Testimony before the Subcommittee on Communications and Technology
Date of Hearing: 21 May 2013
Witness: John W. Lindquist
President & CEO
EWA Information and Infrastructure Technologies, Inc
CEO
EWA North America, LLC

Mr. Chairman and Members of the Committee,

Thank you for the opportunity to testify on the very important issue of the Security of the Communications Supply Chain.
My expertise and that of IIT, the Company I represent, within the overall process of Supply Chain Security is security suitability and acceptability.

The security of our telecom systems is critical. We are all very aware of the myriad number of threats from nations and organizations unfriendly to the U.S. I leave it to the U.S. Intelligence Community to to characterize that threat but I have sufficient insight to be convinced that the threat is very real, is not limited to a single country, geographic area or organization, and that we must protect ourselves..

That protection is made more difficult because the supply chain for electronic systems and devices in general and specifically telecommunications systems is truly global. There are no manufacturers of telecommunications systems in the U.S. Two of the major telecom system vendors are Chinese, and the other three are European and, those European vendors have very large footprints in China and elsewhere around the globe. Many of these worldwide locations are easily and directly accessible by the various threat nations and organizations. Furthermore, it is the nature of system development to make use of software routines and hardware components that are generally available in the market. It is virtually impossible to determine the pedigree of all of the hardware and software that goes into a telecommunications system. Further, it is not practical to impose a system of trusted suppliers for all of the components. Such a system would be virtually impossible to police and self certification of processes is of little to no value. Our adversaries are professional, highly technically capable, intelligence organizations and/or sophisticated criminals, neither of which would have any difficulty circumventing a self certification system. The bottom line is that the embargo of products from certain countries or companies does not provide secure systems.

To address this security dilemma effectively an Evidence Based System Process (EBSP) must be applied that enables informed decisions as to the security suitability and acceptability of a system before it is deployed and throughout its life cycle.

To be suitable and acceptable, there must be reasonable assurance that any system being introduced into our telecommunications networks are free of malicious features and serious security related defects. It is very likely that the legacy systems, those already in operation, are not free of such security defects and it is unknown if malicious capability has been introduced into the systems. However, it is not practical to shut down our networks to assess the current systems. Thus, the focus must be on new systems and system upgrades. The analytical results on new systems provide insight into the nature of probable security relevant defects in the legacy systems which can be addressed through network security techniques, most likely increased effective monitoring.

The EBSP should be comprised of two major phases. The first is an in depth security assessment of the system to include all patches, upgrades, and modifications as they occur, and the second being a delivery process that insures that the deployed system and all patches, upgrades, and modifications are exactly the ones that were evaluated and determined to be suitable and acceptable.

The key features of the EBSP are:

- Willing participation of the developer/vendor.
- A trusted independent evaluator.
- Direct coordination between the stake holders,(telecoms and concerned government agencies) and the evaluator without interference or knowledge of the vendor.
- Correction of unintentional defects before deployment.
- Immediate involvement of law enforcement if evidence of malicious intent is discovered.
- A delivery system that insures the delivered system matches the evaluated system and prevents the vendor or any other un-trusted party from accessing the system during or after delivery.
- A scheme for monitoring the system after deployment.

We have implemented an EBSP that includes the above features with several telecommunications companies here in the US and Canada performing evaluations and deliveries of multiple vendors products which are being integrated into a LTE upgrade. The results of the evaluations, although not completed, have yielded significant security benefit to the recipient. As a result of our analysis, an extremely large number of security relevant defects have been identified and corrected or are in the process of being corrected. Although we have found no evidence of malicious intent, we have caused the elimination of serious vulnerabilities that the threat would have been able to exploit. These serious defects were found equally in Chinese and non-Chinese vendors products.

In our EBSP, the Vendors have been very willing to comply because their participation in the EBSP was a condition of the sale to the telecommunications company.

The vendors have provided:

- Design documentation for hardware, software, and firmware.
- Source code for system software and firmware.
- A complete set of sample components.
- A replication of the compilation environment for their system.
- Advance notice of all design changes, patches, and modifications with subsequent delivery to us of the changed product.
- Access to their development facilities to provide us understanding of their development process.

We have been selected by the vendor and the telecom carrier as the trusted independent evaluator based on their evaluation of the efficacy of our process and the trustworthiness and qualifications of our personnel. Specific criteria used were:

- A comprehensive process with clear analytical and reporting criteria.
- Secure laboratory facilities suitable to protect the intellectual property of the vendor.Our facility is designed to Sensitive Compartmented Intelligence Facility specifications.
- The use of exclusively US personnel with Top Secret security clearances. Although the work is not classified, the use of cleared personnel assures that they have been fully vetted and found to be trustworthy.
- A staff fully qualified and equipped to perform the evaluations and effect trusted delivery.
- We are paid by the telecommunications company not the vendor.

The contracts in each case specifically provide for the direct, private communication between the evaluator and the stakeholders.

- The telecommunications carrier is, by contractual mandate, the primary benficiary of our work
- A condition of acceptance of the product is a report from us describing faults found, correction implemented and any residual risk.

- The evaluator may discuss any issues directly with the telecom and/or government agencies without notifying the vendor or providing the vendor the outcome of any such discussions.

In our labs, we subject the system to a detailed evaluation. The evaluation is designed to identify the existence of paths through which all known threats could compromise the system. The evaluation includes:

- Static and dynamic evaluation of the source code and software binaries.
- Evaluation of the vendor compilation environment and compilation scripts.
- Evaluation of the hardware components at the board and chip level. Hardware is evaluated to the level of detailed printed circuit board layout, discrete components and signal paths in and among circuit boards. Hardware is also characterized to the board and key component level, to enable the trusted delivery verification process. Dynamic testing of the system.

There have been thousands of defects found. In each case the vendor has been asked to explain the design purpose or other reason the condition exists, to include programmer error and to provide their intended fix. In this exchange, the vendor is not provided with a description of the specific test methodology applied by the evaluator, nor any unique information regarding what we might know about the relevant threat or how the vulnerability might be exploited. The vendor's response in consideration of the seriousness of the defect are used to make an evaluation of intent as malicious or not malicious. There have been no findings of malicious intent thus far. If there had been it would have been reported directly to the FBI. Once the fix is negotiated as adequate, the modified code is again subjected to a complete evaluation to insure that the defect was properly corrected and that no other defects were introduced.

Of significance is the value added operational benefits that accrue through this process. Operational efficiencies increase speed, agility, and baseline system performance. We produce for both the vendors and the telecommunication providers a system that has been rigorously tested and enhanced.

Once the system is deemed security suitable and acceptable for deployment by the telecommunications company we implement a trusted delivery process which includes the delivery of the software, firmware and hardware.

- The software is delivered directly from us to the telecommunications carrier via a secure network connection. Prior to delivery, it is compared against a record set of binaries compiled independently by us using evaluated source code. If the two software binaries match, the software is transmitted to the carrier. If problems are detected, the issues are resolved prior to delivery of the software to the carrier.

- The firm ware is generally delivered in a manner similar to the operating software, though it is often addressed through direct re-flashing of the boards by us after the devices have been delivered to the carrier or their trusted logistics provider.
- The hardware is subjected to a process of statistical sampling after delivery to the telecommunications company. The sample size is determined by the level of assurance required by the telecom. The telecom is then responsible for insuring the sample taken is truly random. A separate sample is taken for each shipment and each lot within a shipment. If upon comparison to the archived known evaluated board images. Ifa difference is found, the shipment is rejected.

Although none of the evaluated systems have yet been deployed, provisions have been made to conduct monitoring of special aspects of the system once it is running. This monitoring will be based on:

- Maintenance activities that despite all care might enable the introduction of malicious capability.
- Random scientifically based sampling to manage residual risks.
- Indications of specific activity either through normal monitoring or communication with government intelligence activities advising of additional threats and threat intent.

To date our EBSP has provided the ability to significantly improve the security posture of the affected telecommunications company at a very reasonable cost, when considered as a percent of the total cost of the system. The cost is down significantly after the initial evaluation. Costs are further mitigated by the improved performance of the system stemming from the removal of identified defects, security related or not.
By providing the recipient telecommunications company with the evidence to make an informed security decision, they are able to procure the best systems and benefit from a truly open competitive market environment.

I strongly recommend that the Evidence Based Security Process (ESBP) approach be integrated throughout the NIST Security Framework and other security policy and process initiatives across the government. Although not part of this discussion, it is a fact that our eighteen critical infrastructures rely on System Control and Data Acquisition (SCADA) systems as well as Industrial Control Systems(ICS) in which lack required levels of security. The broad use of independent and comprehensive evaluations of critical systems is the best opportunity to improve security at an affordable cost.