This Position Paper is in response to the NIST Call for Position Papers related to US Executive Order 14028: Improving the Nation's Cybersecurity, that focuses on the process and technology of cyber security checks within software development environments. Specifically area 4: Initial minimum requirements for testing software source code.

It is welcomed that the Executive Order addresses the act of using automated tooling to check software prior to release of the software product, as described in Section 4 (e) (iv):

> *employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update release;*

This position paper highlights areas of concern of the effectiveness of the current wording of this statement in reducing risk to the US Government, whilst providing insights which would help ensure automated tool checks and processes create the desired change. The relevance of this position paper draws to the intention of the Executive Order to have a meaningful effect on increasing the security of software products. Adherence to the text of this portion of the order may allow compliance that does little to reduce the risk of such software, yet may provide unwarranted confidence in that software, which represents a dangerous position.

Most of the software industry does not currently implement a process of running automated tools before software release. Those that do have achieved this state at the expense of technical and process lessons learned, and the cost of significant internal development. This paper wishes to draw attention to these lessons and challenges, such that the software industry can accelerate the time needed to meet the spirit of this Executive Order and reduce the risk of developed software.

Quality

The first aspect of consideration is the scope of security checks provided by automated tools employed. All tools have a limited scope of security checks they can perform. Research of the NIST 800-53 "Security and Privacy Controls for Information Systems and Organizations"[1] shows a majority of security checks, 623 (61.9% of the total 1007), that would be considered procedural and thus would be assured through manual process review. For the remaining 284 (38.1% of the total 1007) checks in NIST 800-53 that would be in scope to be performed on software, analysis indicates 181 could be detected by some form of automated security check[2].

Similar research on the highly technical OWASP ASVS[3] (Open Web Application Security Project Advanced Security Verification Standard) shows 240 checks (80.8% of total) would be detected by some form of automated security check. The 240 automatable checks from OWASP ASVS, and the 181 automatable checks in NIST 800-53, represents a high number of checks that could be applied to software before release.

It should not be assumed that any single security tool will provide even a majority of protection checks. Research of tools shows varying coverage; tool 'Bandit' covers 16 checks (6.7% of automatable OWASP checks (AOC)); OWASP ZAP covers 46 checks (19.2% of AOC), SonarQube covers 31 checks (12.9% of AOC)[4]. A software development environment employing just one of these tools may be adhering to the letter of the Executive Order without providing adequate protection.

Combining automated security tools will increase the scope of checks. Research of combining five security tools increases the coverage to 87 checks (36.3% of AOC). Hence a need for the effective coverage of automatable security tools employed is a factor to be considered.

The second aspect is the ability for automated security tools to check for technical security issue categories that tend to be specific to the software being tested. Research into the NIST and OWASP standards we have mentioned indicates around 50% of 'automatable' checks would require some form of customization, and thus would not be feasibly checked by an 'off-the-shelf' security tool. Examples include business logic, or authorization checks that are specific to the software in question, and thus simply not feasible to appear in

[1] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[2] This research can be provided on request.
[3] https://owasp.org/www-pdf-archive/OWASP_Application_Security_Verification_Standard_4.0-en.pdf
[4] This research can be provided on request.

generic security tooling. A software development environment would therefore achieve less than half of their automatable checks if solely relied upon commercial or open-source automated security checks.

Typically, these 'software specific' security checks would be conducted manually by penetration testing. However, many organisations will create their own 'custom' automated checks for these types of issues. Consideration must then be given to the application of custom developed security checks, in combination with off-the-shelf security tooling. Otherwise, the quality of coverage of automated security checks will leave a sizable scope for undetected security vulnerabilities, and not serve the intended purpose of reducing the risk.

Risk Based Approach

The Executive Order simply cites remediation of vulnerabilities before release, which indicates all issues must be remediated. Requiring the fixing of potential vulnerabilities which do not pose an actual risk would slow down the speed of development releases and increase costs. NIST has acknowledged the benefits of cyber value-at-risk approaches such as those prescribed by the FAIR Institute[5] as methods of evaluating the likelihood and impact of a vulnerability. In the event that a risk-based approach was used to prescribe some measure of risk was communicated to the purchaser, then risk-based decisions can be made by the purchaser.

Development Velocity & Process

Modern software development practices, such as 'DevOps' and 'CI/CD', have greatly increased the speed of software releases, to the point where software changes are created and released within hours. The Executive Order asks that security checks and fixes are applied "regularly, or at a minimum prior to product, version, or update release", which is correct and required to reduce the risk of vulnerabilities from being exploited.

Integrating automated security tools into modern software development practices has been a challenge for many software environments due to issues with the automation of surrounding processes. Challenges such as handling the large number of vulnerabilities, including false positive and duplicate issues, presents a challenge at the point of build and release. Anecdotally, many companies have experienced failures when introducing the automation of security tools into their technical processes, only for the security findings to not be viewed or processed, resulting in no improvement in the risk posture of the developed software. This has been evidenced by Facebook[6] where a near 0% fix rate was seen when automated security checks were applied after release, compared to a 70% fix rate for the same automated security checks applied before release.

With modern software development practices being so fast paced, the introduction of any manual security step quickly becomes unmanageable. The speed and scale mean that manual tasks will create a bottleneck in any security process. Therefore, it is advised that discussions of 'comparable processes' allow for automated handling of the fuller security process related to the handling of security issues identified by automated security tools, and any analysis or decision making necessary before the release of the affected software.

Summary

Advisories arising from this Executive Order and NIST workshop would benefit from inclusion of aspects that not only ensure "automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update release", but to further ensure:

1. The automated tools and checks are of sufficient quality and scope as to provide the expected level of protection.
2. The process of applying these checks is also automated (as far as possible) to allow the process to be effective in reducing risk before release and remove the temptation to bypass the security process.

[5] https://www.fairinstitute.org/blog/nist-maps-fair-to-the-csf-big-step-forward-in-acceptance-of-cyber-risk-quantification

[6] https://cacm.acm.org/magazines/2019/8/238344-scaling-static-analyses-at-facebook/fulltext