Developing a Framework to Improve Critical Infrastructure Cybersecurity

Comments By:

Lineage Technologies, LLC
1455 Pennsylvania Avenue, N.W.
Suite 400
Washington, D.C. 20004

Introduction

Lineage Technologies, LLC welcomes this opportunity to comment upon developing a framework to improve critical infrastructure cybersecurity. Lineage Technologies, LLC is an outgrowth of market demand for secure commercial-off-the-shelf IT hardware components and systems.

Lineage Technologies, LLC is an integrator of state-of-the-art IT components and systems that are designed and manufactured exclusively in the United States. Lineage was established to ensure customers that the devices they buy are free from foreign taint and/or counterfeit components. Lineage Technologies serves the COTS marketplace where today the systems sold in the U.S. contain features and functionality that threaten users.

The threat posed to the United States from tainted IT systems is severe. It encompasses threats to national security and the economic wellbeing of the nation. The breadth of the threat keeps growing and will not abate until effective security measures are instituted that protect critical assets/infrastructure from attack, and secure privacy for individuals and enterprises. In October 2012 Secretary of Defense Leon Panetta described the condition the nation confronts as one where the United States is facing the possibility of a "Cyber-Pearl Harbor" and that the nation is increasingly vulnerable to foreign hackers who can dismantle the nation's power grid, transportation system, financial networks, and government. High profile penetrations and thefts that came to light in 2012 include:

- Aviation Week & Space Technology report that in 2009 Chinese engineers were discovered to have participated in classified program/progress review meetings for the F-35, and had done so consistently for several years.
- NASDAQ's Chief Information Security Officer testified before the House Committee on Finance, telling Members that "they [China] are in our system, and we cannot get them out without the direct support of the U.S. Government".
- Cyber Command Director, General Keith Alexander, told the Senate Committee on Homeland Protection that direct cash outflows from U.S. banks in 2011 exceeded $338 billion, and that IP losses for that year exceeded $225 billion. Cyber Command has estimated the total dollar value of annual U.S. losses (Government and Industry) at $1 trillion per annum, or 8.4 percent of GDP.

The last item reflects a loss rate that is an unsustainable and over a decade will bankrupt the nation.

The tremendous advancement in IT capabilities and functionality has been a boon to all. The ease with which we communicate and transact business has come directly from advances in IT engineering and computing power. These advances have been spectacular and unprecedented in human history. Unfortunately, much of this advancement has come at the expense of security in the design and manufacture of the IT systems we have come to rely upon. Functionality, speed, and other requirements eclipsed security considerations. Thus, today trillions of dollars annually flow across borders from

property owners to thieves and/or nation states over vulnerable IT systems. Cyber Command's Director, General Keith Alexander characterized this as "the largest wealth transfer in all of history". Verizon, in its 2012 annual cyber threat report noted that between 60 – 80 percent of thefts involved (1) trade secrets; (2) sensitive organizational data; and (3) systems information.

Unfortunately, today the vast majority of solutions offered in the cyber security space involve actions that are applied after breaches and thefts occur. Verizon reported that initial-attack-to-initial-compromise occurs in minutes, while the initial-compromise-to-discovery occurs over periods of months. This condition makes traditional remediation and solutions entirely ineffective, in effect closing the barn door after the horse has gone.

Be they firewalls, encryption, consensus standards, best practices, etc., the methods deployed today do not work. At best they serve to credential products and the professionals tasked with protecting assets and systems giving each the imprimatur of acting under false pretense. Reliance upon these metrics has yielded illusory results at best, and so must be viewed with great skepticism and doubt. This is not to say that all such systems have no value, but instead, that before we invest in bolstering their use, we must measure their effectiveness, and jettison those that do not measure up. We must also acknowledge that for the most part international standards are being enforced in the breach, so the noble efforts expended there without strong unilateral national enforcement will be for naught.

Compounding this problem is the pace of innovation and development in the IT space. Today we can produce microchips with transistor densities in the tens of billions on a single chip. Yet we lack the tools and engineering methods necessary to verify the architecture, much less the security of these IT components post manufacture. This inverse trajectory threatens our ability to verify and validate security in an empirical manner, so as the geometry of transistors gets ever smaller (34nm, 22nm, 14,nm, 7nm) and the density of circuits on chips increases, our ability to use empirical test methods and indices to determine security diminishes in equal proportion, leaving little room for traditional methods or procedures to provide the confidence we need in the security of the systems we procure. And because threat vectors increasingly include burned-in/on-silicon backdoors, trapdoors, and Trojan Horses that allow adversaries unobstructed access to systems wherever they are deployed we are left without methods to assure the security of components and systems unless we control the source from which they come.

It is this unfortunate circumstance that leads Lineage to conclude that the Framework must concentrate implementation on policies and procedures that reduce the threat horizon. This, unfortunately, will require reliance upon strict management controls, including restrictive procurement policies.

Congress took prescriptive steps in this direction with the enactment of H.R. 933, sections 516 and 535; the 2012 NDAA, section 818; and the 2013 NDAA, sections 933-937 to drive enhanced supply-chain security, and procurement policy for the Federal Government. These statutes impose limitations on Government IT suppliers and

Government IT buyers. It is conceivable, that when regulations implementing these provisions are issued a new market for IT components and systems will emerge. That market can serve critical infrastructure components as well, and do so in a manner to assure lower-cost product than might be otherwise possible if these two markets were considered separately. Lineage believes the aforementioned legislation compliments EO 13636 and PPD 21, and so should be incorporated in this review. Lineage strongly encourages NIST and DHS to ensure that the Framework implements policies that enhance Management Controls and Procurement Reform for critical infrastructure components. This will reduce market confusion and will facilitate rational pathways to market for those products able to meet new demands.

Comments

These comments are directed at the manufacture of IT components and systems. Lineage is submitting these comments to address only those applications, and so does not intend to address operations issues beyond those associated with IT component and systems manufacture. Lineage's comments do apply equally elsewhere, in some instances, but are not intended for those purposes in the context of this response.

Lineage is an outgrowth of demand for secure COTS IT components and systems. As such the firm is relatively new, and its experience in this market is limited. However, Lineage staff includes experts in IT supply-chain management and security, and methods for establishing levels of assurance for IT products. Lineage's founders and executives hail from the IT industry, and so offer views from the perspective gained from past activities in this arena.

As a matter of principle the Company adopted management practices that closely align with the aforementioned statutory requirements. The Company did so before conception of those laws, and based its decision upon an evaluation of risk that yielded to the conclusion that sourcing of supply was the most critical factor in addressing risk in this marketplace. This principle is evidence-based and tracks the Department of Defense requirement in DODI 5200.44 that requires vendors to prove the negative regarding penetrations, in other words that a component and system has not been tainted and/or counterfeited. That requirement is almost impossible to meet, unless one employs management controls to address sourcing.

Air Force Chief Scientist, Dr. Mark Maybury, has noted that we know how to manage most IT threat vectors, but that unless the IT supply-chain is made secure we will continue to build castles on foundations of sand. In a talk by RSA Chief Scientist Ari Juels in March 2013 concurred with this conclusion when asked which strategy (encryption or hardware) will yield the best result in securing cyberspace. He sided with hardware security. Lineage concurs with these assessments, and has aligned its business accordingly.

Lineage's decisions regarding risk are also heavily influenced by China's policy to limit oversight and inspection of plants, equipment, personnel and products, including oversight and inspection of foreign owned enterprises located there. Sovereignty rights asserted by Chinese Officials has made it impossible to provide adequate assurance and risk control for products manufactured there.

Additionally, evidence developed in 2012 by Cambridge University researchers Sergei Skorobogatov and Christopher Woods that demonstrated burned-in/on-silicon threats on Actel/Microsemi's ProASIC3 chip produced for them by TSMC (Taiwan) suggests that sourcing is a pervasive threat vector that must be tightly managed. The Cambridge University researchers found keys on the ProASIC3 chip that:

> *"…would allow an attacker to disable all the security on the chip, reprogram any cryptography and access keys, modify low-level silicon features, access unencrypted configuration bit-stream, or permanently damage the device".*[1]

They concluded the device was wide open to intellectual property theft, fraud, re-programming, etc. They also concluded that the penetration enabled attackers to reverse engineer the design of the chip thereby facilitating the design and introduction of newer versions of Backdoors or Trojan Horses. Lastly, they concluded that these penetrations could not be reversed or patched leaving every user vulnerable to unobstructed attack.[2]

This threat has caused several U.S. owned fabless design houses to move all manufacture back to the U.S. This little known "quiet revolution" gives further evidence to the need for supply-chain control and management. The decision by these firms concerned the theft of their intellectual property. Thus, despite the penalty they may encounter in terms of loss of market share in that region of the World they decided their survival depended upon forgoing work there.

Thus, sourcing components and systems from suppliers must be limited to those over which specific controls can be placed. This is essential to establishing trust, and mitigating risk. Without such controls, ensuring security in IT components and systems cannot be achieved.

The mechanisms to do this will require law and regulatory changes that will allow, even encourage, close collaboration between IT enterprises. If this is not possible the Framework must foster policies and incentives that encourage and drive reintegration of operations by IT device designers and manufacturers. Outsourcing of design and manufacture of IT components and systems has demonstrated remarkable achievements in terms of functionality, speed and economic growth. Unfortunately, these achievements have come recently at a heavy cost, the price of which is ever increasing in terms of the loss of sovereignty, wealth and privacy.

---

[1] Sergei Skorobogatov, Christopher Woods, "Breakthrough Silicon Scanning Discovers Backdoor In Military Chip", http://www.cl.cam.ac.uk/~sps32/ches2012-backdoor.pdf: 1

[2] IBID: 1

To combat these threats we may have no choice but to reduce the size of this threat vector, by reducing the size of the supply base. This is antithetical to free market principles, and may come at a cost to innovation, but in the near-term the nation may have little choice but to implement such policies if it is to reduce its exposure to cyber attack and theft.

(1) What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure

Market response to cyber threats is highly inconsistent, and reflects uncertainty regarding emerging requirements, liability, costs, the effectiveness of standards, differences in technology configuration, etc. In sum the environment is quite varied and extremely fluid. Decisions regarding response strategies are as varied as the industries and institutions that confront the threat.

Lineage is limiting its response here to the question as it relates to addressing sector specific issues. The answer to that portion of this question that relates to collaboration was provided in (1) above.

Lineage believes that the Framework would be best implemented on a sector-by-sector basis. This would allow for variations in requirements that reflect response strategies best suited to differing market segments and will allow the implementation process to develop a level of granularity necessary to effectively address sector specific characteristics, thereby reducing risk. It is our fear that a one-size-fits-all solution will crumble under its own weight.

Sections 10(a) & (b) of the EO provide the foundational structure for this strategy. Those provisions envision a sector-by-sector assessment of regulatory authority that corresponds to risk. While existing statutory authorities do not correspond exactly to market sectors, they come reasonably close and allow for application of defensible boundaries. Furthermore, they have been in place in most instances for decades and as such have fostered institutional mechanisms through which policy and policies can be effectively and efficiently implemented. By exploiting existing relationships between critical infrastructure components and Government regulatory experts, communication about issues and technical considerations can be achieved. To ensure an informed dialogue between these parties on cybersecurity NIST and DHS must provide cyber experts. Cyber considerations should be socialized to these groups simultaneously, and coherency must be demanded and measured.

Questions regarding individual threat profiles are already being addressed by the FBI through InfraGard, but issues surrounding data-sharing, liability, and privacy still must be adjudicated by Congress, and so should be excluded from discussion between the Parties until such time as new laws are enacted for those purposes.

The need for a sector-by-sector approach can be illustrated by the difference in EPA regulations governing Clean Air, Water, Groundwater emissions/discharges, and FDA's authority governing the manufacture of prescription drugs. Both require strict adherence to empirical data as required in their respective regulations. Each Agency requires the demonstration of assurance, either in the form of data records, or sampling and analysis, or both. Systems for each operate in exacting and unique environments that demand precision and accuracy yielding measurements and reporting in increments in parts per billion. However, the IT equipment used for one purpose is not the same as that for another purpose. Control systems deployed in these sectors are designed, developed and deployed separately and often times do not have designs in common. What they do have is measurements and outcomes in common. Thus, when addressing their respective cybersecurity needs Lineage believes they should be addressed on a component and system basis not a measurement or outcome basis.

It can be argued that devices that deployed for such measurements are becoming more homogenous, but the market has not achieved a level of commonality yet. In fact the Telvent example has a great many firms seeking alternatives to common architectures, even Company specific alternatives. So to preserve the opportunity to develop a level of granularity desired to implement sound policy across the spectrum, Lineage recommends a sector-by-sector approach.

(2) Describe your organizations policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures.

Lineage Technologies, LLC is an outgrowth of the demand for secure COTS IT components and systems. As such the Company's policies and procedures are focused entirely on risk and the best methods and procedures available to us to assure security in the components and systems it takes to market.

Lineage examined a great many procedures, most expressed in standards and found them wanting. Most are not enforced and so do not yield security. Therefore the Company has developed its risk mitigation processes around National Security standards, methods and procedures. This initially complicated our relationship with commercial vendors, which objected to intrusions into IP, Plant, Processes, Personnel, etc. However, with an understanding of the nature and extent of the cyber threat confronting the nation, and the market potential this offers, those concerns are abating.

The benefits from using secure sourcing and understanding every element of design, fabrication, packaging, functionalization, test, surface mount, assembly, test, delivery, test, and integration has allowed the Company to coordinate with suppliers to ensure the highest level of assurance possible.

The following steps illustrate some of the management procedures Lineage established to inculcate the highest assurance possible:

I. US citizenship for all personnel involved in any project involving Lineage product, to include, at the very least, FBI background checks, and in most instances National Security Clearance
II. Identification/verification/inspection of all critical design and component features of a product
III. Sourcing based solely upon security provenance of vendors and components processes, and inspection and verification of same
IV. Evaluation procedures designed and implemented to assure National Security, including:
Inspection/verification/test of reticles
Inspection/verification/test of all process and inspection equipment
Inspection/verification/test of fabrication processes
Inspection/verification/test of packaging
Inspection/verification/test of firmware/installation
Inspection/verification/test of surface mount
Inspection/verification/test of assembly
Inspection/verification/test of integrated systems
Inspection/verification/test of installation
Inspection/verification/tracking for all transport

Lineage requires tagging, tracking and locating of its components and systems in real time 24/7/365. Thus, once a design/process/component enters the Lineage system it is totally controlled and supervised until it is transferred to customers.

Lineage focuses its attention on critical path components, such as I/O, Logic, Memory, Mass-storage, Controllers, Antenna, Wire/Cable, Connectors (USP, CAT, etc.), Case, etc., that can facilitate penetrations. Lineage uses performance indices (e.g. IEEE, SAE, SPE, ASTM, ANSI, ISO standards, etc.) to evaluate all other components to a system (e.g. fasteners, solder, flux, resin, adhesives, etc.). Batch testing, process examination, and audits are used to assure quality and performance for these items.

Management controls are employed in a straightforward manner. For the most part this means limiting the supply base to those enterprises that Lineage can trust, and echoing all others. Lineage only engages in direct supplier relationships. No Third Party can ever enter the Lineage supply chain for critical path items.

Since these policies and attendant procedures are at the heart of the Lineage enterprise, all employees are trained to understand them. Training includes but is not limited to the following:

I. Overview of all current legal and regulatory drivers affecting this marketplace
II. Overview of economic market drivers affecting this marketplace
III. Detailed description of all vendor relationships
IV. Detailed description of all process controls, and attendant Agreements with vendors
V. Detailed training regarding specific job duties, including ND/NC Agreements

VI. Detailed training regarding all legal and regulatory obligations directly affecting Lineage its vendors and customers
VII. Semi annual reviews of (I-IV)
VIII. Annual review of (V-VI)

There is not much that distinguishes these management practices from traditional management training, six sigma, and related policies and procedures. Lineage is a lean integrator of IT systems, and as such relies upon trusted suppliers to provide a reasonable level of assurance in the process of delivering trusted components and systems to the COTS community.

It should be noted that by and large the design and features of COTS hardware are inherently vulnerable to cyber attack because of inherited flaws that persist in the design of components, and familiarity with these features by designers and adversaries throughout the globe. Exploitation of these feature flaws is one of the most common attack vectors. Considerable efforts are underway to overcome these flaws and to reduce the threat space on chips, yet here too, unless we control the processes by which we fabricate chips and assemble IT hardware we cannot reduce the threat horizon.

Lineage and its supply base is aiming for a level of security and assurance that is better than can be expected from foreign sourced suppliers, and is as close to National Security standards as can be achieved with the design and supply resources that exist within the United States. Thus, while we impose strict process and supply-chain controls we realize that perfection is beyond the Company's reach. Nonetheless, by eliminating the persistent threat posed by foreign sourced supply Lineage will have significantly reduced the threat profile to U.S. Government and Industry, and will give other security measures such as encryption and firewalls a better chance at performing their functions.

NIST and DHS are asking for comment on whether we can build upon existing guidelines, standards, and regulations, and improve them sufficiently to achieve an acceptable outcome. In the absence of effective enforcement, and the cessation by nation states to view cyberspace as a treasure trove to plunder, Lineage thinks not. Despite adherence to existing guidelines, standards and requirements trillions of dollars in the form of cash, IP, and technology continues to flow out of the United States to cyber assailants annually. We cannot reconcile these losses with the prospect that all users of guidelines, standards and regulations are dullards and fools. Instead we conclude that despite adherence to these requirements, the mechanism by which these thefts are occurring is highly engineered and directed, in essence baked into the IT hardware we employ, and cannot be repaired, patched, or removed.

Sourcing then becomes the key if only parameter over which we can exercise control, and by which we can measure security and assurance. It is here where the Framework must focus attention.

NIST and DHS must also address key technological challenges that have industry cannot approach alone. Until very recently, the only design, engineering and manufacture

metrics employed in the IT manufacturing realm addressed functionality, quality, and application. Metrics to measure security did not exist outside of national security domains. Those metrics cannot be developed by industry for its own sake as they will serve Government and critical infrastructure customers, and so require collaborative development. Lineage has proposed management controls for the time being, but also supports the development of defensible technological tools and methods by which security can be established and measured.