Published on *The National Law Review* https://natlawreview.com

White House’s Cybersecurity National Action Plan Includes Cybersecurity Awareness Campaign, Creation of Federal Privacy Council

Article By:

Caleb Skeath

Following the announcement of the President’s ***Cybersecurity National Action Plan (CNAP)***, an initiative designed to “enhance cybersecurity capabilities within the Federal Government and across the country,” the White House has released a fact sheet outlining the different components of the CNAP. The announcement of the CNAP follows the President’s request for $19 billion in funding for cybersecurity initiatives in fiscal year 2017, an increase of 35% over the previous year’s request. The CNAP includes a mixture of near-term measures and long-term objectives, with the ultimate goal of enhancing the federal government’s cybersecurity posture while encouraging private citizens and businesses to do the same. Some of the most significant aspects of the CNAP, discussed further below, include:

- The launch of a cybersecurity awareness campaign to promote the use of multi-factor authentication;
- A “systematic” review by the White House to identify areas where the federal government can reduce the use of Social Security Numbers as individual identifiers;
- Plans for the development of a Cybersecurity Assurance Program to test and certify connected devices against certain security standards;
- The creation of a Chief Information Security Officer (CISO) position within the federal government, coupled with a $3.1 billion initiative to modernize federal agencies’ IT systems and applications;
- The establishment of a commission of private sector cybersecurity experts to offer recommendations on cybersecurity initiatives; and
- The establishment of a Federal Privacy Council, composed of representatives from various key federal agencies, to coordinate guidelines for the federal government’s collection and storage of data.

As part of the CNAP, the President signed an Executive Order establishing the Commission on Enhancing National Cybersecurity. This Commission will assemble twelve leading cybersecurity and privacy experts from across the private sector to provide recommendations for procurement and management of federal civilian IT systems, state and local cyber initiatives, and critical infrastructure protection. The Commission's final report to the President will be due on December 1, 2016. In recognition of the growing cybersecurity risks presented by the Internet of Things, the Department of Homeland Security will collaborate with UL and other industry stakeholders to develop a Cybersecurity Assurance Program to test and certify connected devices. The fact sheet notes that the Program will allow consumers to purchase certified devices with confidence that they "meet security standards."

The CNAP fact sheet also announced the kickoff of the National Cybersecurity Awareness Campaign in coordination with the National Cyber Security Alliance and other private-sector entities. This campaign will focus on promoting the use of multi-factor authentication, whether through biometrics, one-time codes, or otherwise. The fact sheet notes that the National Cyber Security Alliance will partner with Microsoft, Facebook, PayPal, Google, Dropbox, MasterCard, Visa, Venmo, and other private sector entities to focus on securing online accounts and transactions. As part of this campaign, the federal government will undertake a systematic review to identify opportunities to reduce reliance on Social Security Numbers as individual identifiers.

To promote public-private collaboration on cybersecurity, the CNAP includes several initiatives from the federal government to offer cybersecurity assistance to the private sector. The Department of Homeland Security, the Department of Commerce, and the Department of Energy will establish a National Center for Cybersecurity Resilience, which will allow entities to test the security of systems, such as electric grids, in a contained environment. The Department of Homeland Security will double the number of cybersecurity advisors available to assist private entities, while the National Institute of Standards and Technology will solicit feedback to further develop its Cybersecurity Framework for critical infrastructure. The fact sheet also notes that the administration plans to release a policy for national cyber incident coordination, and an accompanying severity methodology for evaluating cyber incidents, by the spring of 2016.

To improve the federal government's cybersecurity posture, the CNAP establishes the position of a Federal Chief Information Security Officer, and creates a $3.1 billion Information Technology Modernization Fund to speed up agencies' efforts to upgrade older systems and applications. The federal CISO, who will work within the Office of Management and Budget and report to the Federal Chief Information Officer (currently, Tony Scott), will oversee cybersecurity policy for all federal civilian agencies. The administration hopes to fill this new position within the next 60 to 90 days. The IT Modernization Fund, which builds off of the administration's previously released Cybersecurity Implementation Plan, will allow agencies to upgrade legacy systems and create savings through reduced maintenance costs. The GSA will administer the fund, focusing on efforts to move from high-cost applications to modern architectures, such as the cloud and shared services.

President Obama also signed an executive order establishing the Federal Privacy Council, which will bring together top privacy officials from agencies across the federal government to recommend improvements for the federal government's privacy policies and requirements. Finally, the CNAP provides for funding the deployment of the Department of Homeland Security's Einstein and Continuous Diagnostics and Mitigation programs across federal civilian agencies during fiscal year 2017, in addition to funding for increased recruitment of federal cybersecurity employees.

National Law Review, Volume VI, Number 41

Source URL:https://natlawreview.com/article/white-house-s-cybersecurity-national-action-plan-includes-cybersecurity-awareness