Middle Class Economics: Cybersecurity

The President's 2016 Budget is designed to bring middle class economics into the 21st Century. This Budget shows what we can do if we invest in America's future and commit to an economy that rewards hard work, generates rising incomes, and allows everyone to share in the prosperity of a growing America. It lays out a strategy to strengthen our middle class and help America's hard-working families get ahead in a time of relentless economic and technological change. And it makes the critical investments needed to accelerate and sustain economic growth in the long run, including in research, education, training, and infrastructure.

These proposals will help working families feel more secure with paychecks that go further, help American workers upgrade their skills so they can compete for higher-paying jobs, and help create the conditions for our businesses to keep generating good new jobs for our workers to fill, while also fulfilling our most basic responsibility to keep Americans safe. We will make these investments, and end the harmful spending cuts known as sequestration, by cutting inefficient spending and reforming our broken tax code to make sure everyone pays their fair share. We can do all this while also putting our Nation on a more sustainable fiscal path. The Budget achieves about $1.8 trillion in deficit reduction, primarily from reforms to health programs, our tax code, and immigration.

****

Computers, information, and communications technology are increasingly the foundation of the U.S. economy and driving the technological change that allows small and medium-sized U.S. businesses to compete in the global marketplace. Yet that same economic growth is threatened by a corresponding growth in cyber threats. Increasing data breaches, theft of intellectual property through cyber means, and cyber attacks are resulting in real costs and consequences for the American economy. Consequently, the Administration is taking actions to better prepare our Government, our economy, and our Nation as a whole to defend against growing cyber threats.

Cyber threats continue to evolve, posing one of the gravest national security dangers to the United States. The Administration has outlined several budgetary, programmatic, and legislative strategies to improve the Government's cybersecurity infrastructure and combat this growing threat domestically and globally. In addition to the FY 2016 Budget, the President recently provided Congress with an updated cybersecurity legislative proposal that will provide the Federal Government and private sector the necessary tools to improve our Nation's cybersecurity.

In FY 2016, the President's Budget proposes $14 billion in cybersecurity funding for critical initiatives and research. The Budget makes the following strategic investments:

- **Securing Federal Networks.** $582 million is included for DHS to lead implementation of the Continuous Diagnostics & Mitigation (CDM) program. This program will assist agencies in managing cybersecurity risks on a near real-time basis. The investment in DHS also supports deployment of the National Cybersecurity Protection System (better known as Einstein) to enable agencies to detect and prevent evolving cyber threats. The Budget also sustains support for agencies to reach the Cybersecurity Cross-Agency Priority goal and implement post-Wikileaks security improvements on classified networks, pursuant to E.O. 13587.

- **Outreach to the Private Sector.** $149 million is included across the Federal Government to support ongoing proactive efforts to improve the cyber security posture of our private sector partners.
- **Shaping the Future Cyber Environment.** $243 million is included to support research and development at civilian agencies to support innovative cybersecurity technologies.
- **National Security and Cyber Threats.** $514 million is included for the Department of Justice to investigate cyber intrusions which pose serious threats to National security and the Nation's economic stability and to prosecute the offenders. The Budget also addresses economic security by sustaining efforts to modernize and vastly increase the efficiency and capacity of our Mutual Legal Assistance Treaty capabilities, and to support our diplomatic efforts to protect the free flow of information and commerce in cyberspace. Within the Department of Defense, the Budget includes funding to continue developing U.S. Cyber Command to its full strength.
- **Supporting Long-Term Cyber Investments.** The Budget also makes key long-term structural investments in cybersecurity, including:
    - $227 million to fund the first phase of construction of the Federal Civilian Cyber Campus, which will collocate the DHS and FBI operational cyber missions to improve collaboration and efficiency, provide a secure and modern technical footing, and improve the ability to collaborate with private industry and external partners
    - $35 million to improve cyber intelligence integration, analysis, and planning within the Federal Government.

In addition to these critical investments, we are asking Congress to take legislative action to further protect our cybersecurity. The Administration's 2015 Cybersecurity Legislative Proposal has three central elements, aimed at ensuring the continued safety of our Nation, while also protecting the personal data and privacy of citizens. The proposal includes the following:

Proposal to Enhance Information Sharing.

- Facilitates greater voluntary sharing of cyber threat information between the government and private sector.
- Incentivizes the further development of Information Sharing and Analysis Organizations to improve the voluntary sharing of cyber threat information within the private sector and between the private sector and the government.

Protects the privacy of Americans by requiring private entities that share voluntarily under the proposal's authority, to comply with certain privacy restrictions, such as removing unnecessary personal information in order to qualify for liability protection

Establish Data Breach Standards.

- Establishes a single Federal standard for notifying individuals in a timely, consistent way when private sector data breaches occur; this helps businesses and consumers by simplifying and standardizing the existing patchwork of 47 state laws that contain data breach report requirements into one federal statute. This is part of our commitment to balance security and privacy, ensuring citizens receive timely information on their data in the event of a breach. This will:
    - Provide a single threshold for notification.
    - Establish deadlines for notification of cyber incidents.

- Require notification of the Federal government in certain instances where Federal information may have been compromised.

Modernizing Law Enforcement Authorities and Criminal Penalties.

- Ensures law enforcement has the tools to investigate, disrupt, and prosecute cybercrime.
- Allows prosecution for the sale of botnets.
- Better enables law enforcement to prosecute the overseas sale of stolen U.S. financial information like credit card and bank account numbers.
- Expands federal law enforcement authority to deter the sale of spyware used to stalk or commit ID theft.
- Gives courts the authority to shut down botnets engaged in distributed denial of service attacks and other criminal activity.