Information Technology Industry Council

January 17, 2014

Information Technology Industry Council (ITI)
Response to Assistant Secretary of Defense for Research and Engineering (ASD(R&E)
Request for Information for Software Assurance[1]
Solicitation # HQ0034RFIHQ027

ITI Point of Contact:

Danielle Kriz
Director, Global Cybersecurity Policy
Information Technology Industry Council
1101 K St. NW, Suite 610
Washington, DC 20005
dkriz@itic.org
p: 202-626-5731
m: 202-351-1661

[1] On January 6, 2014, ASD(R&E) provided ITI an additional week to provide these comments, allowing us to submit them by January 17, 2014. ITI appreciates this extension.

Introduction

The Information Technology Industry Council (ITI) appreciates the opportunity to respond to the Office of the Assistant Secretary of Defense for Research and Engineering (ASD(R&E))'s Request for Information (RFI) for Software Assurance. ITI is the premier voice, advocate, and thought leader in the United States for the information and communications technology (ICT) industry. ITI's 55 members[2] comprise the world's leading technology companies, with headquarters worldwide. Cybersecurity is rightly a priority for all governments. We share the goal with governments of improving cybersecurity and therefore our interests are fundamentally aligned. As both producers and users of cybersecurity products and services, ITI's members have extensive experience working with governments around the world on cybersecurity policy.

ITI supports ASD(R&E)'s focus on software assurance (SwA). Software security—and IT product security generally—is critical to ITI companies because we must be responsive and transparent to a global customer base, which includes the defense enterprise. Security is important to our customers who use software to process critical information and to manage critical business processes. Commercial-off-the-shelf (COTS) software developers, including ITI companies, make major investments in processes and tools used to improve the security of software they produce. As such, we would like to offer the following thoughts about the approach you should take in your pre-solicitation discovery efforts.

Further, as you advance this solicitation toward the pre-RFP and RFP phases and you further refine the requirements and evaluation criteria to be used, we would offer that the final request for proposals can only be improved through continued open dialogue with both individual and collective industry organizations. We would request that you foster and encourage such engagement. We would further encourage and support the convening of public meeting opportunities as indicated in the RFI.

Improving SwA should avoid mandates for one-size-fits-all tool or standard

We wish to reframe an underlying assumption in the RFI on which some of its questions are based: that automated vulnerability detection tools gauged to a common standard for effectiveness are the answer to improving SwA. While coding standards and tools are important elements of a secure development process (coding standards help developers use programming languages in safe ways, and tools can automatically detect deviations from those standards and tell the developers to correct them), there is no one-size-fits-all standard or tool. Tools are an important element of a secure development process and many COTS vendors use static analysis and "fuzz testing" tools. However, because organizations use different programming languages, compilers, operating system platforms and versions, and build software for different purposes, coding standards and tools must vary among organizations. We must also recognize that tools actually hinder rather than help addressing certain coding issues, in particular by flagging too many 'false positives'. In fact, when using tools is appropriate, vendors use a variety of different tools, often more than one, and some companies use "home grown" tools or tool extensions. Regardless of the tool or tools used, every company has to "tune" or tailor them to find real software vulnerabilities while minimizing the number of "false positives" that the tools emit.

[2] See attached ITI member list.

These practices (such as tuning or extending the tools) are required because each developer has a different code base with different technical attributes.

In fact, DoD-mandated one-size-fits-all for secure coding tools and standards would have a number of downsides.

First, they would likely decrease SwA. If procurement requirements mandated the use of specific tools, some highly effective tools would likely not be on the "qualified" list while inappropriate or ineffective tools would be. As a result, developers would still have to use their own tools, tuning, and extensions – in spite of an incentive not to - to improve security, and also run the "qualified" tools and then manage the increased number of false positives they produce – which will incur more cost, divert scarce security resources—in particular expert personnel, which is one of the least abundant security resources—and extend product cycles. Developers would spend time recoding to the coding standard instead of improving the real security of their software. And this assumes that the mandated approaches are even compatible with the programming languages and software development methods used by a given vendor.

Secondly, such an approach would be incompatible with the federal government's longstanding policy to purchase affordable, innovative, and interoperable COTS technologies. Any requirements to use particular tools or standards would require companies to undertake extraordinarily large resource commitments and product customization for government customers and would be better suited for application and use with DoD-specific modifications to COTS products. Greater reliance on these customized products will result in higher costs, limited interoperability, less access to innovation, and fewer IT suppliers available to the government. These requirements on software development also would be incredibly burdensome to industry, ultimately translating into fewer resources companies can devote to cybersecurity research and development (R&D). In short, this type of mandate could have the opposite intended effect and lead to weaker security for the federal government.

Finally, a mandate to use a particular tool or standard could unintentionally impede U.S. ICT companies' ability to compete in the global marketplace and lead to the balkanization of the Internet. Efforts to improve cybersecurity must take into account the global nature of cyberspace. Any approach the United States takes will be watched carefully, and perhaps emulated, by governments around the world. If foreign governments are empowered to similarly dictate particular coding tools and standards on U.S. companies as a condition to sell to their government markets, not only could the Internet's global interoperability and security be undercut, but our companies may lose market share and, ultimately, cutting-edge U.S. jobs.

Recommended alternative approaches for improving SwA

Assured software results when the developer follows a process that is designed to produce assured software. Many COTS vendors apply such processes, and their collective experience shows that these processes result in fewer vulnerabilities and reduced severity and increased difficulty of exploitation of the vulnerabilities that remain. The industry group Software Assurance Forum for Excellence in Code (SAFECode) has documented collective processes,

although other COTS vendors also apply software development processes tailored to their specific technologies and product offerings.

In lieu of mandating a specific tool or standard, we suggest DoD do the following to improve SwA related to its own procurements.

Follow a technology-neutral and vendor-agnostic approach. We urge DoD to ensure that any new requirements for SwA be technology-, method- and vendor-neutral. While it is acceptable for procurement policies to specify security objectives (e.g. the use of a process for minimizing the occurrence of coding errors), the decisions regarding how to meet those objectives (such as what tools, processes, methods or standards to use) must be left up to the vendor that would like to sell to a government entity. This will ensure that no specific approach—including an automated vulnerability detection tool—is wrongly consecrated as a requirement, and instead that software developers can focus on selecting tools and other measures among a continuously evolving panoply of competing solutions. This also will preserve and promote our industry's ability to innovate, which is critical to ensuring that our industry remains globally competitive—further strengthening SwA and cybersecurity generally.

Avoid any new standards. In its RFI, DoD asks about creating and maintaining standards (p. 3). DoD should not attempt to develop its own independent set of SwA standards. As noted above, this could embolden other countries to similarly develop and mandate new country-specific standards. Instead, should the Department wish to identify compliance with a standard or standards as one means of demonstration of compliance for evaluation purposes, it should focus on using consensus-based international standards and ensure that those standards will be uniformly accepted across the user community and not intermittently accepted for use and application. Among such standards, we recommend DoD look to the Common Criteria (CC)/ISO 15408 to address its SwA interests. CC is the existing international standard on product assurance and integrity, is already required for federal acquisitions of National Security Systems, and has been recognized by 26 countries under a multinational agreement called the Common Criteria Recognition Arrangement (CCRA), indicating broad global acceptance. Current CC reform activities include efforts to add SwA interests in the CC, efforts that DoD should support. Further, because the U.S. Government is represented by the National Security Agency/National Information Assurance Partnership (NIAP) in the CCRA and is recognized as one of its de facto leaders, DoD has an important stake in this standard (and many of DoD's major IT COTS vendors are active supporters of NIAP's efforts to continuously improve the CC).

Avoid new government-run certification or testing regimes. In its RFI, DoD asks about creating and maintaining a certification process (p. 3). DoD should not create a new government-run certification and security testing regime as part of any new acquisition requirements. Many ICT providers adopt security practices and have a variety of methods of conveying those practices to their customers. These may range from attestation, to having products certified against global standards, to having their processes accredited against global standards. Not only would new government-run regimes be redundant with these processes, but they would likely add cost and bureaucracy with no demonstrable impact on security. To the extent that certifications or accreditations are to be required, they should only be to existing global certification or accreditation regimes already used by industry to attest to global standards.

Continuing to rely on existing, market-driven global conformity assessments related to cybersecurity risk management has key benefits:

- It allows for the conformance assessment industry to move at a pace more closely tied to the pace at which threats develop and at which industry designs, develops and implements solutions that respond to these threats.
- There are standards for how to appropriately conduct conformity assessment that are based on global consensus and are globally deployed.

Rather than developing a new conformity-assessment scheme, we recommend that DoD seek an approach that allows for company attestation/ evidence of their security assurance practices in conformance to global standards, or to their products' conformance to global assurance standards. This would focus on reasonable accountability and how companies can demonstrate accountability.

Reform DoD procurement processes by weighting SwA appropriately in contracting.
Currently, many federal procurements give disproportionate weight to factors such as cost, schedule, supplier diversity, or other factors. In fact, some procurement officials are rewarded based on how much money they save their agency, not on whether the ICT procurements increase the agency's security. If contracting officers are making decisions based on getting the lowest price, there is a chance the products they procure will not have the security features or functions needed for the system or application in which they will be used. Security (including SwA processes) should be adequately weighted as a factor in a "successful" procurement so that decisions are not driven by other factors at the security's expense.

Conclusion

ITI and its member companies strongly support DoD's efforts to improve SwA. We understand DoD seeks greater assurance regarding the security and quality of software it procures. The objectives of these efforts can be best achieved by leveraging the existing processes used by global COTS developers.

Innovation.
Insight.
Influence.

member companies