



World Wide Technology, Inc.

National Institute of
Standards and Technology

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

***Bridging the Divide: A discussion of Federal Government and Industry's
Thoughts and Vision for ICT Supply Chain Risk Management.***

Craig S. Corbin
October 15, 2012

Agenda

- Current requirements we are seeing
- WWT response
- Challenges (opportunities) we see
- Recommendations



From a Very Current Solicitation

In accordance with Section 806 of Public Law 111-383, the 2011 National Defense Authorization Act, the Army is currently developing a system to assess supply chain risk. The details of this system are not defined at this point, but will potentially involve a mechanism for evaluating a particular vendor's supply chain risk (regarding unwanted intrusion, counterfeit hardware, sabotage, etc.), and suspending or revoking a vendor's ability to sell products to the Army/DoD until its supply chain risk issues have been addressed. Because the details of this system have not yet been finalized, this notice is intended to alert offerors that if they receive an award under this solicitation, a modification may be made at a later date to all contractors in the ITES-3H pool to implement this supply chain risk management system. This change would be negotiated and implemented at a future date, per the Changes clause (FAR 52.243-1).



From a Recent RFP from an SI on a Large Government Program Buying IT Gear

4.5 Counterfeit Parts

Supplier will provide copies of policies and procedures in place to ensure that all products furnished to buyer under any order as a result of this agreement will not be counterfeit parts or products as defined below:

A counterfeit part or product is not genuine if:

If it is an unauthorized copy

Does not conform to the original OCM design, Model and or Performance Standards

Is not produced by the OCM or is produced by an unauthorized contractor

Is an off-specification defective or used OCM product sold as “new” or working

Has incorrect or false markings and or documentation



From Another Recent Solicitation:

The Contractor shall identify to the government how they are addressing supply chain risk management issues. At a minimum, the below areas must be addressed. Updates shall be provided annually.

Methods for reducing the risk of malware introduced via the supply chain

Methods for secure delivery of software provided to the government

Methods for differentiating and then mitigating between unintentional software defects (or bugs) and ones that may have been intentionally inserted by an attacker in the supply chain

Best practices used to counter risks associated with malware introduced in the supply chain

Methods used to support detection of malicious additions / modifications to firmware introduced via the supply chain in equipment purchased by the government

Techniques or technologies used to reduce the risk of malicious firmware introduced via the supply chain

Methods used to detect changes to hardware introduced via the supply chain

Methods used to help differentiate between a counterfeit hardware incident (for pure profit motives) and one that may have been introduced by a sophisticated attacker



Where does SCRM fit in Procurement Evaluation?

- Requirements are nebulous – Is the plan for mitigation or the mitigation more important?
- Small Business – Socio Economic Goals vs. choice of a vendor with experience and investments for SCRM implementation
- Lowest Price Technically Acceptable (LPTA).. And where does SCRM fit in?
- Best Value (Cost-Performance Tradeoff) Evaluation - ... And where does SCRM fit in Section M – Eval criteria?
- Interpretation and execution of “3 Bids” and usually choosing “low price”...



What is WWT's Current Response

- Concerned about priorities in procurement. Again, will the Government put teeth in evaluation around SCRM?
- Targeting investments to where we think the puck is and where the puck is going
- Many customers now willing to have discussions and have supply chain concerns
- WWT has created a full SCRM plan that it can use to work with Government customer for mitigation
- WWT has created a fully functioning SCRM process which we believe is industry leading:
 - White labeling
 - Secure delivery
 - Inspection and analysis
 - Electronic and biochemical tagging
- **BIG QUESTION: CAN THESE INVESTMENTS BE MONETIZED?**



World Wide Technology, Inc.

- ❑ Founded in 1990, St. Louis Missouri
- ❑ Revenue of \$3.3B in 2010 & \$4.2B 2011
- ❑ Largest Federal VAR for Cisco
- ❑ Major Partner with HP, Dell, EMC, NetApp & others
- ❑ Largest Supplier – Army ITES 2H, NASA SEWP IV
- ❑ **Provided \$500M+ of Products to Fed Gov in 2011**
- ❑ Specializing in Complex Logistics & Supply Line Solutions



Secure Supply Chain Experience

- ❑ **Homeland Security, TSA, FBI, ICE (Boeing)**
 - ❑ Turn key management of the IT deployment process
 - ❑ End-to-end system integration for order fulfillment & asset management
- ❑ **US Army – Ft. Monmouth**
 - ❑ Complete supply chain visibility for PM DCATS
 - ❑ Fully integrated system with multiple manufacturers
- ❑ **Northrop Grumman**
 - ❑ MDA
 - ❑ USAF
 - ❑ Intel



Midwest Warehouse and Distribution Center



St. Louis Integration Technology Center (ITC)



World Wide Technology, Inc.

Questions...