THE NATIONAL LAW REVIEW

Thomas Bossert Selected to be President-elect Trump's Top Counterterrorism Adviser

Wednesday, December 28, 2016

As we've noted previously, **President-elect Trump**'s campaign was light on details about his plans to address cybersecurity. However, his announcement yesterday that Thomas P. Bossert will serve as his assistant for homeland security and counterterrorism, a position equal in status to national security adviser according to the transition team, may offer greater insight into the President-elect's intentions and plans for cybersecurity and related issues.

jackson lewis.

Article By   Damian J. Privitera
Damon W. Silver Joseph J. Lazzarotti
Jackson Lewis P.C. Workplace Privacy Blog

Communications, Media & Internet
All Federal

Mr. Bossert, who served as a top homeland security advisor to the latter President Bush, and who is currently the president of a risk management consulting firm that provides services to companies and governments, noted in the statement announcing his appointment:

We must work toward cyberdoctrine that reflects the wisdom of free markets, private competition and the important but limited role of government in establishing and enforcing the rule of law, honoring the rights of personal property, the benefits of free and fair trade, and the fundamental principles of liberty.

Mr. Bossert's statement – in particular the portion regarding the "limited role of government" – suggests that the Trump Administration may be slow to pursue new federal cybersecurity statutes and regulations, and that it may give federal agencies, such as the FTC, FBI, and DHS, shorter leashes to enforce existing cybersecurity laws. This statement is consistent with Mr. Bossert's past advocacy of utilizing a free market approach to cyber insurance, instead of a government-backed program.

That said, given the prominent role cybersecurity issues have played in the lead-up to and wake of the presidential election, and the increased incidence in recent years of cyberattacks against high-profile businesses and government entities, the Trump Administration could face enormous political pressure to take action on the cybersecurity front. One way Mr. Trump may respond to that pressure is by investing heavily in measures designed to protect public and private organizations in the U.S., including private businesses, from cyber conduct perpetuated by foreign actors. Mr. Bossert, who has warned that businesses "don't have enough money to compete with a motivated Chinese intelligence community data collection apparatus that can spend billions when [businesses] can only spend millions," would likely agree with such an approach. The business community should bear in mind, though, that an effective plan for disrupting international interference with U.S. business affairs will likely require some degree of domestic regulation.

Additionally, it is worth noting state and local governments have not waited for the federal government to act, and have legislated in a number of areas concerning cybersecurity. Examples include stringent regulations in California and Massachusetts designed to safeguard information systems and personal data. More recently, New York State is poised to finalize new, stringent cybersecurity regulations, potentially prompting other states to do the same. Indeed, other states and cities have already signaled their intent to pursue activist immigration and climate change agendas in response to what they believe the Trump Administration's agenda will be.

We will keep you posted as Mr. Trump's cybersecurity policies, and state and local responses thereto, come into

clearer view.

Jackson Lewis P.C. © 2019