Carnegie Mellon University
Software Engineering Institute

CERT/CC Comments on Standards and Guidelines to Enhance Software Supply Chain Security (Question 1, designating “critical software”)[1]

Corresponding author: Art Manion <amanion@cert.org>

Deployment methods and infrastructure

Federal systems are a combination of acquired software and services on diverse infrastructure, including

- Software acquired for deployment on government hardware (e.g., desktop operating systems)
- Software acquired for deployment on service provider hardware (e.g., hosted servers)
- Software used as part of a service purchased by the government (e.g., software-as-a-service)

Software security risks are posed by vulnerabilities rather than the method of deployment. Therefore, policy for designating *critical software* should be consistent regardless of deployment method. More concretely, minimize gaps between this policy effort and those applicable to FedRAMP systems.

Context is king

Software and its context of use are inseparable for the purposes of determining the “critical” designation. The designation should not be based only on proximate technical features of the software. Consider OpenSSH, which accepts untrusted network traffic, handles authentication, and relies on cryptography.[2] These features map to the E.O. guidance about “...level of privilege or access required to function, ... direct access to networking and computing resources, [and] performance of a function critical to trust.” OpenSSH implies some degree of context by its design: the use case of secure remote access. However, the criticality of OpenSSH must be considered in context. A hobbyist web server hosting cat pictures and a nuclear power plant have different “...potential for harm if compromised,” even if both use OpenSSH.

A complex definition for a complex concept

A static dictionary entry will not adequately capture the complexity of the term “critical software.” Similarly, we do not expect that a master list of critical software will be effective. Instead, we suggest that NIST develop a mechanism to designate software as critical or not. This mechanism *is* the definition. Designators need a transparent, reliable, repeatable, and explainable mechanism.

Decision trees are best suited to meet these design requirements. The Stakeholder-Specific Vulnerability Categorization (SSVC) was designed for prioritization decisions during vulnerability management.[3] We suggest an adaptation of the concepts in SSVC to account for the criteria in the E.O. The methods developed in SSVC are appropriate because the E.O. is also making a prioritization decision. Table 1 maps guidance from the E.O. to SSVC features.

The decision tree in Figure 1 suggests how to designate critical software. We encourage NIST to treat software and its context together in a decision tree with appropriate features. The tree can and should be modified as necessary.[4] Figure 1 uses the more coarse Public Safety Impact and Mission Prevalence.[5] These are effective when the designator has coarse visibility into mission and safety context.

[1] https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/workshop-and-call-position-papers
[2] https://datatracker.ietf.org/doc/html/rfc4251
[3] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=653459
[4] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=653459 pg 36.
[5] For example, Mission Prevalence could be measured by the Core Infrastructure Initiative Census Program II https://www.coreinfrastructure.org/programs/census-program-ii/

E.O. Criteria	SSVC Features
“level of privilege or access required to function” “integration and dependencies with other software” “direct access to networking and computing resources”	Value Density (value to adversary of compromising the system) System Exposure
“performance of a function critical to trust"	Public Safety Impact (based on FAA and CDC guidance) Situated Safety Impact
“potential for harm if compromised”	Mission Impact (based on FEMA[6] guidance) Mission Prevalence

Table 1: Mapping E.O. criteria to SSVC features

Who designates

In most cases, agencies have the expertise, knowledge and resources to provide the necessary context to the decision process. We suggest that agencies should have the authority and responsibility to use the definition to make the initial designation. For example, the “Categorize” step in RMF[7] outputs a security categorization of the system. NIST SP 800-60[8] provides guidance for mapping systems to security categories. This guidance should be updated to incorporate the “critical software” definition. An oversight function could monitor and review designations (both critical and non-critical). Such a function would have the necessary perspective to notice trends or otherwise make changes to initial designations.

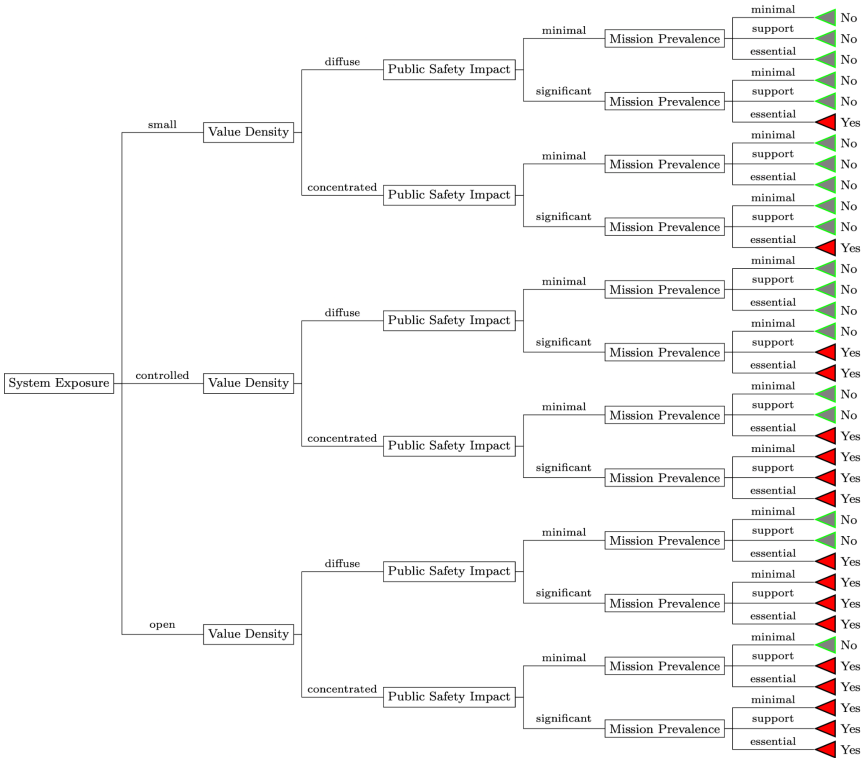

Figure 1: Suggested decision tree definition of how to designate “critical” software

(Repeated on page 3)

[6] https://www.fema.gov/media-library-data/1499702987348-c8eb5e5746bfc5a7a3cb954039df7fc2/FCD-2June132017.pdf
[7] https://csrc.nist.gov/projects/risk-management/about-rmf/categorize-step
[8] NIST SP 800-60 volumes 1 and 2, https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final and https://csrc.nist.gov/publications/detail/sp/800-60/vol-2-rev-1/final

Figure 1: Suggested decision tree definition of how to designate "critical" software