Response to NIST RFI "Information on Current and Future States of Cybersecurity in the Digital Economy"

John Pescatore
Director, Emerging Security Trends
SANS Institute
Bethesda, MD
jpescatore@sans.org

Summary

In the subject Request for Information, the Commission on Enhancing National Cybersecurity requested information about current and future states of cybersecurity in the digital economy. The comments in this response are focused on items 2 and 4 from the following section in the RFI:

The Commission also seeks input on the following:

1. Emerging technology trends and innovations; the effect these technology trends and innovations will have on the digital economy; and the effect these technology trends and innovations will have on cybersecurity.

2. Economic and other incentives for enhancing cybersecurity.

3. Government-private sector coordination and cooperation on cybersecurity.

4. The role(s) of the government in enhancing cybersecurity for the private sector.

5. Performance measures for national-level cybersecurity policies; and related near-term and long-term goals.

6. Complexity of cybersecurity terminology and potential approaches to resolve, including common lexicons.

The topic area I am focusing on **is increasing the security of the software and services the government buys.** There are well proven ways the government procurement process can require software and online services vendors to demonstrate due diligence levels of security in their offerings. This will serve to increase the security of government systems, but Federal purchasing power will also help drive the overall level of security in the commercial market to higher levels.

High level take-away – Require all government procurements of software (including embedded software) and online services to include **as a minimum a clause requiring the offeror to provide evidence that commercially available application vulnerability testing tool was used to demonstrate that no known vulnerabilities are present in the product at sale**.

The appendix below shows some examples of where this approach is in use at the National Credit Union Administration and the Department of Homeland Security, as well as suggested clauses by a commercial tool vendor (Veracode) and the non-profit Open Web Application Security Project. If the OPM and /or GSA were to support, expand and require this approach across all government procurements, the

number of vulnerabilities available for attackers to exploit would be dramatically reduced. Essentially, the government would be requiring software quality and safety as part of acceptance criteria.

Beyond this simple first step, there are additional requirements around the maturity and security-focus of software development processes that could be required, but that process-centric approach has been tried in the past and does not work without first requiring a simple, achievable level of software quality and safety.

John Pescatore

SANS, Director Emerging Security Trends.

APPENDIX/REFERENCE INFORMATION

Examples from existing Application Security contract language guides:

Veracode "*Recommended Secure Software Purchasing Contract Language*":

3. SECURITY REVIEWS

(a) Independent Review
Vendor shall have their software reviewed for security flaws, in binary format (i.e. compiled or byte code; source code is not required), by an independent organization that specializes in application security, at their expense, prior to delivery to the Client.

(b) Review Coverage
Security reviews shall cover all aspects of the software delivered, including third party components, and libraries.

(c) Scope of Review
At a minimum, the review shall cover common software vulnerabilities. The review may include a combination of static analysis of the binary code, dynamic web application vulnerability scanning, and manual penetration testing.

…

(e) Standard Benchmarks
To ensure that all parties have a common understanding of any security issues uncovered, the independent organization that specializes in application security shall provide a rating based on industry standards as defined by First's Common Vulnerability Scoring System (CVSS) and Mitre's Common Weakness Enumeration (CWE).

(f) Review Frequency
Reviews shall be conducted to revalidate the software prior to delivery of any new major or minor release prior to delivery to Client.

OCC/NCUA "INFORMATION SYSTEMS & TECHNOLOGY APPLICATION SECURITY"

Does the vendor have an industry-recognized third party who conducts application vulnerability assessments on the applications, including security? If so, credit union management should before purchase or during the RFI/RFP process:

- obtain the third party's name,
- determine how often the assessment is conducted,
- determine the date of the last assessment,
- secure a copy of the most recent assessment, if possible,
- determine whether the application has any known open vulnerabilities,
- determine the nature of the vulnerabilities, and

- determine if the vendor is willing to share its secure coding processes and practices.

...

- Where appropriate, management should include in the contract language the need for current and ongoing application vulnerability assessments, including security, and who will conduct the assessments. Depending on the risk profile of the application, management may request the full vulnerability assessment report or a summary.

DHS/US CERT “Software Assurance in Acquisition and Contract Language”

The SwA SMEs should review each software deliverable and analyze test results produced by the contractor or independent tester to ensure that SwA requirements are met.

OWASP Secure Software Contract Annex

(e) Security Analysis and Testing

Developer will perform application security analysis and testing (also called "verification") according to the verification requirements of an agreed-upon standard (such as the OWASP Application Security Verification Standard (ASVS)). The Developer shall document verification findings according to the reporting requirements of the standard. The Developer shall provide the verification findings to Client.