Developing a Framework to Improve Critical Infrastructure Cybersecurity

Comments Submitted by RedSeal Networks of Santa Clara, CA in Response to the February 26, 2013 Request for Information Noticed by the National Institute of Standards and Technology (NIST):

Contact: Parveen Jain, President and CEO, RedSeal Networks, parveen@redsealnetworks.com

The consideration of standards relative to cyber security tends to focus almost immediately on whether they should be voluntary or mandatory, and whether they should be developed by the private sector or mandated by government. Too little time is spent on the question of compliance and how that can best be measured. No matter how standards are set, and no matter how owners and operators of elements of critical infrastructure and other entities are incentivized to adopt them, standards do not make a demonstrable contribution to network security unless compliance with them can be assured.

Until 2010, at least in the federal government, compliance was typically measured by infrequent manual audits which, particularly on complex networks, were both difficult to administer and costly. Most importantly from a security standpoint, they were of limited utility because they could measure compliance only in the "snapshot" in time in which they were administered, a result at odds with the constantly changing nature of modern, interconnected networks. In 2010, the Office of Management and Budget (OMB) issued new guidance to federal agencies on reporting requirements under the Federal Information Security Management Act of 2002 (FISMA). FISMA requires that federal agencies report annually on the security status of their information systems. The OMB guidance of 2010 encouraged a move away from reliance on the "snapshot" approach to compliance assessment, and toward a process in which actual audits are supplemented and reinforced by a system of continuous monitoring.

NIST Special Publication 800-37 defines Information security continuous monitoring as: "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions." That definition is further clarified in NIST Special Publication 800-137 thusly: " the terms 'continuous' and 'ongoing' in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information." Under this definition, monitoring at widely varying periods of time measured in months, weeks, days, or minutes could be regarded as a sufficient frequency, and therefore as "continuous".

Developing a Framework to Improve Critical Infrastructure Cybersecurity

The advantages of continuous monitoring are clear. By providing an up to date security status, continuous monitoring enables organizations to make cost-effective and risk-based decisions about their information systems. Continuous monitoring offers an additional layer of oversight over the existing security architecture that can attest to the effectiveness of internal controls. In addition to assuring the optimized effectiveness of security technologies, there is a greatly lessened workload on IT departments when an actual audit approaches, because proof of compliance with required standards and regulations is available through an historical record of change control and validation.

RedSeal Networks believes, therefore, that any framework for standards setting on cyber security must include a requirement for continuous monitoring. Given the increasing complexity of networks, the rapidity with which they change in size and composition, and the ever-increasing sophistication of cyber- attacks, RedSeal Networks also believes that the term "continuous monitoring" should be defined in such a way as to underscore the values of constancy and speed. The worth of near real-time reporting in this context is inescapable. Transactions and controls must be monitored constantly if the best possible risk based assessments of the effectiveness of compliance methods are to be made. A proactive approach to network security requires not only investments in the means by which to meet standards and regulations, but an ability to validate that compliance with those standards and regulations is being maintained continuously. If continuous monitoring is to be a tenet of network security, then the term must be understood to apply literally; that is, it must mean that surveillance and risk assessment of the network is done on a constant basis.

As NIST considers the methodologies, procedures, and processes which should compose the Framework, RedSeal Networks urges that a requirement for compliance validation through constant network monitoring and risk assessment be included.