2-Year Interagency Initiative Aims to Define and Integrate Secure Systems Engineering

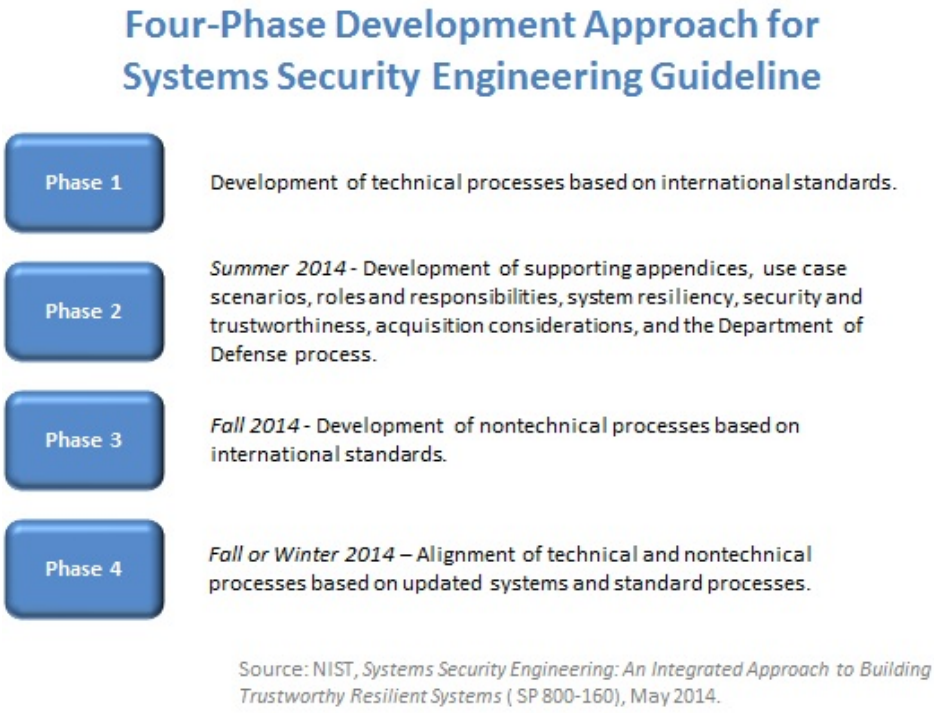
Posted At : May 27, 2014 3:26 PM | Posted By : Kyra Fussell

Related Categories: Critical Infrastructure Protection, Information Security, Cybersecurity, Department of Commerce

Mid May 2014, the National Institute for Standards and Technology (NIST) released an initial public draft of guidance for secure systems engineering. The document is part of NIST's 800 series of special publications, which provide computer security resources.

According to NIST fellow Ron Ross, "We need to have the same confidence in the trustworthiness of our IT products and systems that we have in the bridges we drive across or the airplanes we fly in." To that end, computer security experts are working to incorporate security into IT systems through systems and software engineering principles. An initial set of guidelines has been released by NIST for public comment in the draft document ***Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems***. The ultimate objective, as the document puts it, is "to address security issues from a stakeholder requirements and protection needs perspective and to use established organizational processes to ensure that such requirements and needs are addressed early in and throughout the life cycle of the system."

The process for developing the guidance has four stages. The phased approach of the initiative will allow the numerous stakeholders to focus their review and feedback on key elements of the engineering process as different parts of the guidance are developed. The current draft is part of the first stage of the guidance development process.



Source: NIST, *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems* (SP 800-160), May 2014.

The secure systems engineering guidance produced by this process is intended to be applied to both public and private systems, including financial systems, critical infrastructure, and defense systems. Building on the federal cyber security strategy and information security efforts, the detailed guidelines pursue an objective of reducing the susceptibility of systems to threats. Taking a systems engineering approach allows security to be addressed at every stage of the lifecycle for new systems, upgrades, modifications, planned upgrades that result in a new system, systems-of-systems, and retiring systems.

Although security professionals are the primary target audience for the publication, the information may be of use to a range of roles throughout the system lifecycle. Specific examples of such roles include those with risk management or oversight responsibilities, acquisition and budgeting roles, systems design and integration roles, auditing and monitoring roles, as well as providers of products, systems, or services. The 120 page draft document is available for review at **http://csrc.nist.gov/publications/PubsDrafts.html#800-160**. Public comments may be submitted to **sec-cert@nist.gov** through July 11, 2014.

---

*Originally published for Federal Industry Analysis: Analysts Perspectives Blog. Stay ahead of the competition by discovering more about **GovWinIQ**. Follow me on twitter **@FIAGovWin**.*