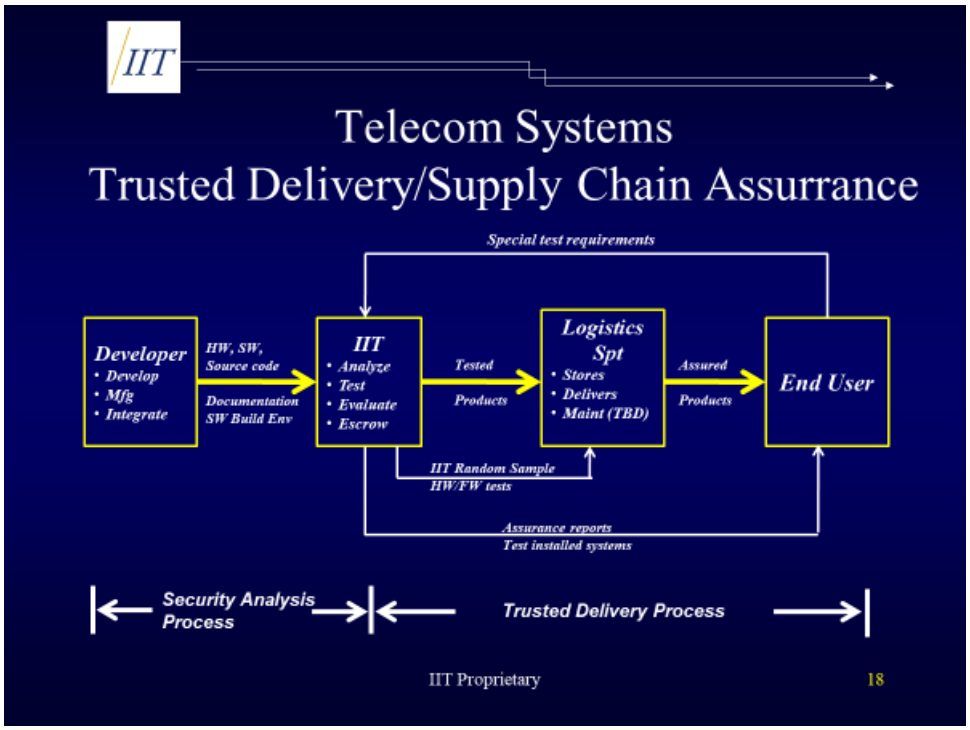
SOFTWARE, HARDWARE, & FIRMWARE ASSURANCE

INDEPENDENT HIGH ASSURANCE EVALUATION AND TRUSTED DELIVERY (HATD)



1. Introduction – Security and Operational Problem. For more than a decade there has a been an absolute consensus across US Government, Department of Defense, and the Private Sector Critical Infrastructures that more effective and comprehensive security evaluation methods are needed for advanced infrastructure technology solutions and key applications contemplated for deployment into telecommunications and information technology production networks. This is especially true for critical national telecommunications infrastructures, financial management and payment solutions, and the complex networks that control/manage freight rail and public transportation operations.

2. Independent Solution. The primary objective of a solution is to identify and mitigate security vulnerabilities and weaknesses *before* they become exposures that are exploitable by Advance Persistent Threat (APT) attackers. Of primary interest is the identification of vulnerabilities that

are not detectable by current security testing capabilities that are routinely and often vigorously applied to compiled software and firmware binaries that are present in operational networks.

For nearly the last decade, as a vendor neutral and independent company, Information and Infrastructure Technologies, Inc. (IIT) has worked closely with a Key Critical Telecommunications Infrastructure Stakeholder (a U.S. Tier 1 Carrier) and specific USG agencies to develop the policy framework and methodology required to implement a high impact, Independent High Assurance Evaluation and Trusted Delivery program (HATD). Initially, policies were created that required execution of this process for any technology contemplated for deployment into the carrier's production networks. IIT executes the actual deep evaluation of the technology solutions, including in-depth assessments of software/source code and hardware designs and implementations in US Government cleared laboratories with Top Secret and above vetted analysts and engineers. The assessments include:

- Static Analysis of Source Code. IIT conducts static analysis of all underlying source code. We use custom-configured versions of multiple industry standard automated tools. The custom configuration relates to adjusting the tools in a manner that assigns priority to identification of security relevant issues, though "code quality" data is also collected and mitigated. IIT also applies a number of internally developed tools to address high priority issues, such as embedded passwords and evidence of the existence of back-doors.
- Dynamic Analysis and System Level Testing. IIT conducts extensive system level testing in secure laboratory environments. This testing is "informed" by the source code analysis, allowing IIT to construct and execute tailored attack tools to confirm identified or suspected vulnerabilities as actual exposures.
- Hardware Analysis. IIT applies proprietary and advanced third party tools to fully evaluate hardware implementations to the board and component level. This effort includes deep analysis of hardware-enabled functionality to preclude the deployment of devices possessing undocumented and vulnerable features.
- Reporting. IIT reports all findings to both the developer and the end-user. Findings are coordinated with the developer/OEM to achieve effective mitigation solutions that are fully vetted when implemented.

For every new software release, IIT typically identifies hundreds, if not thousands (for large bodies of code) of embedded vulnerabilities that are completely invisible to conventional post-delivery/deployment security testing protocols. Many of the identified issues rise to the level of exposures that are often observed in reporting of "Zero-Day Vulnerabilities" that typically prove extremely damaging with very costly mitigation efforts being required.

IIT also couples a Trusted Delivery protocol/procedure with the evaluation effort. The goal of Trusted Delivery is to provide a meaningful guarantee to the end-user that that the technology presented for deployment into the production network exactly matches that which was evaluated in IIT laboratories. Upon receipt of production binaries from the OEM, IIT closely examines them and compares them against binaries independently compiled and evaluated by IIT. Once the binaries are validated by IIT, they are transmitted directly to the end user via a custom, secure process. This entire process generally only requires one to two hours. In general,

software binaries are never deployed directly to the end user by the OEM. A statistically significant sampling of hardware systems, where appropriate, are also validated by IIT using custom developed, proprietary tools. This solution dramatically impacts the security of relevant supply chain operations, fully precluding malicious or unexpected changes during shipment/delivery.

Additional realized benefits of the HATD Program are dramatic increases in operational efficiencies due to the identification and required deletion of forgotten and unnecessary source code. We continually witness four to ten fold increases in the speed of the evaluated software upon our recommended adjustments to the software.

3. Summary. The key features and benefits of the HATD methodology and program are:

- Comprehensive, standards-based assessment of software, firmware and hardware
- Fully independent process integrity with appropriate separations and no conflicts of interest
- Security-centric; not a Capability Maturity Model – based source code evaluation
- Threat oriented; integrates U.S. Government vetted intelligence threat reporting and assessments into the underlying target assurance cases and testing methods. It is not a generic set of "one size fits all" test processes
- Provides long-term, continuing assurance, when coupled with a customized trusted delivery process; Guarantees that only fully evaluated products are deployed into production infrastructures, removing the issue of possible malicious changes being effected after initial evaluation
- Integration into vendor patch and new release development processes, insuring that all software, hardware and firmware modifications are evaluated and isolated before deployment
- Isolates vendors from having any possible opportunity to effect unauthorized/unevaluated changes
- Provides continuous verification through pre-deployment checks and random field testing to guard against implementation of malicious attacks later in the supply chain or at actual production/operational sites
- Of note the costs for these efforts are borne by the vendor of the product vice the end user as a required element of the Request for Proposals (RFP) and Contract Award.

This methodology has been fully vetted and has delivered on the promise of dramatically raising the bar for the security of a U.S. national telecommunications infrastructure, as well as improving the performance of complex networked systems. As further validation of the merits of this process, the Committee on Foreign Investment in the United States (CFIUS) determined that this process fully mitigated validated national security threats related to significant foreign investment in a U.S. critical infrastructure entity, and mandated ongoing application of the methodology in a formal National Security Agreement.