



FBI Criminal Investigation: Cisco Routers

The overall classification of this presentation is
UNCLASSIFIED

Section Chief Raul Roldan
Supervisory Special Agent Inez Miyamoto
Intelligence Analyst Tini Leon

January 11, 2008



Agenda

- FBI Criminal Investigation
- Supply Chain
- Critical Infrastructure Threats
- Government Procurement Problems
- FBI Coordination
- Intelligence Gap

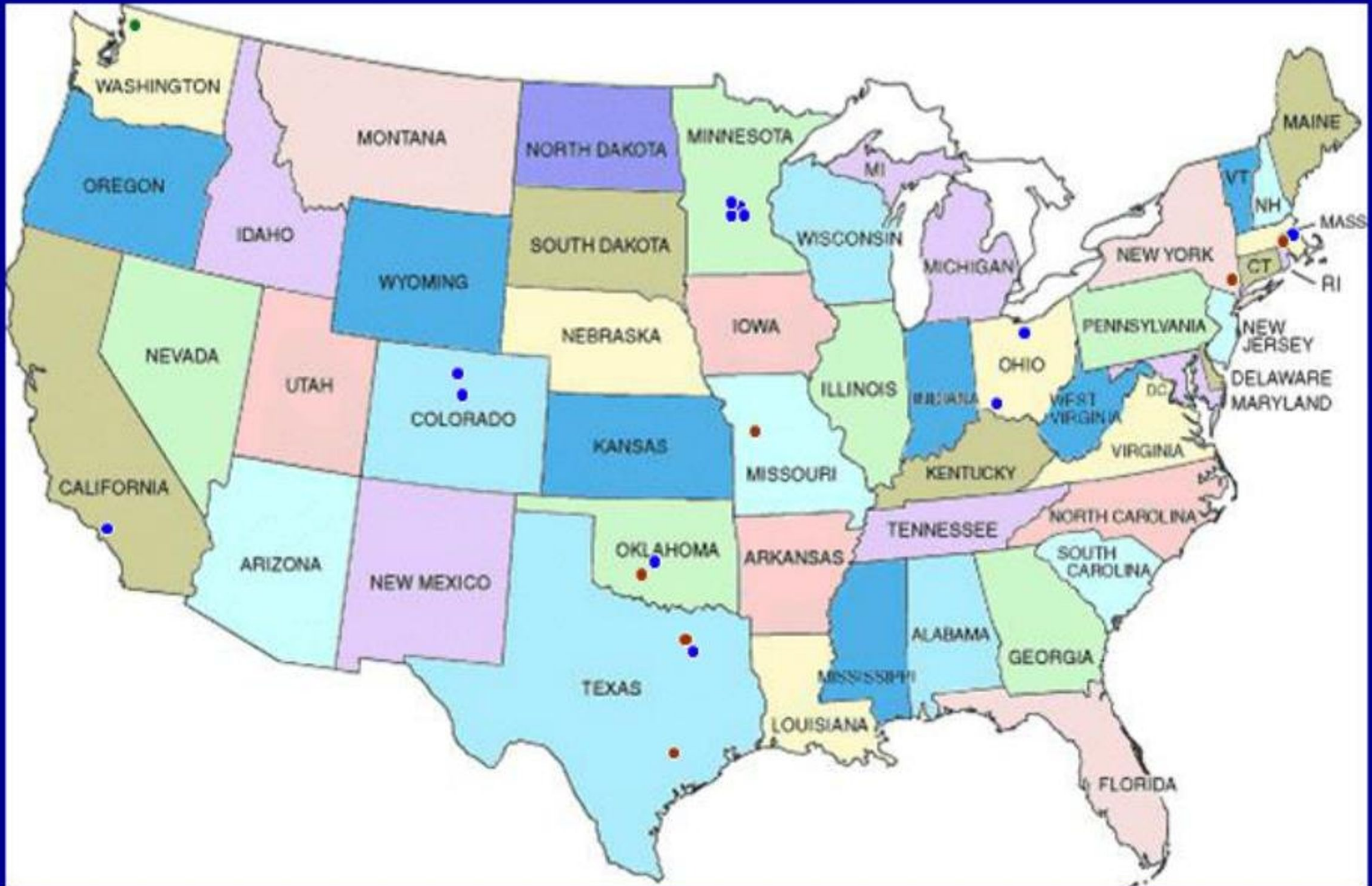


FBI Criminal Investigation

Cisco Routers



Nationwide Cases



Green – DCIS; Red – FBI joint cases; Blue – FBI

Search Warrants Executed





Counterfeit Equipment

- Routers
 - Models: 1000 and 2000 Series
- Switches
 - Models: WS-C2950-24, WS-X4418-GB (for CAT4000series)
- GigaBit Interface Converter (GBIC)
 - Models: WS-G5483, WS-G5487
- WAN Interface Card (WIC)
 - Models: VWIC-1MFT-E1, VWIC-2MFT-G703, WIC-1DSU-T1-V2



Counterfeit Products



Cost Comparison Example



- Counterfeit
 - 1721 Router
 - \$234.00
- Genuine
 - 1721 Router
 - \$1,375.00

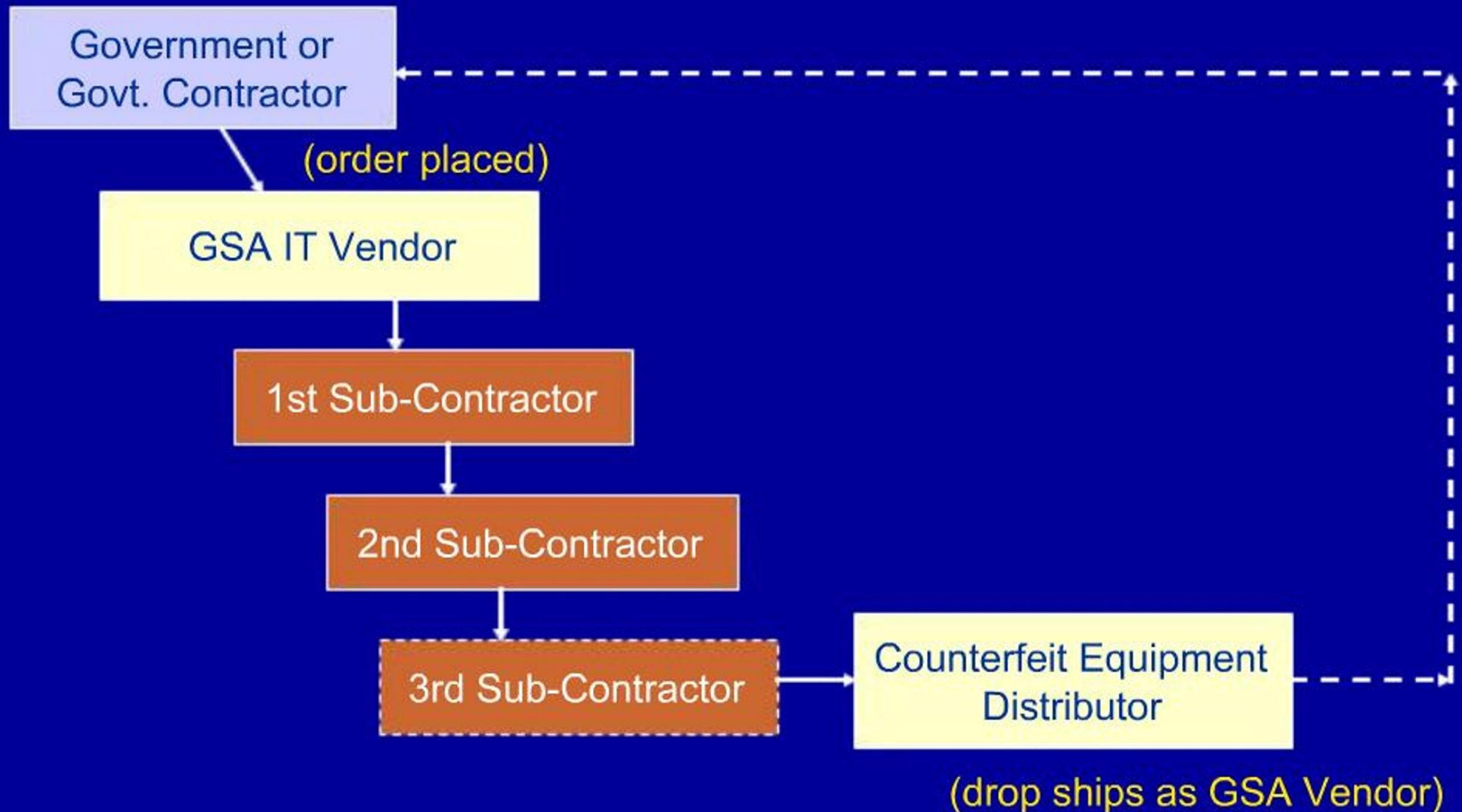


Cisco Identified Problems

- Problems
 - Low manufacturing standards
 - Higher failure rate
 - Duplicate MAC addresses of routers and switches can shut down an entire network
- Examples
 - In 2002, duplicate MAC addresses shut down an end user's network in Pittsburgh
 - In 2004, a government agency conducted a network upgrade to its North American weather communication system—it failed upon installation
 - Cisco 1721 router installed in a network caught fire due to a faulty power supply



Sub-Contracting Process





Supply Chain

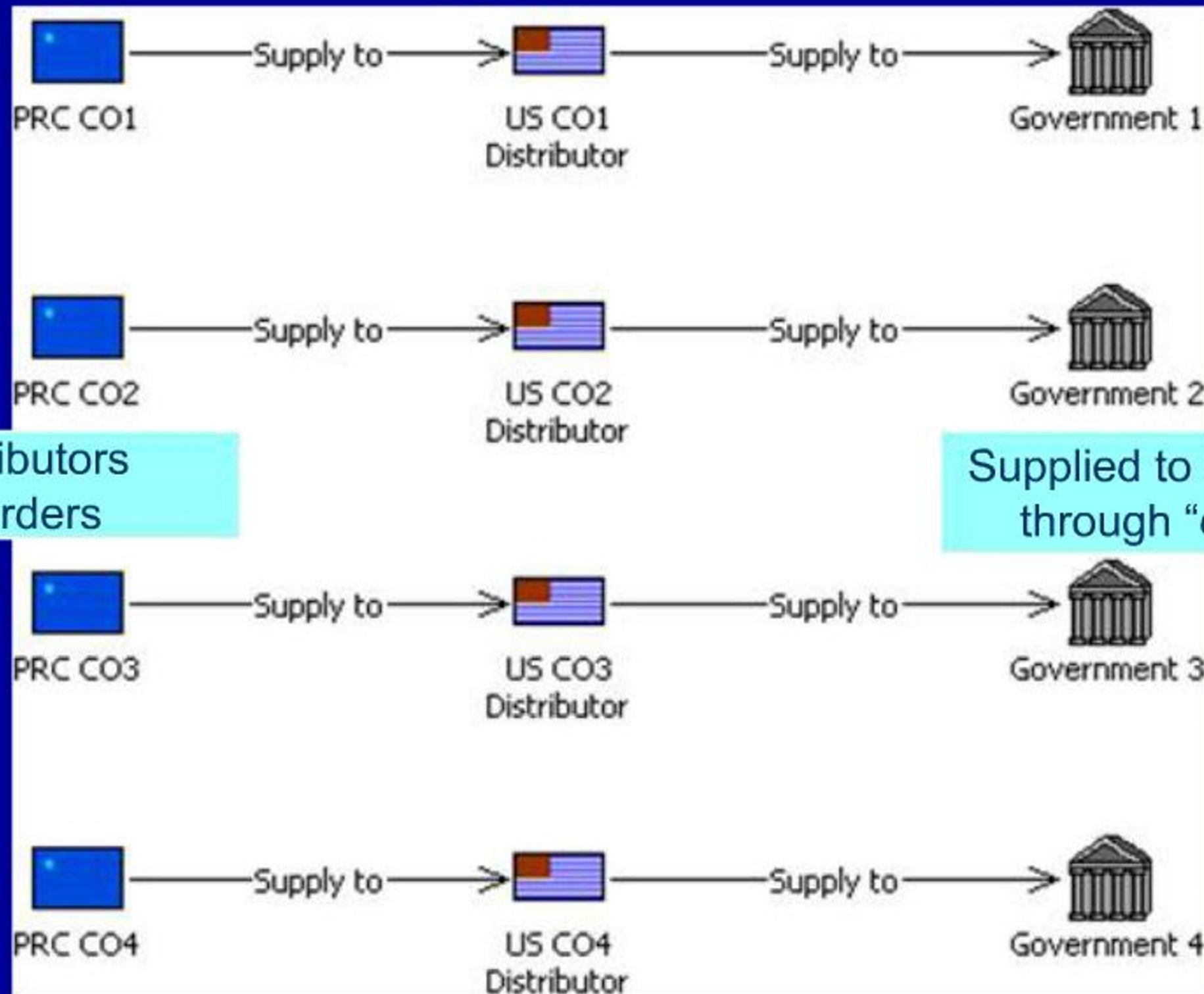


ShenZhen, PRC





Supply Chain 1 – Directly from PRC

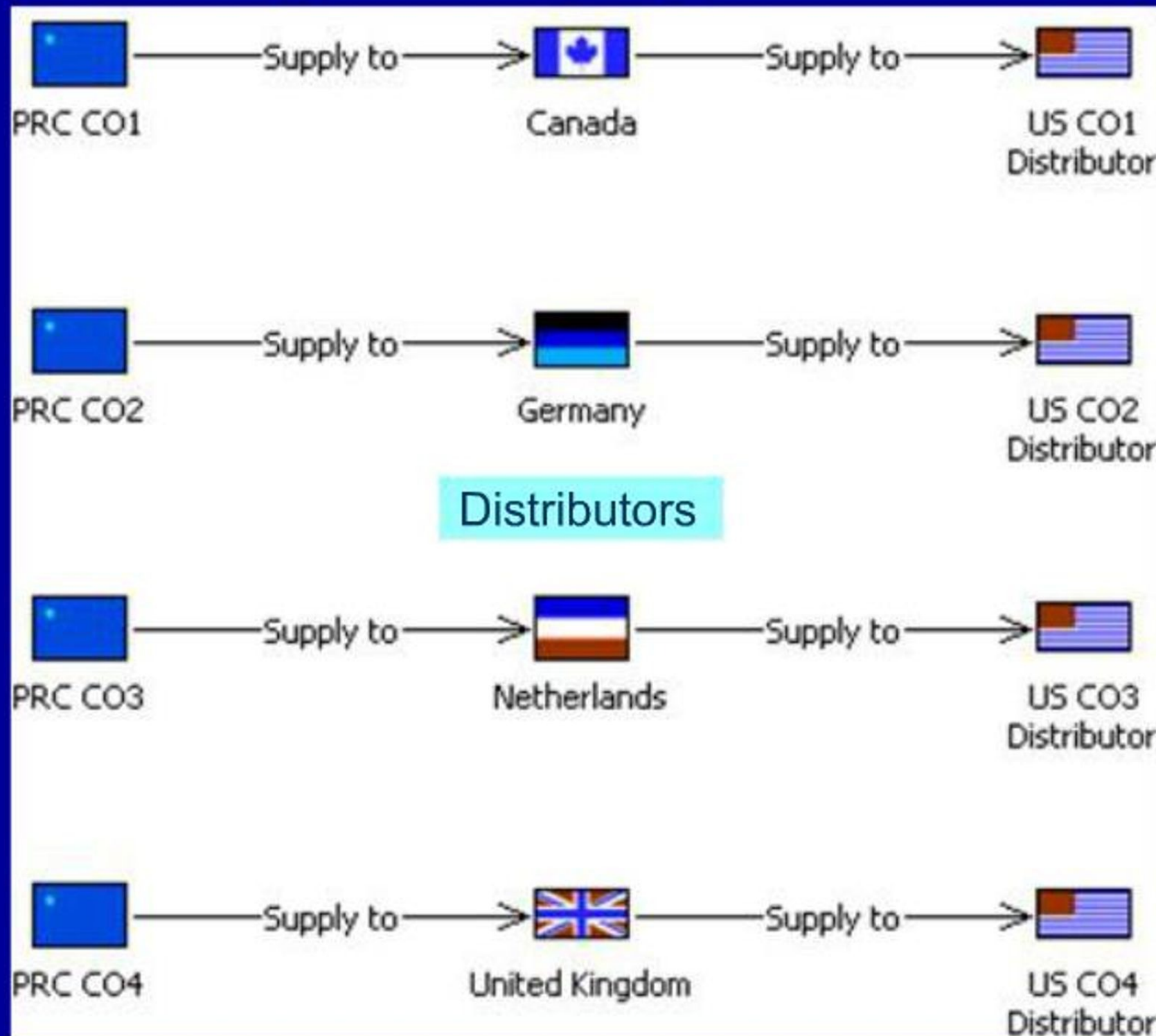


U.S. Distributors
places orders

Supplied to Government
through "drop ship"

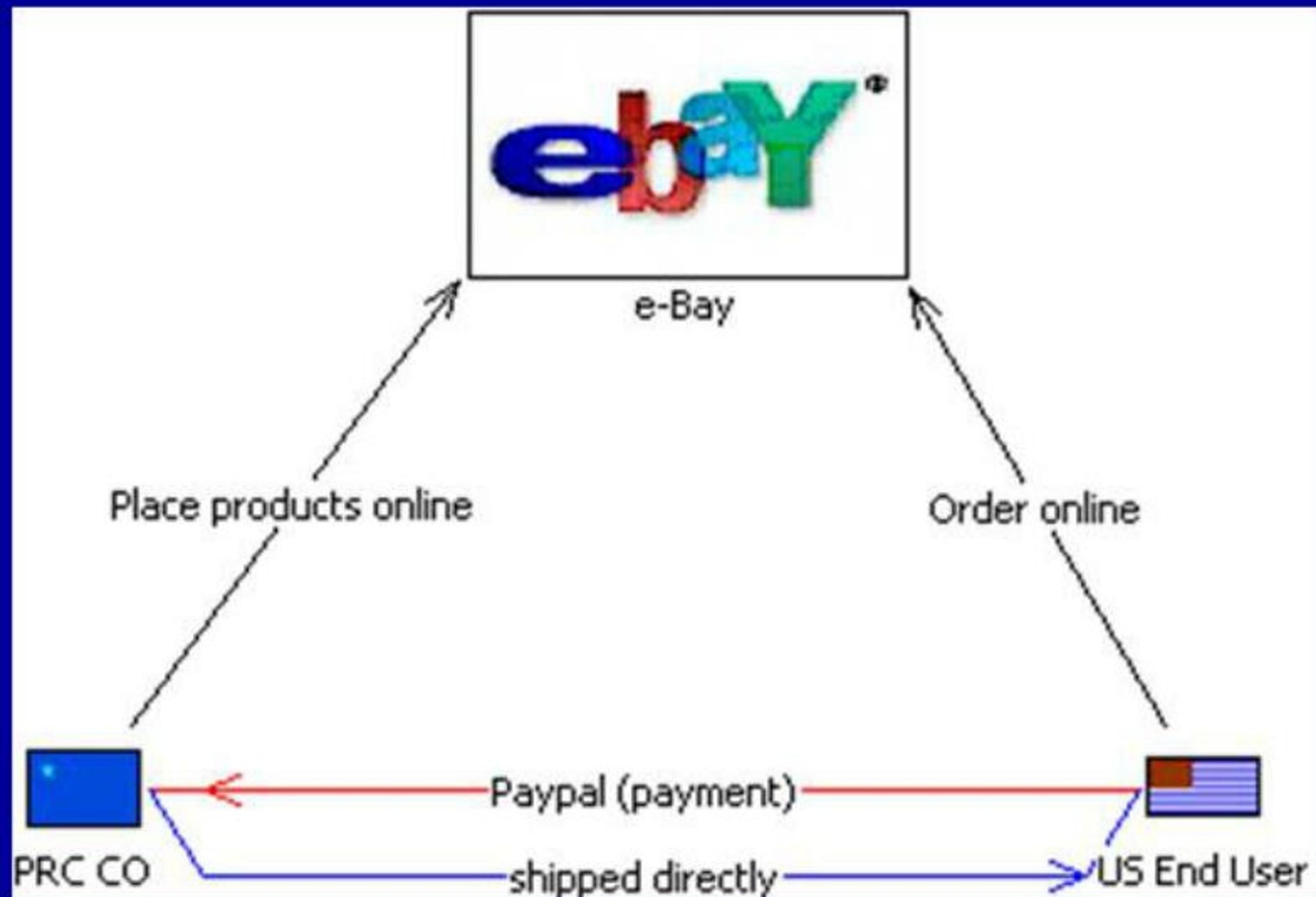


Supply Chain 2 – Through Foreign Country





Supply Chain 3 – ebay





Supply Chain 4 – Government Credit Card



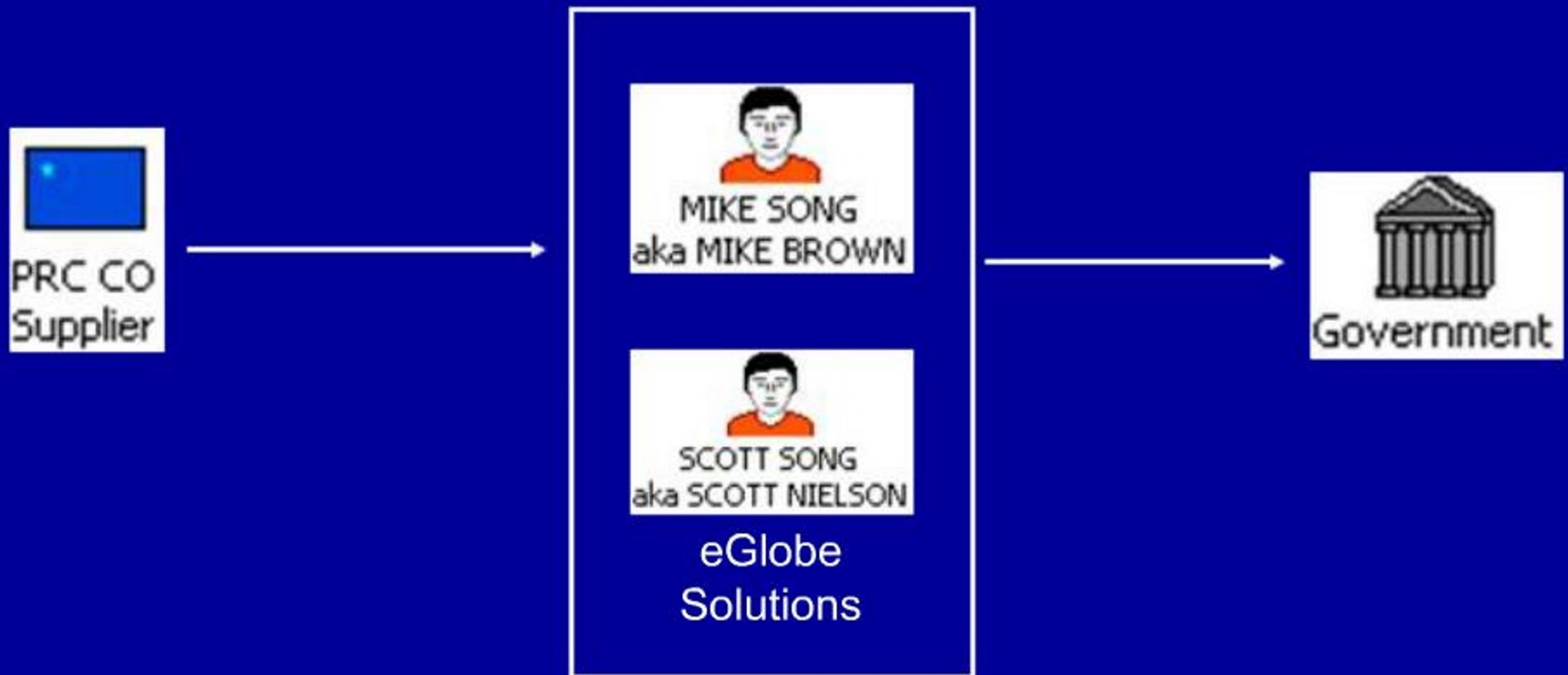


Open Source Examples

- Supply Chain 1 – Directly from PRC
 - eGlobe Solutions Inc.
 - Syren Technology
 - Navy Project
 - MortgageIT
- Supply Chain 3 – ebay
 - Todd Richard
- Supply Chain 4 – Government Purchase Card
 - FBI



eGlobe Solutions Inc.



(Authorized Cisco Vendor)

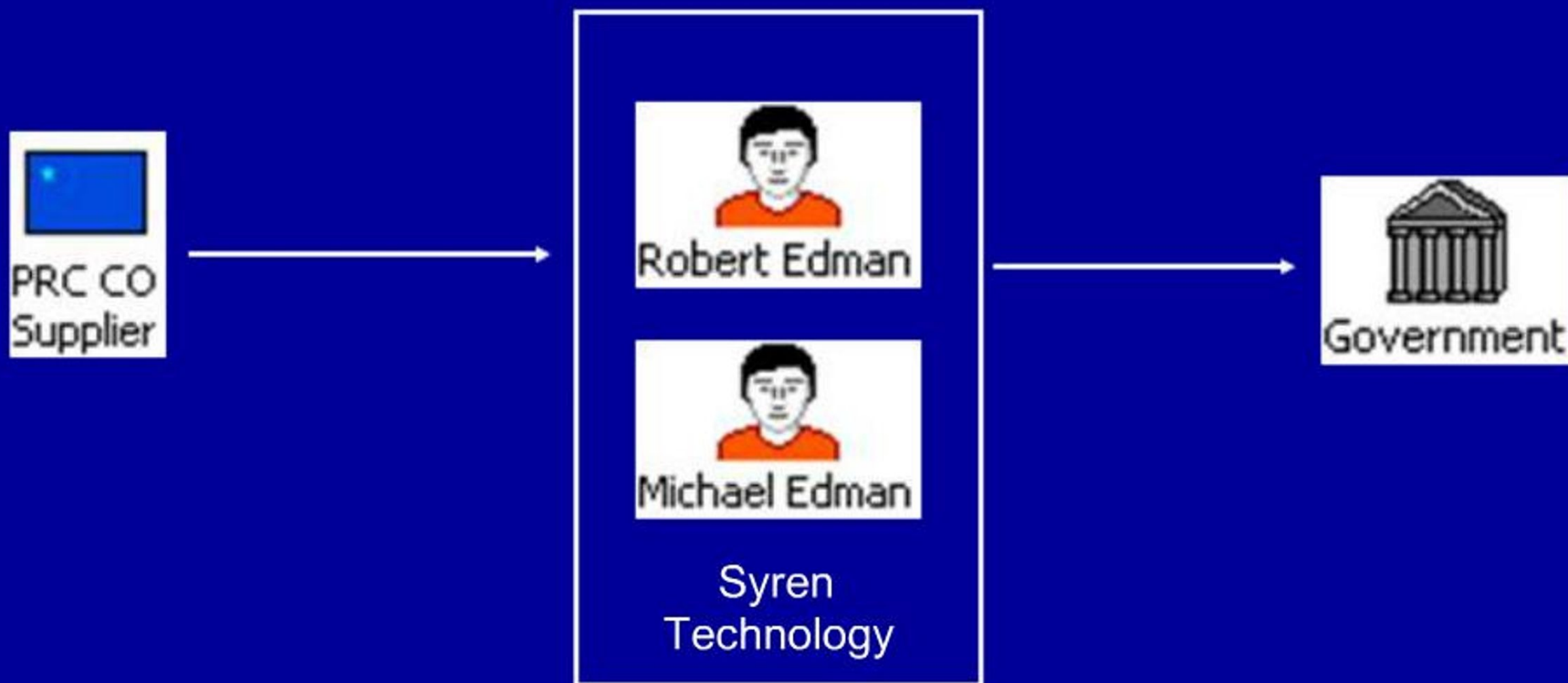


eGlobe Solutions Inc.

- May 2003 – July 2005
 - \$788,000 counterfeit equipment
- November 2006 Indicted
 - Conspiracy, Mail Fraud, and Counterfeit Trademark
- Sold to
 - U.S. Naval Academy
 - U.S. Naval Air Warfare Center
 - U.S. Naval Undersea Warfare Center
 - U.S. Air Base (Spangdahelm, Germany)
 - Bonneville Power Administration
 - General Services Administration
 - Raytheon (Defense Contractor)



Syren Technology





Syren Technology

- August 2002 – July 2004
- December 2007 Indicted
 - Trafficking in counterfeit Cisco products
- Sold to
 - Marine Corps
 - Air Force
 - Federal Aviation Administration
 - FBI
 - Defense Contractors
 - Universities and Financial Institutions



U.S. Navy Project



(Won bid for US Navy Project)

U.S. Navy



(Unauthorized Cisco reseller)



Sub-contractor

(Ships counterfeit to U.S. Navy)

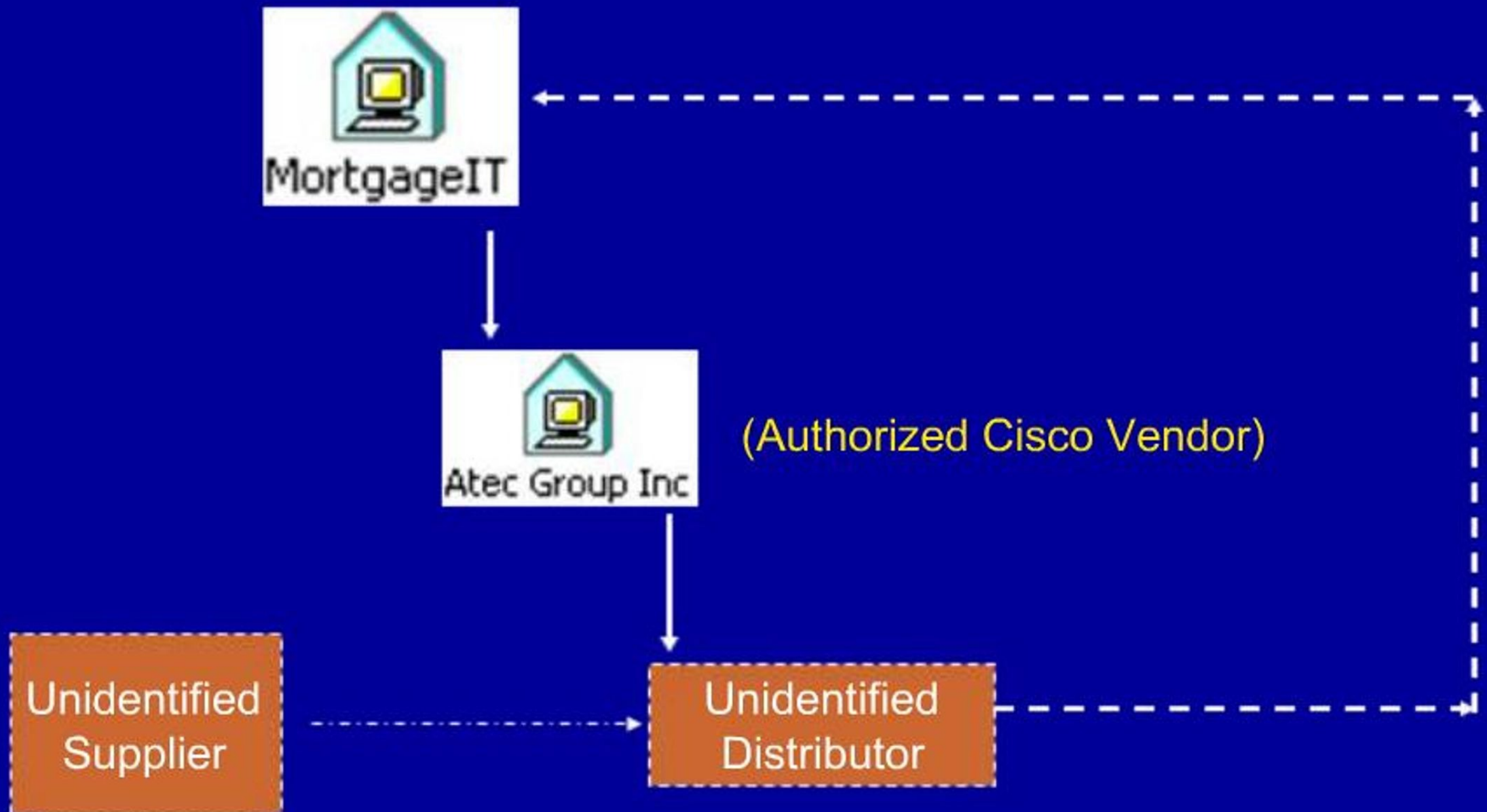


U.S. Navy Project

- \$250,111 counterfeit Cisco equipment
- Lockheed Martin
 - Did not use GSA IT Vendor or authorized Cisco reseller
 - Discovered duplicate serial numbers Cisco switches



MortgageIT: Non-government Example

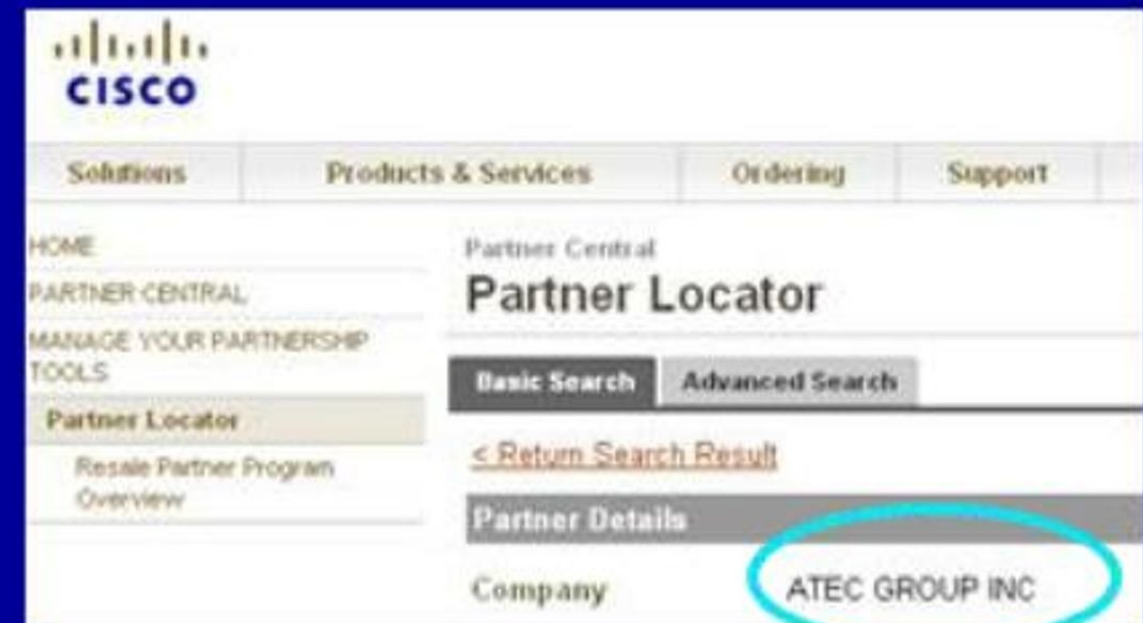




MortgageIT:

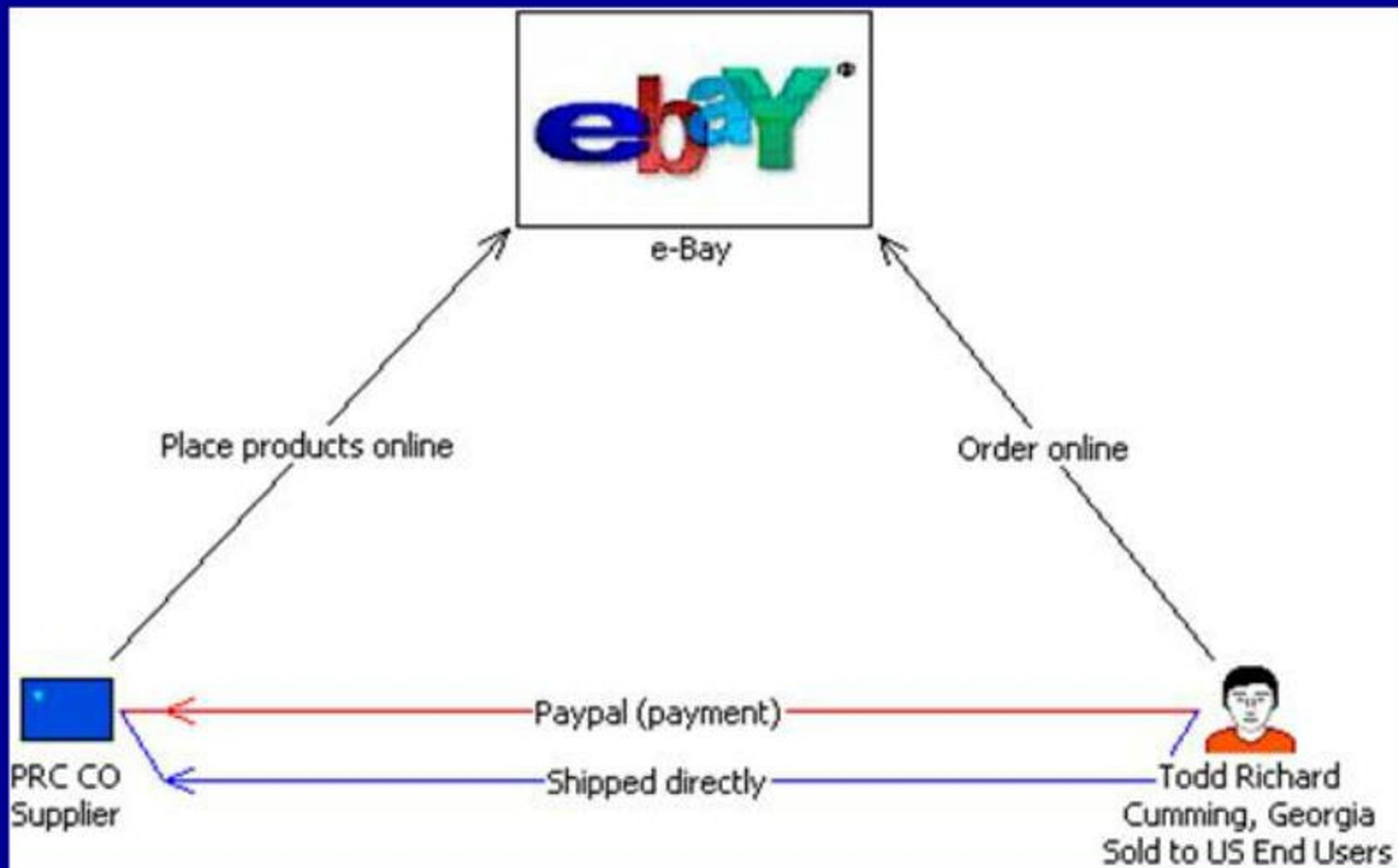
Non-government Example

- Discovered WICs were faulty during routers upgrade
 - 30 counterfeit WAN Interface Cards (WIC)
- Atec Group Inc.
 - Authorized reseller selling counterfeit
 - Cisco
 - Microsoft
 - Symantec





Todd Richard





Todd Richard

- Between 2003 – 2007
 - \$1,000,000 counterfeit equipment
- October 2007 Indicted
 - Trafficking in counterfeit Cisco trademarks
- Separate shipments
 - Counterfeit equipment, labels, boxes, and manuals

Supply Chain 4 – Government Credit Card



Non-GSA Vendor
Selling Cisco Equipment



Government
Purchase Card



Critical Infrastructure Threat



Scope of the Problem

- Alliance for Gray Market and Counterfeit Abatement (AGMA) & KPMG White Paper
 - 1 in 10 IT products sold are counterfeit
 - 10% IT products counterfeit
 - \$100 billion

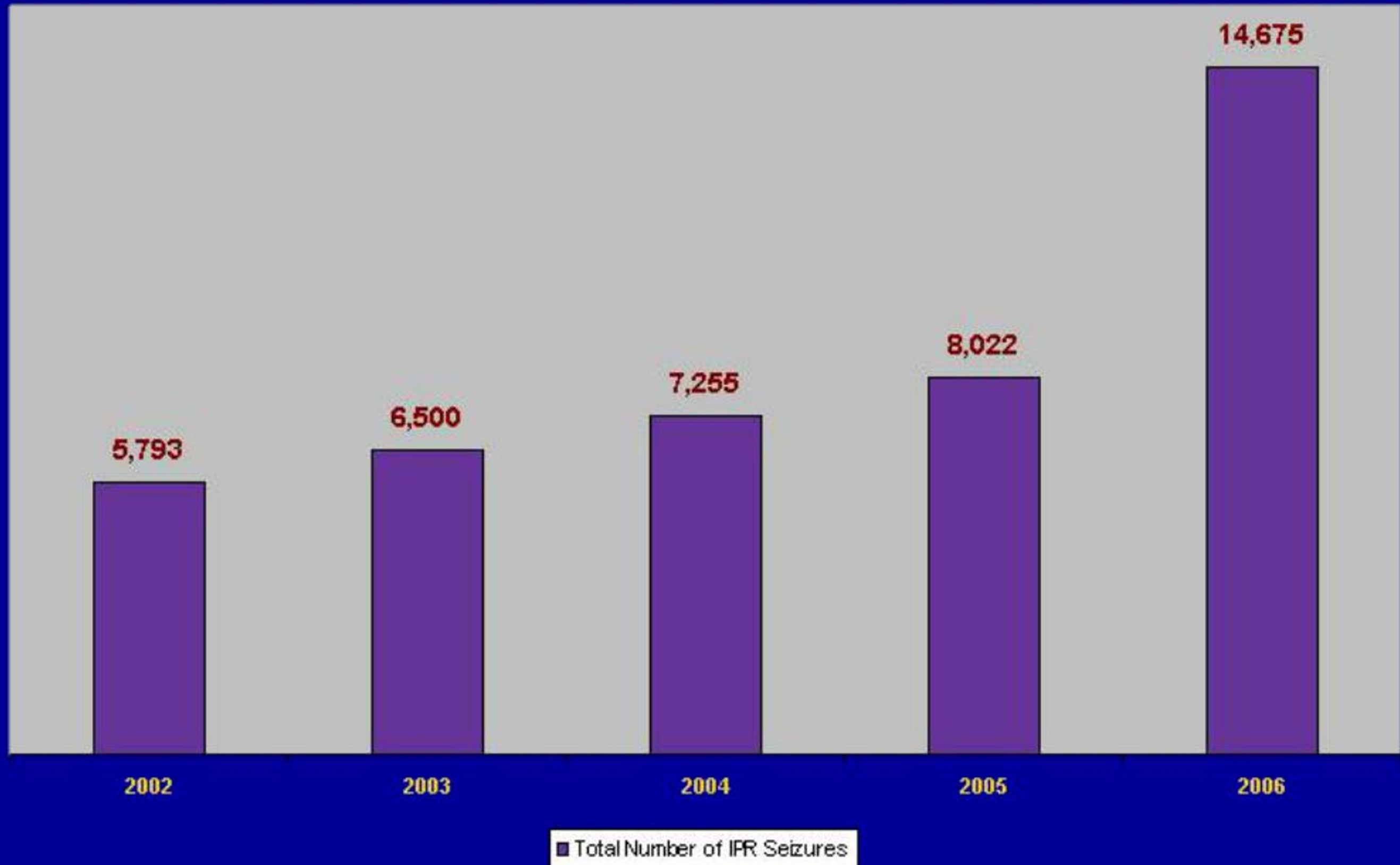


Scope of the Problem

- Law Enforcement estimates much higher
 - Customs and Border Protection (CBP)
 - Only seize registered items
 - Dell Computers not registered
 - No label = no seizure
 - Cannot check every container
 - FBI
 - Chinese postal service vs. shipping services
 - Smaller shipments
 - Hardware, software, manuals and labels shipped separately
 - Assembled in United States

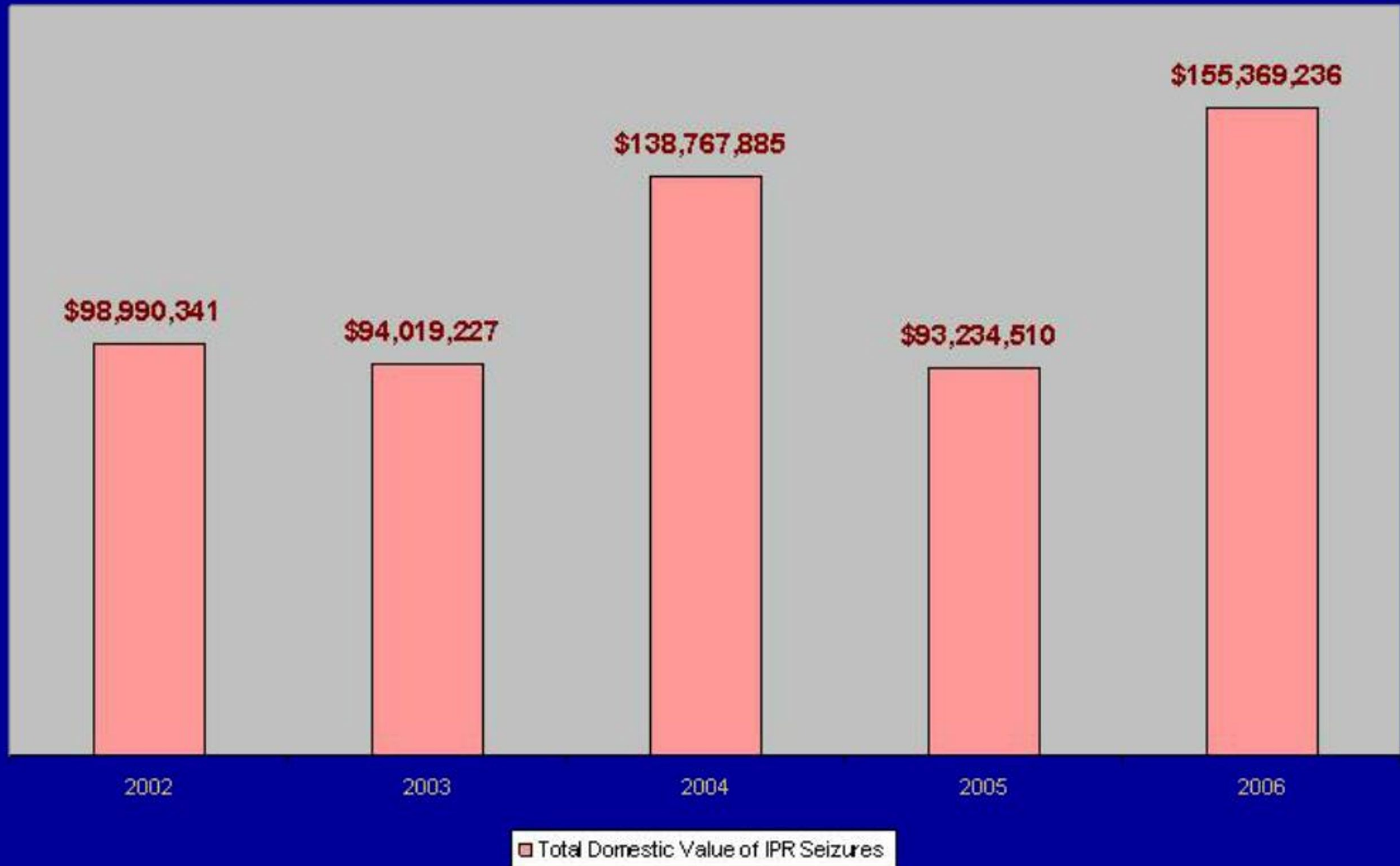


Total Number of IPR Seizures





Total Domestic Value of IPR Seizures





Government Procurement Problem

Government Procurement



- Most government agencies use enterprise information system
 - Coordinate business process
 - Standard data structure
 - Standard equipment
- Cisco routers used in enterprise information systems



Why Cisco Routers?

- Cisco has 80% market share



Government Procurement

- Government searches for lowest price
- Contract language allows for
 - Subcontracts
 - 2 to 3 levels of sub-contractors
 - “Blind drop” or “drop ship”
 - Non-OEM purchase
 - Smaller businesses
- No vetting of vendors by Cisco or GSA
 - If done by government, usually only background check



Problems with Cisco

- No Direct Sales
 - Cisco has 5 major distributors
 - 2 distributors sell to government via GSA
 - Comstor.net (200+ vendors)
 - Immix Group (not awarded yet - ? vendors)
- Exceptions
 - Highly specialized equipment sales
 - Intelligence community agencies
 - Large telecom providers



Problems with Cisco

- Cisco's solution:
 - Use Cisco Gold/Silver Partners
 - Training/support designation given by Cisco



Problems with Cisco

- Government's Problem:
 - Gold/Silver Partners
 - purchased counterfeit
 - sold counterfeit to government and defense contractors
 - Cisco's Brand Protection does NOT coordinate with Cisco's Government Sales



FBI Effort to Combat Problem



FBI Coordination

- 3 Case Coordination Meetings (2006-2007)
 - Immigration & Customs Enforcement (ICE)
 - Customs & Border Protection (CBP)
 - Defense Criminal Investigative Service (DCIS)
 - Department of Interior (DOI)
 - Environmental Protection Agency (EPA)
 - Department of State (DOS)
 - Department of Defense (DOD)
 - Local Police Departments



FBI Coordination

- General Services Administration (GSA)
 - Ongoing coordination
 - 03/2007, GSA attended FBI Case Coordination Meeting (Dallas)
 - 07/2007, GSA-FBI-DCIS Coordination Meeting (Seattle)
 - GSA Actions
 - Letters of supply
 - Policy review - ongoing
 - Expansion of investigation to address all counterfeit IT equipment
 - Supporting FBI investigations



FBI Coordination

- Department of Defense – multiple investigations
 - Defense Criminal Investigative Service (DCIS)
 - Naval Criminal Investigative Service
 - Air Force Office of Special Investigations
 - Army Criminal Investigative Service
- All services concerned with critical infrastructure protection
 - DCIS-FBI Counterfeit IT Equipment Working Group



US-China Joint Liaison Group

- Co-chaired by US DOJ and Chinese Ministry of Public Security (MPS)
 - Facilitate cross-border criminal enforcement operations
 - Intellectual Property Criminal Enforcement Working Group
 - Submitted requests for investigation
 - Example: Summer Solstice (Microsoft software investigation)



Overseas Coordination

- Canada
- Germany
- United Kingdom



Intelligence Gap



Intelligence Gap

- Purpose of counterfeit:
 - For profit or state sponsored?
- Scope of counterfeit equipment problem:
 - Routers?
 - Other IT equipment (PCs, printers, etc.)?
- Effect on the critical infrastructure?



The Threat

- IT Subversion/Supply Chain Attack
 - Cause immediate or premature system failure during usage
 - Gain access to otherwise secure systems
 - Weaken cryptographic systems
- Requires “intimate access to target system”