MICRO FOCUS
Government Solutions

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

Software Security is National Security

Why the U.S. Must Replace Irresponsible Practices with a Culture of Institutionalized Security

April 2019

Link to Full Report

Executive Summary

Software development that does not incorporate comprehensive security throughout the lifecycle of the application jeopardizes national security by increasing the threat landscape surrounding high-value networks and sensitive data. The following problems were found to be systemic throughout the software development landscape:

- Current development prioritizes speed to market over security and relies on practices that shift liability and risk onto consumers. Security is an afterthought in the product development lifecycle.
- “Deploy now, patch later” has become standard operating procedure for most technology firms, resulting in applications known to be vulnerable to adversarial compromise at release.
- Open source solutions are popular; however, many are not secured against injected vulnerabilities or malicious compromise.

A cultural renaissance in secure software development is essential to national security. The following guidelines and frameworks were briefly explored as potential methodologies to introduce security throughout the application development lifecycle:

- NIST SP 800-37 / 800-53 / 800-64
- Motor Industry Software Reliability Association (MISRA) Guidelines
- CERT Secure Coding Initiative
- SAMATE
- OASIS SARIF
- Common Weakness Enumeration (CWE™)
- Security Technical Implementation Guides (STIGs)
- OWASP

The following actions should be taken to stymie negligent software development:

- Incorporate layered Security-by-Design at each stage of the development lifecycle
- Evaluate the quality of code through penetration testing and other debugging processes prior to release
- Institutionalize security during development through meaningful regulation and oversight similar to what is seen in the Health, Financial, and other sectors
- Recognize that secure software development does not stymie innovation and may result in more reliable, innovative, and efficient products

- Accept that security requirements are a necessary barrier of entry to market because they ensure that developers do not shift risk and liability onto consumers
- Dismiss the notion that security requirements are not scalable because numerous frameworks can be scaled to sector, purpose, and function for every piece of software
- Hold software developers and other stakeholders accountable when they knowingly release vulnerable code that was not developed with layered security throughout its lifecycle

By recognizing the factors contributing to the development of vulnerable software, following appropriate frameworks and heeding the proposed recommendations in this document, technology manufacturers can develop more secure applications that will ultimately reduce threats to our national security and improve critical infrastructure resiliency.