Middle Class Economics: Cybersecurity

Updated August 7, 2015

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.

****

Ensuring the cybersecurity of our critical assets, systems and data is one of the most significant challenges we face as a Nation. Every day, the Federal Government experiences increasingly sophisticated and persistent cyber threats, which threaten to outpace efforts to prevent, mitigate, and respond to them. Because the President recognizes the seriousness of these challenges, his FY 2016 Budget request included a significant increase in resources to dramatically accelerate improvement in Federal cybersecurity using a risk-based approach to identify and protect critical information assets.

The President’s FY 2016 Budget requests $14 billion across the Federal Government to support the Administration’s cybersecurity strategy. This is an increase of $1.4 billion, or 11 percent, above the level provided in FY 2015, an investment made possible by the fact that the President’s Budget reverses both defense and non-defense sequestration funding cuts.

<u>These additional resources are critical for</u>:

- Protecting high-value assets and sensitive information;
- Quickly detecting and responding to cyber threats;
- Rapidly recovering from incidents;
- Ensuring the recruitment and retention of cybersecurity talent; and
- Keeping government systems and practices current with emerging technology.

The President's 2016 Budget request improves cybersecurity across the Federal Government through targeted investments across a range of Federal departments and agencies. Some of the most significant examples are described below.

Department of Homeland Security ($1.4 billion; 7% increase over FY 2015)

The Department of Homeland Security's (DHS) FY 2016 Budget supports critical investments needed to improve cybersecurity and protect government networks from malicious cyber attacks. DHS maintains two critical programs that support the Administration's overall cyber strategy:

1) the EINSTEIN intrusion detection and prevention system; and,
2) the Continuous Diagnostics and Mitigation (CDM) program.

The President's Budget requests **$480 million to expand the intrusion detection and prevention capabilities of EINSTEIN** to protect federal agencies from new tactics used by malicious actors. To address cybersecurity vulnerabilities, the Budget requests **$102 million to continue the deployment of CDM tools and sensors** that agencies and DHS can use to detect vulnerabilities on agency networks before they can be exploited by malicious cyber actors. Addressing both cyber threat vectors and vulnerabilities on agency networks is **critically necessary to prevent cyber attacks** and quickly mitigate them if they do occur.

While technology is an important aspect in addressing sophisticated cybersecurity threats, DHS also needs to recruit and retain a talented cybersecurity workforce to support the Administration's cybersecurity efforts. The Budget requests **$32 million to help multiple DHS components better recruit and retain a skilled cybersecurity workforce**.

Department of Justice ($636 million; $14% increase over 2015)

Funding requested for the Department of Justice (DOJ) in FY 2016 primarily supports furthering cyber detection and response capabilities. In particular, the FY 2016 request includes:

- **$514 million for the Department of Justice to investigate cyber intrusions** that prose serious threats to the Nation's security and economic stability, as well as to prosecute the offenders.
- The FY 2016 Budget request also includes **$10.3 million for the FBI's Next Generation Cyber Initiative**. This initiative would improve cyber collection and analysis and allow the FBI to extend advanced cyber capabilities to the field. In addition, the President's Budget funds needed investments to recruit, retain, and train the cyber workforce, including training attorneys on cybercrime and digital evidence.
    - Specifically**, $12.2 million and 114 positions is requested to support the current network of Computer Hacking and Intellectual Property (CHIP) and National Security Cyber Specialist** (NSCS) attorneys across the nation and to expand digital evidence expertise; increase training, and focus resources on

intrusions that threaten economic stability and public safety. These resources also support enhanced digital forensics and technical expertise as well as improved information sharing and relationship building with domestic and foreign partners.

- The Budget request also makes key investments that keep government systems current with the latest technology. Included in DOJ's request is **$1.7 million to support the acquisition of cybersecurity tools, such as advanced persistent threat or insider threat detection tools**.

Department of Defense ($9.5 billion; 11% increase over 2015)

The Department of Defense (DOD) plays a leading role in defending the nation from cyber attacks. DOD's FY 2016 Budget requests increased cyber funding to support all aspects of the Administration's cyber strategy. This includes targeted investments to protect high-value assets and defend DOD's networks; improve defensive and offensive cyberspace operations capabilities; and continue to develop DOD's cyber workforce through recruiting, hiring, and training. Specifically, the 2016 Budget includes:

- **Over $3 billion to prevent malicious cyber activity**, which includes monitoring and analyzing the systems and events occurring in the DOD network to prevent intrusions; ensuring trusted internet connections; establishing confidence in the identity of DOD users and systems; protecting the data and networks of the DOD systems; gathering counterintelligence to protect against cyber espionage; and keeping audit tools in place, along with other actions, to protect against insider threats. Increases to these activities include strengthening the ability to defend the DOD network, control and manage network accesses, and identify intruders.
- The 2016 Budget also includes **$5 billion for shaping the cyberspace environment and cyber operations**. These activities include training in order to sustain a skilled cyber workforce; outreach to partners outside the federal government, such as the Defense Industrial Base and our international partners; research and development; analysis of cyber operations capabilities; and infrastructure activities, including construction.

In addition, the 2016 Budget increases funding in other key areas of DOD, including nearly **$500 million for the continued implementation and support of the Cyber Mission Forces (CMF).** The CMF program includes military and civilian billets in all of the Services to include their training and support. The teams are located across the US. FY 2016 will be the third year in this multi-year DOD initiative. The Budget also adds funds to improve infrastructure at multiple sites, as well as increases for computer network operations.

Internal Revenue Service ($242 million; 72% increase over 2015)

The Internal Revenue Service (IRS) maintains data on hundreds of millions of individuals and business taxpayers, which makes it a prime target for bad actors. Protecting this sensitive information is an important aspect of the Administration's cyber security strategy, and the

President's FY 2016 Budget supports the critical investments needed to increase cyber security and protect taxpayer information at the Internal Revenue Service (IRS).

Under the President's Budget, the IRS would bolster cybersecurity by improving detection and prevention of online data attacks through investments in advanced technology, information technology infrastructure, and data analytics. It would also invest in enforcement, including investigations of international criminal actors. Meanwhile, the IRS would take especially aggressive steps to fight identity theft and Stolen Identify Refund fraud. These include systems improvements and new information sharing with States and industry to help detect and prevent identity theft before tax refunds are paid; major investments in victim assistance, including comprehensive taxpayer account recovery services; and increased enforcement resources to ensure that perpetrators can be caught and prosecuted.

Cybersecurity is a top priority for the IRS, which has, for example, substantially increased its investment in combatting identity theft and refund fraud since 2010. But despite prioritizing these issues, IRS cybersecurity efforts to date have been hampered by severe funding cuts. Appropriately funding the IRS is a critical component of the Administration's overall cybersecurity strategy.

Health and Human Services ($262 million; 23% increase over 2015)

Over the past fiscal year, Department of Health and Human Services (HHS) has seen an increase in cyber threats. As threats continue to multiply and become more complex, enhanced controls and threat management strategies, as well as a mature Cybersecurity workforce – equipped with appropriate training, education, and skill sets, are vital to managing evolving threats and implementing controls necessary to protect IT assets. In particular, HHS is working to: (1) ensure there is a complete, comprehensive inventory of all systems in order to protect high-value assets and sensitive information; (2) implement a robust cybersecurity-focused workforce development program to recruit, reward, and retain cybersecurity expertise across the Department; and (3) develop enforceable security-focused contract language and ensure such language is included in all HHS contracts.

To support these and other cybersecurity efforts, the FY 2016 Budget includes increases for:

- **A Computer Security Incident Response Center**, which will provide network situational awareness through acquisition of emerging technologies across the Department. Software such as EINSTEIN and Continuous Diagnostics and Mitigation (CDM) programs provide real-time data to support the monitoring of HHS's IT assets and networks. These technologies provide HHS situational awareness of its cybersecurity posture and allow HHS's Operating Divisions to quickly share security incident information in order to coordinate strong response and recovery activities.

- **Trusted Internet Connection**, which supports network continuous monitoring activities to rapidly identify, respond, and recover from cyber incidents and includes resources related to the EINSTEIN intrusion detection and prevention system, which furnishes network security.

- **FISMA Program Management**, which performs IT asset inventories and updates Department-wide IT security policies in order to maintain compliance with DHS and FISMA Cybersecurity requirements.

Department of Commerce ($187 million, level with FY 15)

The Department of Commerce (DOC) is responsible for supporting government-wide cybersecurity by developing standards for use by both government and private sector entities and safeguarding demographic and economic data collected by the U.S. Census Bureau on behalf of itself and other Federal statistical agencies. The National Institute of Standards and Technology (NIST) within DOC is at the forefront of these efforts. NIST operates the national program office for executing the National Strategy for Trusted Identities in Cyberspace (NSTIC), a public-private effort to raise the level of trust associated with the identities of individuals, organizations, services, and devices involved in online transactions. Additionally, in 2014, NIST released the "Framework for Improving Critical Infrastructure Cybersecurity" to provide standards, guidelines, and best practices to the private sector to promote the protection of critical infrastructure. The FY 2016 Budget continues support for both of these initiatives and also requests additional funding for NIST to strengthen its cryptographic capabilities.

With components like the Census Bureau and the National Oceanic and Atmospheric Administration (NOAA), DOC is also one of the largest holders of government data. While these data are already safeguarded by deployment and use of intrusion detection and prevention systems and the recent initiation of 24x7/365 continuous monitoring by DOC's Enterprise Security Operations Center, DOC continues to improve these safeguards. This includes a request for an additional $13 million in the 2016 Budget for department-wide cybersecurity improvements that will network infrastructure upgrades, cyber security incident response enhancements, and improved credentialing and access management, which will help DOC in the timely detection and response to cyber incidents. Finally, the 2016 Budget requests additional funding as part of the 2020 Decennial Census research and testing program to consolidate IT systems across all Census programs in an effort to streamline operations that will also improve IT security.

Department of Veterans Affairs ($180.3 million; 15.5% increase over 2015)

The 2016 Department of Veterans Affairs' (VA) Budget requests:

- **$180.3 million to ensure VA information and network security**, including through continuous secure monitoring, continuity of operations, and a host of smaller cyber security programs. In addition to VA's network operations and monitoring office, VA's 2016 budget will enhance general system capabilities across the Department and improve threat intelligence by developing partnerships with other federal and state government partners and shared mission partners.
- FY 2016 funding will also support the maintenance of a Trusted Internet Connection (TIC) initiative and create a program management office to address VA's Continuous Readiness in Information Security Program (CRISP). The CRISP program is designed to

identify, prioritize, and remediate vulnerabilities on VA information systems; ensure baseline configurations and security standards are updated as new vulnerabilities are discovered and remediated; ensure software standards are continually reviewed and updated and that installed software versions comply with these standards; identify, collect, analyze, and report performance metrics to measure the effectiveness of the patch and vulnerability management, baseline configuration maintenance, and software standards maintenance processes; and propose changes to improve these processes. VA's program also includes funding for privacy and records management, business continuity support in case of emergency, field security services at remote locations, and identity and credential management.