THE
NATIONAL LAW REVIEW

National Institute of Standards and Technology Releases Cybersecurity Guide for Small Businesses

Friday, November 11, 2016

Article By Ashden Fein
David J. BenderCovington & Burling LLP
Inside Privacy

Communications, Media & Internet
All Federal

The ***National Institute of Standards and Technology (NIST)*** released guidance today designed to help small businesses improve their cybersecurity preparedness. The document, *Small Business Information Security: The Fundamentals*, is based on NIST's 2014 Framework for Improving Critical Infrastructure Cybersecurity, a widely used cybersecurity framework (Cybersecurity Framework).

According to NIST's press release, the guidance is "written for small-business owners not experienced in cybersecurity and explains the basic steps they can take to better protect their information systems." The guidance notes that small businesses are often viewed as soft targets by cyber criminals because they have fewer resources to devote to information security than larger organizations. For purposes of this guidance, NIST defines small businesses as for-profit, non-profit, and similar organizations with up to 500 employees; however, this guidance provides an overview of information security and cybersecurity along with key recommendations that are generally applicable to all businesses regardless of size.

The guidance is divided into four sections and appendices. The first section provides background on information security and cybersecurity and provides context for the additional sections. The second section provides recommendations on how to identify, understand, and manage certain cyber-related risks and outlines when it is appropriate to seek outside assistance. The third section sets forth programmatic steps that small businesses can take to develop or improve their cybersecurity maturity using the Cybersecurity Framework's broad categories: Identify, Protect, Detect, Respond, and Recover.

The fourth section provides a list of "recommended practices" that small businesses can immediately implement to better protect their systems and information. These practices include the following:

- Pay attention to the people you work with and around.
- Be careful of email attachments and web links.
- Use separate personal and business computers, mobile devices, and accounts.
- Do not connect personal or untrusted storage devices or hardware to your computer, mobile device, or network.
- Be careful downloading software.
- Do not give out personal or business information.
- Watch for harmful pop-ups.
- Use strong passwords.
- Conduct online business more securely.

Lastly, the appendices contain helpful information security resources for small businesses, including risk analysis

worksheets and sample information security policy and procedure statements.

Source URL: https://www.natlawreview.com/article/national-institute-standards-and-technology-releases-cybersecurity-guide-small