Understanding the NIST Cybersecurity Self-Assessment Tool

By: Scott Geye, CISSP, CISA

In George Washington's first annual message to Congress as President of the United States, he stated that "Uniformity in the currency, weights, and measures of the United States is an object of great importance, and will, I am persuaded, be duly attended to". Eventually, the Office of Standard Weights and Measures was established under the Department of the Treasury to manage these standards. In 1901 the National Bureau of Standards was established to take over this responsibility, and also served as the national physical laboratory. Under Herbert Hoover's direction, the Bureau began developing commercial standards for materials and products, including quality standards. During World War I and II the Bureau took on a research and development role for a variety of technology and production issues. In 1988, The National Bureau of Standards was renamed the National Institute of Standards and Technology. Now NIST leads research initiatives across a variety of spectrums, in addition to developing and maintaining numerous critical standards and publications.

The National Institute of Standards and Technology ("NIST") publishing standards and guidance on information security since 1977. The NIST information security guidance is used by organizations that have the highest level of requirements when it comes to information security, such as the Department of Defense. The NIST Special Publication ("SP") 800 series provide comprehensive guidance for the implementation, governance, and maintenance of an information security management framework, including detailed guidance on many subcomponents. The NIST publications cover more topics than can be mentioned here. Suffice it to say that just about every other information security framework is merely a subset of what NIST covers, and that is especially true when compared to compliance frameworks such as Health Insurance Portability and Accountability Act ("HIPAA"), Payment Card Industry Data Security Standard ("PCI-DSS"), or Sarbanes-Oxley ("SOX").

NIST *SP 800-30 Guide for Conducting Risk Assessments* and *SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations* provide valuable guidance for performing an information security risk assessment and selecting the appropriate controls to implement to mitigate those risks. However, to those outside of government agencies or other very large organizations, the processes laid out in these documents can seem daunting. Fortunately, in 2014 NIST released the Cybersecurity Framework, which is intended to be a more accessible guidance for implementation a cyber security program. The Framework Core defines key activities, including Identify, Detect, Protect, Respond, and Recover, and maps these areas to control activities defined by standards including NIST, Control Objectives for Information and Related Technologies ("COBIT"), and International Organization for Standardization ("ISO") 27001. The Framework also includes guidance for the performance of a risk assessment, and measuring maturities levels in the key activities noted above.

Continued on page 2

In September 2016, NIST released a draft of the Baldridge Cybersecurity Excellence Builder (PDF warning), which is a self-assessment tool intended to help organizations assess the effectiveness of the cybersecurity programs. This self-assessment tool can be used as a guide when performing the first three steps presented in the NIST Cybersecurity Framework:

- 3.1 Basic Review of Cybersecurity Processes: Use the information gained from answering the self-assessment questions to compare your current cybersecurity activities with those outlined in the Cybersecurity Framework Core.
- 3.2 Establishing or Improving a Cybersecurity Program: Use your answers to the self-assessment questions to inform the seven steps in creating or improving a cybersecurity program.
- 3.3 Communicating Cybersecurity Requirements with Stakeholders: Your answers to the questions might inform the creation of a Target Profile to express cybersecurity risk management requirements to stakeholders.

The Federal Trade Commission ("FTC") is among the most active enforcement bodies on issues of cybersecurity ruling against 60 organizations since 2001 under deceptive and unfair trade practices. The FTC recently released a publication stating their position that "By identifying different risk management practices and defining different levels of implementation, the NIST Framework takes a similar approach to the FTC's long-standing Section 5 enforcement."

If your organization has not performed a cybersecurity assessment, or is looking for guidance on cybersecurity governance, consider utilizing the NIST Cybersecurity Self-Assessment Tool as a guide. Whitley Penn's Risk Advisory Services team can help improve your information security program by performing the cybersecurity assessment. Our Risk Advisory Services team can also perform IT control reviews, vulnerability scanning, and penetration testing to test the effectiveness of your information security program. To learn more about how Whitley Penn can assist in developing, assessing, or auditing your information security and anti-fraud controls, please visit our website or contact Scott Geye at c.scott.geye@whitleypenn.com or 214-393-9592.

whitleypenn