U.S. DEPARTMENT OF HOMELAND SECURITY

Office of Intergovernmental Affairs

Please see the advisory below from our partners in the Cybersecurity and Infrastructure Security Agency (CISA) regarding the release of a new Cyber Essentials toolkit to assist small businesses and government agencies understand and address cybersecurity risks.

May 28, 2020

CISA Advisory

CISA Releases New *Cyber Essentials* Toolkit

As a follow-up to the November 2019 release of Cyber Essentials, the Cybersecurity and Infrastructure Security Agency (CISA) released the first in a series of six Cyber Essentials Toolkits. This is a starting point for small businesses and government agencies to understand and address cybersecurity risk as they do other risks. CISA's toolkits will provide greater detail, insight and resources on each of the Cyber Essentials' six "Essential Elements" of a Culture of Cyber Readiness.   Today's launch highlights the first "Essential Element: Yourself, The Leader" and will be followed each month by a new toolkit to correspond with each of the six "Essential Elements." Toolkit 1 focuses on the role of leadership in forging a culture of cyber readiness in their organization with an emphasis on strategy and investment.

"We thank all of our partners in government and the private sector who played an essential role in the development of CISA's Cyber Essentials Toolkit," said CISA Director Christopher Krebs. "We hope this toolkit, and the ones we are developing, fills gaps and provides executives the tools they need to raise the cybersecurity baseline of their teams and the organizations they lead."

Developed in collaboration with small businesses and state and local governments, Cyber Essentials aims to equip smaller organizations that historically have not been a part of the national dialogue on cybersecurity with basic steps and resources to improve their cybersecurity. Cyber Essentials includes two parts – guiding principles for leaders to develop a culture of security, and specific actions for leaders and their IT professionals to put that culture into action.

Each of the six Cyber Essentials includes a list of actionable items anyone can take to reduce cyber risks. These are:

- Drive cybersecurity strategy, investment, and culture;
- Develop heightened level of security awareness and vigilance;
- Protect critical assets and applications;
- Ensure only those who belong on your digital workplace have access;
- Make backups and avoid loss of info critical to operations; and
- Limit damage and restore normal operations quickly.

To learn more about the Cyber Essentials Toolkits, visit https://www.cisa.gov/cyber-essentials.