Cooley

The 'New' Cybersecurity National Action Plan

February 10, 2016

The Obama administration has introduced its Cybersecurity National Action Plan (the "CNAP") in connection with its 2017 budget proposal. The CNAP aims to protect Americans, government agencies, and companies against the growing number of cyberattacks by fortifying America's digital defenses. The CNAP would (1) establish a new commission tasked with providing recommendations on protecting computer networks, (2) create a federal Chief Information Security Officer (CISO) to modernize IT across the government, and (3) empower Americans to secure their online accounts by using additional security tools.

Strengthen federal cybersecurity

The President's budget proposal will look for Congress to approve a 35% increase in the cybersecurity budget to secure $19 billion in funding for implementation starting next year. The funding includes a $3.1 billion Information Technology Modernization Fund to help retire, replace, and modernize legacy IT across the government. The federal Chief Information Security Officer will oversee the IT modernization and be responsible for developing, managing, and coordinating cybersecurity strategy, policy, and operations across the entire federal domain.

The Administration is requiring agencies to identify and prioritize their highest-value and most at-risk IT assets and then take additional concrete steps to improve their security. Federal agencies will increase the availability of government-wide shared services for IT and cybersecurity to ensure efficient, effective, and secure options are available to individual agencies to defend themselves against the most sophisticated threats.

Part of CNAP is aimed at increasing training and recruiting for cybersecurity specialists. The federal government will enhance cybersecurity education and training nationwide and hire more cybersecurity experts to secure federal agencies. In addition, the budget includes plans for offering scholarships and forgiving student loans in an attempt to expand the cybersecurity workforce.

Commission on Enhancing National Cybersecurity

The Commission on Enhancing National Cybersecurity ("Commission") would be comprised of top strategic, business, and technical thinkers from outside of government. The Commission is tasked with making detailed recommendations on actions that can be taken to enhance cybersecurity awareness and protections, to protect privacy, to maintain public safety and economic and national security, and to empower Americans to take better control of their digital security.

Empower individuals

The CNAP includes multiple new actions to strengthen the security of consumer data:

- The President is calling on Americans to move beyond use of a password alone to leverage multiple factors of authentication when logging in to online accounts.
- Private companies, non-profits, and the federal government are working together to help more Americans stay safe online through a new public awareness campaign that focuses on broad adoption of multi-factor authentication and is designed to arm consumers with simple and actionable information to protect themselves in an increasingly digital world.
- The federal government is accelerating adoption of strong multi-factor authentication and identity proofing for citizen-facing federal government digital services, and is conducting a systematic review of where it can reduce the use of Social Security numbers.
- The Small Business Administration will offer cybersecurity training to over 1.4 million small businesses and their workers

Enhance critical infrastructure security and resilience

The CNAP calls for strengthened partnerships with the private sector to deter, detect, and disrupt threats, including to the nation's critical infrastructure. The federal government inaugurated a new cybersecurity Center of Excellence, which will bring together industry and government experts to research and develop new cutting-edge cyber technologies. A national testing lab will be established, where companies can test their systems' security under simulated attacks.

Next steps

The IT modernization fund and other cybersecurity proposals still need to make it through the congressional budget cycle but federal IT leaders are hopeful that the initiatives will survive. Even if the CNAP funding is approved, however, questions remain as to whether these initiatives will improve a seemingly losing battle to cybercriminals. As one commentator recently opined, "the government, our government will be permanently late for your cybersecurity." Many of the "new" CNAP efforts have either already been suggested or rolled out (e.g., two-factor authentication). Further, despite prior government efforts (including the Commission on Cybersecurity for the 44th Presidency, the Cyberspace Policy Review, the Comprehensive National Cybersecurity Initiative (CNCI), the National Strategy for Trusted Identities in Cyberspace (NSTIC), the NIST Cybersecurity Framework, and other programs), the attacks continue to worsen.

It remains to be seen whether the CNAP will have an effect on this trend, but it does make clear that all stakeholders (government, businesses, and individuals) must be vigilant in order to make progress. Cooley's Privacy & Data Protection practice has significant experience and expertise counseling clients on these issues. If you would like more information regarding the CNAP, please contact one of the attorneys identified on this alert.

Key Contacts

Matthew D. Brown **San Francisco**	**brownmd@cooley.com** **+1 415 693 2188**
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090