Ion Channel Response to Area 4 NIST & Executive Order Executive Order 14028 of May 12, 2021: Improving the Nation's Cybersecurity

This white paper is a response to **Area 4** of NIST's call for responses to Executive Order 14028: initial minimum requirements for testing software source code including defining types of manual or automated testing (such as code review tools, static and dynamic analysis, software composition tools and penetration testing, their recommended uses, best practices, and setting realistic expectations for security benefits, referencing EO sections 4(e)(iv and v) and 4(r).

One flaw and gap of both current practice and, implicitly, section 4(iv), which recommends automated tools or comparable process run regularly, or at a minimum prior to product, version, or update release is that this use of tools generates snapshot results which are not longitudinally registered to verify security responsiveness on the part of suppliers. While it is true that more snapshots are better than fewer snapshots - a daily scan gives vendors more live-state decision support for risk remediation than a monthly scan, and automated test in a build pipeline allows for better governance than post-build scans, even the most sophisticated static analyzers and software composition analysis tools provide no evidence of a supplier's security responsiveness per se. Code, if vulnerable, might be newly vulnerable - or those vulnerabilities may have been present in a product for years, during which time customer enterprises were exposed. Absent time as a dimension of risk - exposure time and remediation time - it is impossible to differentiate suppliers based on security responsiveness (e.g. Mean Time to Remediation) for supply chain risk, which is a proxy metric for engineering process maturity as well as an engineering culture that values maintenance vs. marketing and customer safety vs. customer capture.

Resilience as a first-order "ility" requires longitudinal audit not only of a software product or component's risk status, enabled by ongoing monitoring of an SBOM, but also of changes in that status over time. One enabling elements of leading-indicator risk detection in the software supply chain is derivation of patterns of life for software products and components: risky patterns of maintenance, end-of-life detection, change of control and compliance history in several dimensions of cyber diligence, including both known and potential vulnerabilities. The ability not only to detect a vulnerable component but to rank components, products and suppliers based on how long they have (or have not) been in compliance with customer security criteria allows customers to:

1. Quantify and reward security responsiveness and active maintenance that may incur the opportunity cost of that supplier's not getting as many new features out the door. The government says it's willing to pay for security, but without the hard math to rank suppliers based on security responsiveness, sales flash trumps active maintenance.
2. Automate verification of compliance with cyber terms and conditions, which in turn enables enforcement of security SLAs. Absent automated verification of time thresholds for responsiveness, enforcement of security SLAs requires manual audit, which is prohibitively time-intensive and expensive.
3. Inclusion of security responsiveness in analyses of alternatives and proposal evaluation matrixes, and preferential selection of security-responsive suppliers for either bid or award.
4. Higher security standards for active maintenance of software used in critical infrastructure, and competitive advantages for active maintainers providing software to both the public and private sector.

Submitted by:

JC Herz (female presenter): Co-chair, Department of Commerce (NTIA) multi-stakeholder working group on Software Transparency and Visiting Fellow at the National Security Institute, GMU Scalia Law School.

References:

JC Herz, "Maintenance: The Biggest Risks are Boring," internally funded case study: https://ionchannel.io/media/Ion%20Channel%20-%20Maintenance%20and%20Risk%20Management.v.2.pdf.

jc.herz@ionchannel.io, 202.213.3151, www.ionchannel.io

JC Herz, "A Plea to the Pentagon: Don't Sacrifice Resilience on the Altar of Innovation." Atlantic Council *New Atlanticist* blog, May 4, 2021. https://www.atlanticcouncil.org/blogs/new-atlanticist/a-plea-to-the-pentagon-dont-sacrifice-resilience-on-the-altar-of-innovation/