PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Biden Administration Announces National Cybersecurity Strategy

By Thomas J. DeMayo, Principal, Cybersecurity and Privacy Advisory

The Biden-Harris Administration recently revealed their vision for enhancing and overhauling the cybersecurity posture and fundamental mindset of the United States. Although not law, the strategy does call for new legislation and the use of existing powers to "rebalance the responsibility to defend cyberspace" and "realign incentives to favor long-term incentives."

The Five Pillars of Cybersecurity

The strategy is structured around the following five pillars:

1. **Defend Critical Infrastructure by:**

    - Expanding the use of minimum cybersecurity requirements in critical sectors, ending an era that encouraged, but not mandated, companies to enhance their cybersecurity programs;
    - Enabling public-private collaboration; and,
    - Defending and modernizing federal networks and updating federal incident response policy.

2. **Disrupt and Dismantle Threat Actors by**:

    - Employing all tools of national power to disrupt adversaries;
    - Engaging the private sector in disruption activities; and,
    - Addressing the ransomware threat though greater international collaboration.

3. **Shape Market Forces to Drive Security and Resilience by**:

    - Promoting privacy and the security of personal data through legislation;
    - Making software vendors more accountable for the security of their software and products;
    - Utilizing federal grants to enhance cybersecurity programs; and,
    - Exploring a federal cyber insurance backstop in the event of a catastrophic cybersecurity event.

4. **Invest in a Resilient Future by:**

    - Securing the technical foundation of the internet;
    - Prioritizing cybersecurity R&D; and,
    - Enhancing the national cyber workforce.

5. **Forge International Partnerships to Pursue Shared Goals by:**

    - Leveraging like-minded nations to counter digital threats through joint preparedness, response and costs;
    - Increasing the ability of our partners to defend themselves against cyber threats; and,
    - Working with our allies to secure global supply chains for communication and operational technology products and services.

Ambition Must Become Reality

The above listing is incredibly ambitious; however, necessary. We the people – those most often the significant bearers of the consequences of cybersecurity lapses that are the direct result of those failing to exercise cybersecurity due care – need to take a stand to ensure ambition becomes reality. It is not only a matter of national security, but the very safety of those we care for most.

Contact Us

PKF O'Connor Davies is here to help you. If you have concerns about the new privacy rules, reach out to your engagement team or to our Cybersecurity and Privacy Advisory specialists:

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Principal
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com | 646.449.6353