software to exploit my systems and get to my information now or later?
What is the risk ***TO*** my supply chain that delivers critical products and services that I need to mitigate?	What is the risk ***TO AND THROUGH*** my supply chain to my business and mission that I need to mitigate?

What are the risks?

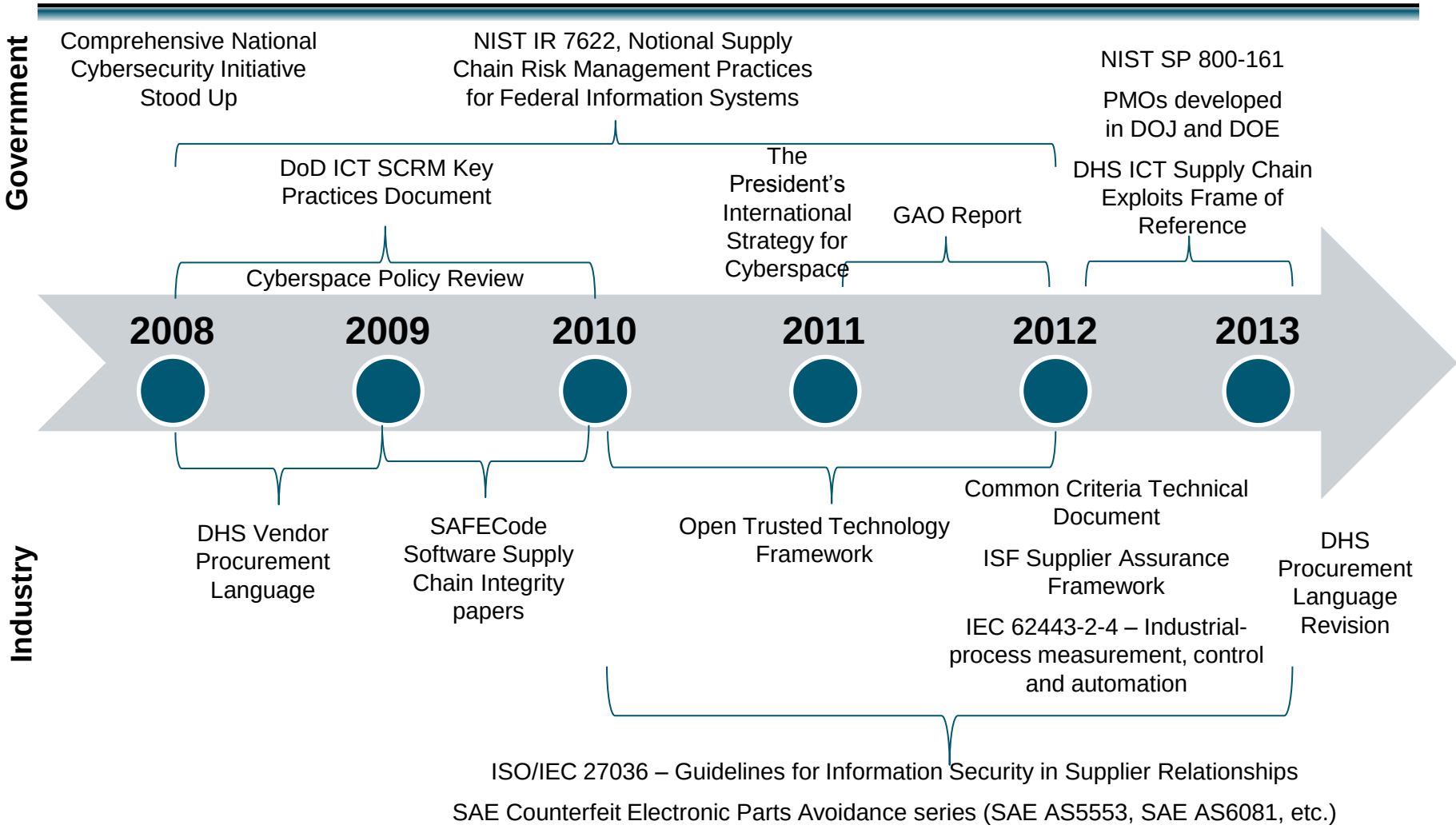
- Intentional insertion of malicious functionality
- Counterfeit electronics
- Poor practices upstream

Solutions Are Multidisciplinary

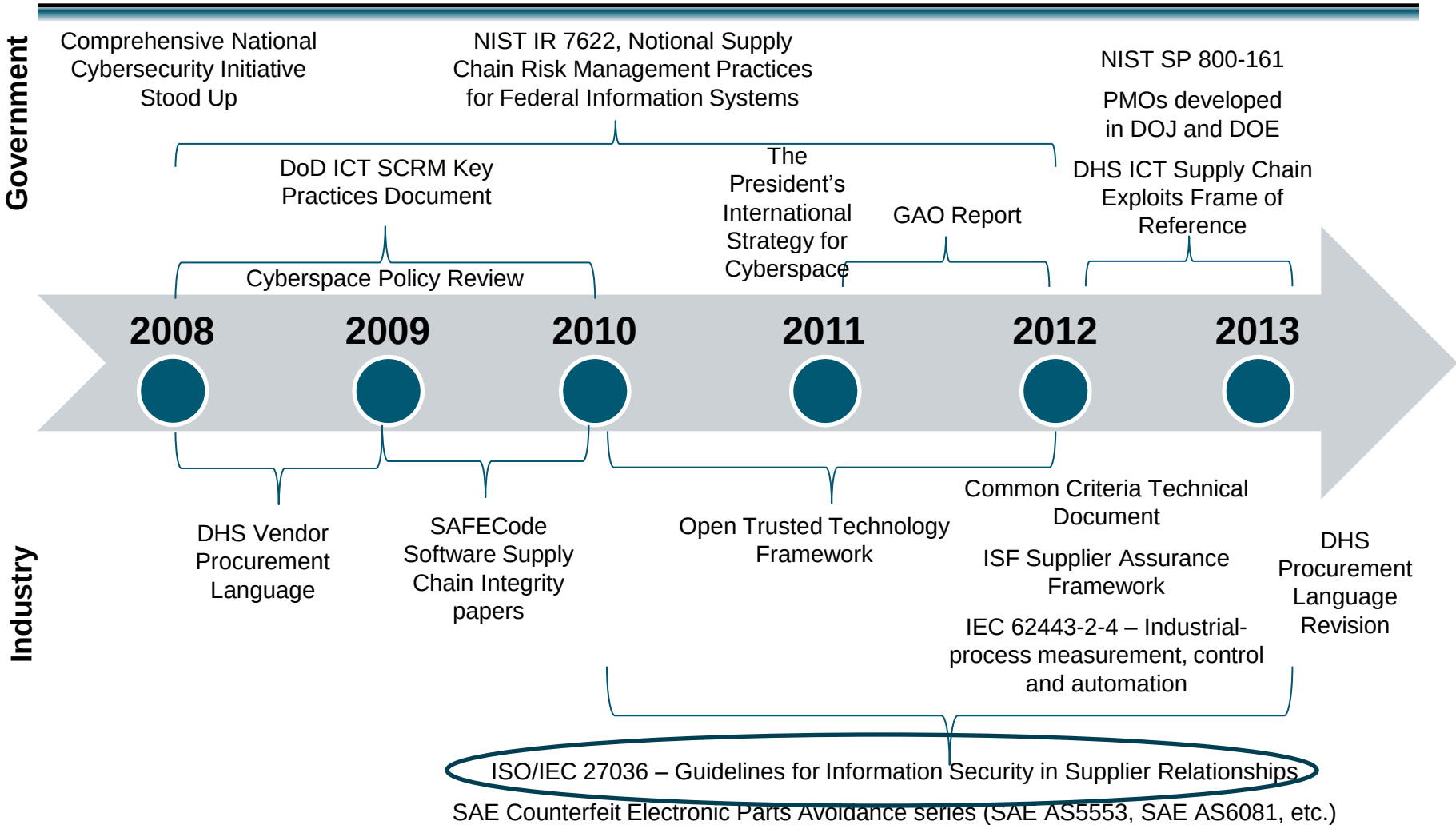


Source: NISTIR 7622

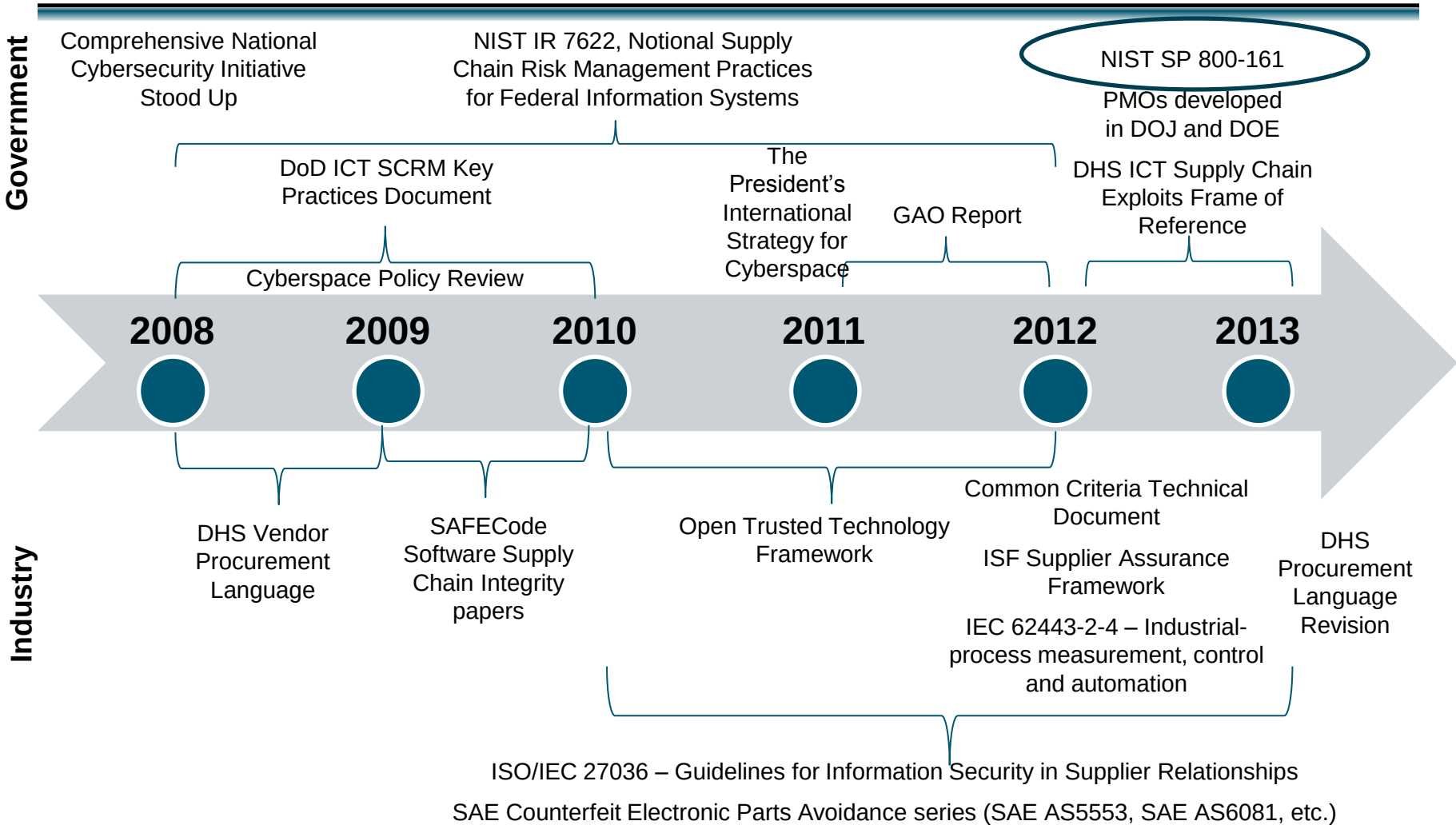
Existing and Emerging Practices



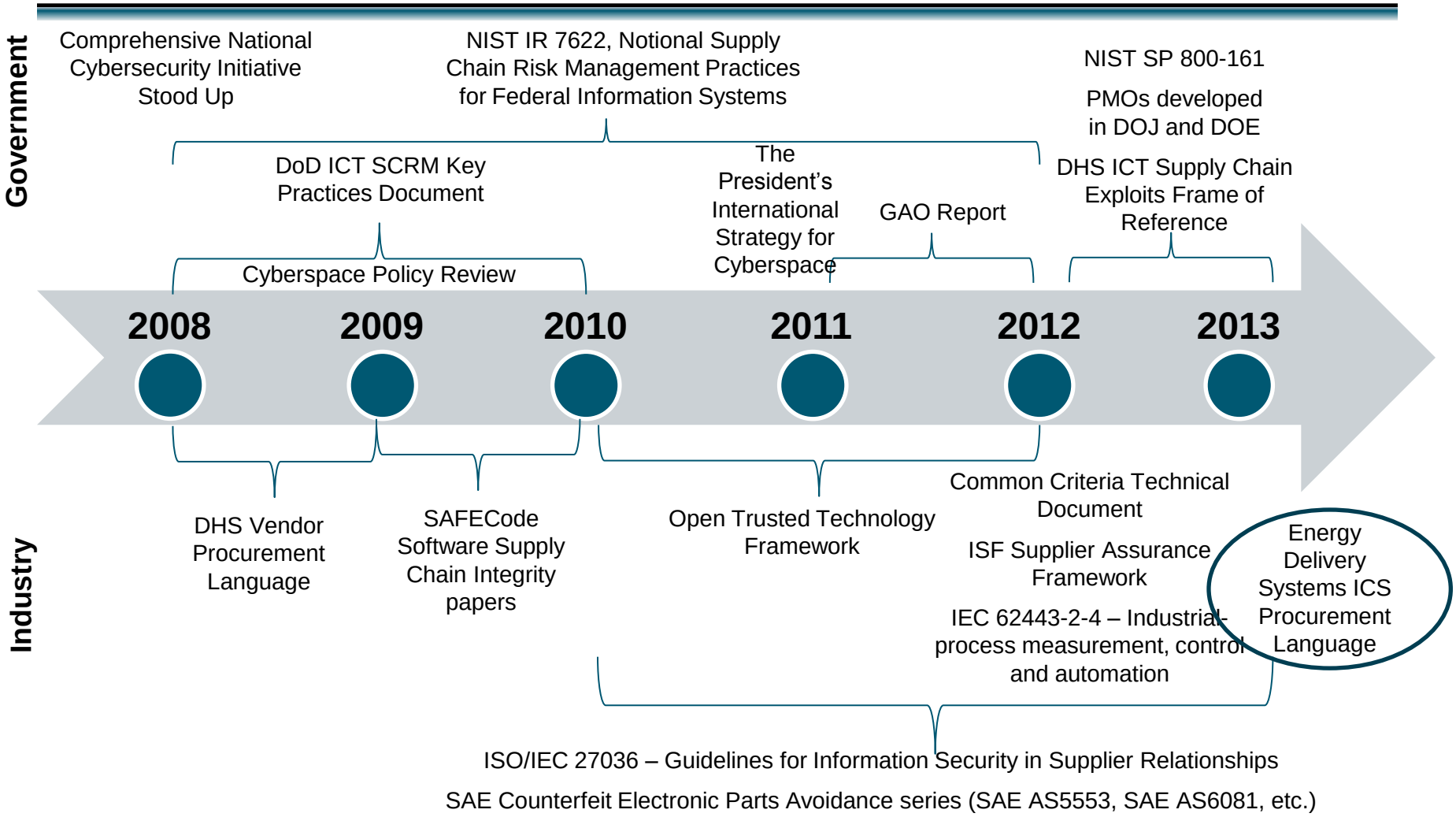
Existing and Emerging Practices



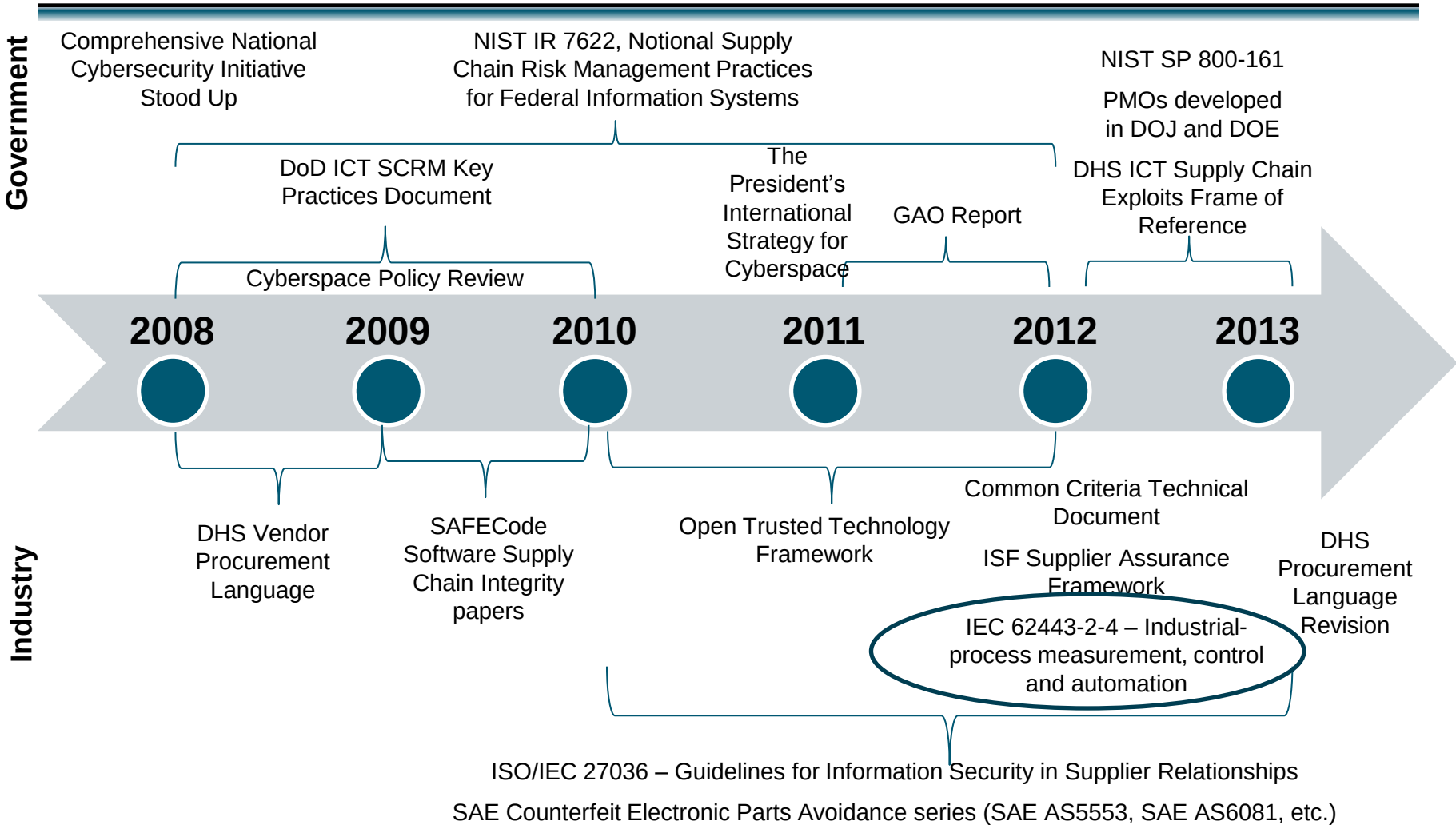
Existing and Emerging Practices



Existing and Emerging Practices



Existing and Emerging Practices



How do these standards help?

By answering the following key question:

- How should an organization manage security risks associated with acquiring ICT products and services?

AND

By providing a rich menu of items to chose from to

- Define your own processes for supplier management
- Ask your suppliers about their processes

In Summary

- The problem is real
- Practices are available to make things better
- Solutions come from multiple disciplines
- This is complex – start somewhere and improve

Contact Information

- Nadya Bartol
  nadya.bartol@utc.org