THE
NATIONAL LAW REVIEW

CISA Releases “Cyber Essentials” to Assist Small Businesses Updated

SheppardMullin

Article By
Jonathan E. Meyer
Townsend L. Bourne
Sheppard, Mullin, Richter & Hampton LLP
Government Contracts, Investigations & International Trade Law Blog

- Communications, Media & Internet
- Government Contracts, Maritime & Military Law

- All Federal

Monday, November 25, 2019

On November 6, 2019, the Department of Homeland Security (“DHS”), Cybersecurity & Infrastructure Security Agency (“CISA”) released its Cyber Essentials guide. Consistent with the NIST Cybersecurity Framework, these Cyber Essentials provide “a starting point to cyber readiness,” and are specifically aimed at small businesses and local government agencies that may have fewer resources to dedicate to cybersecurity.

The guide suggests a holistic approach for managing cyber risks, and is broken down into six “Essential Elements of a Culture of Cyber Readiness,” specifically:

- Yourself – driving awareness, strategy, and investment to build and sustain a culture of cybersecurity.
- Your Staff – developing awareness and vigilance because your staff is often the first line of defense.
- Your Systems – protecting your information and critical assets and applications.
- Your Surroundings – limiting access to your digital environment.
- Your Data – having a contingency plan to recover systems, networks, and data from trusted backups.
- Your Actions Under Stress – planning and conducting drills for cyberattacks to

bolster readiness to respond, limit damage, and restore operations in the event of an attack.

The final section of the guide provides a list of steps that small businesses can take immediately to increase organizational preparedness against cyber risks. These include backing up data (automatically and continuously), implementing multi-factor authentication (particularly for privileged, administrative, and remote access users), enabling automatic updates, and deploying patches quickly.

CISA's Cyber Essentials guide is just the most recent example of a user-friendly resource aimed at assisting small businesses seeking lower-cost cybersecurity solutions. Recognizing that investing in cybersecurity may be difficult for some small businesses, Government agencies are making an effort to help small businesses understand the importance of cybersecurity.

For example, the U.S. Small Business Administration ("SBA") has a page dedicated to providing information and resources for small business cybersecurity. It outlines common threats, risk assessment, and cybersecurity best practices. It also provides a list of upcoming training and events related to small business cybersecurity. Other entities, including the National Institute of Standards and Technology, the Federal Trade Commission, and the Federal Communications Commission also provide similar resources specifically tailored to small businesses.

The main takeaway here is that all organizations – regardless of size or resources – should take basic steps to improve their cybersecurity resilience

Co-author Nikole Snyder is a Law Clerk in the firm's Washington, D.C. office.

Copyright © 2020, Sheppard Mullin Richter & Hampton LLP.

Source URL: https://www.natlawreview.com/article/cisa-releases-cyber-essentials-to-assist-small-businesses-updated