Pacific Northwest National Laboratory

Advancing scientific discovery and delivering solutions for sustainable energy and national security

Pacific Northwest NATIONAL LABORATORY

National Institute of Standards and Technology
U.S. Department of Commerce
1401 Constitution Ave NW Washington, DC 20230

Subject: Comment of Pacific Northwest National Laboratory RE: NIST Workshop and Call for Position Papers on Standards and Guidelines to Enhance Software Supply Chain Security

---

Pacific Northwest National Laboratory (PNNL), managed by Battelle for the U.S. Department of Energy, advances the frontiers of knowledge, taking on some of the world's greatest science and technology challenges. For over two decades, PNNL has advanced resilient cyber capabilities to thwart adversaries seeking to infiltrate and damage our national security through digital means. Working in partnership with government agencies and industry, we deliver unique solutions to protect critical strategic assets. Heavily rooted in a scientific perspective, our methodologies, algorithms, and tools enable stronger, more resilient technologies and systems to analyze threats and understand, predict, and control complex adaptive systems. We leverage expertise in information assurance, computer network defense operations and development, system architectures and integration, mission assurance and resilience, assessments and evaluations, and software development.

PNNL has extensive experience assessing, auditing, and mitigating software supply chain resilience. As one of the nation's leading labs in cybersecurity, PNNL conducts research for a variety of sponsors, including DOE, DHS, DOD and the intelligence community. PNNL leverages these capabilities to benefit DOE in two areas: the Cybersecurity Risk and Information Sharing Program (CRISP) to assist utilities with grid security; and the Cooperative Protection Program (CPP) to provide real time cyber monitoring across the DOE enterprise. In supply chain risk management, we currently support the US Air Force Space and Missile Systems Center, the DOE Office of Cybersecurity, Energy Security, and Emergency Response, and the NNSA Tritium Production efforts. Our current research and development efforts are focused on understanding, evaluating, and developing trusted systems for critical infrastructure.

PNNL Position:
(2) Initial list of secure software development lifecycle standards, best practices, and other guidelines acceptable for the development of software for purchase by the federal government. This list of standards shall include criteria and required information for attestation of conformity by developers and suppliers. See EO Section 4(e)(i, ii, ix, and x).

There are several standards, tools, and techniques (ST2) for ensuring security in different parts of the software design lifecycle. These include a range of NIST and IEEE standards (notably including the 800 series and 12207), an even broader range of commercial tools, and several best practices or polices which are intended to ensure the correct application of the standards and policies. These various ST2 are available for the majority of the lifecycle of software, including both pre-release and during use. It is our position that new ST2 are not required at this time, but rather what is required is threefold:

1. We must be able to provide direct recommendations for applications or usage of the ST2. The guidance available is often designed for a specific technical expert, but due to the severe lack of supply chain/software/ cybersecurity experts, less-expert individuals are often responsible for implementation.

2. We must connect the standards that already exist. One standard may cover a certain portion of the lifecycle, but not another and it is inapt to assume that any single person knows all the standards well

enough to know when is more applicable than another and to what point. A consolidated standard would enable users to more effectively apply the ST2 which do exist.

3. We must connect the actors that exist. Research performed at PNNL has shown that while there are largely sufficient standards for specific portions of the software lifecycle, there are gaps in the areas between actors. The manufacturer may be following one standard or performing one type of testing, but they are not them communicating with the end user those standards or results, and not assisting the end user with verification and validation regarding the end software product.

4. These ST2 must also interface with the human education and training components of security as well as the hardware upon which it will be implemented. Software is neither designed nor used in a vacuum; to ensure secure software, it is also critical to ensure that connection points with the hardware system the software operates on and the human system which uses the software are well-designed and secure.

5. Of especial concern is the secure supply chain for operational technology products, including those which control our power grid, oil and natural gas pipelines, and water treatment plants. The software we use to run our daily lives (operating systems, text editors, etc) are critical and can provide weak points which lead to entry into our networks. However, of especial concern and focus should be the software that runs in operational environments; the mis-operation of this software could cause a loss of life.

PNNL has been exploring and mapping the ST2 based around operational systems for many years. If the workshop organizers would be interested, we can also provide supplementary information such as Secure Design and Development Principles for Operational Technology Systems (PNNL PACIFIC Agile Investment Technical Report); ST2 Mapping (PNNL VARS Technical Report); and several other relevant documents.

Please direct any questions to jess.smith@pnnl.gov or david.manz@pnnl.gov.

If requested, we would be happy to present this position and its supplementary information. The coordinating author will be:

Jess Smith, PhD
Jess.Smith@PNNL.gov
509 372 4213