Strengthening Federal Cybersecurity

Meeting Our Greatest Challenges: The President's Fiscal Year 2017 Budget

Under the President's leadership, we have turned our economy around and created 14 million jobs. Our unemployment rate is below five percent for the first time in almost eight years. Nearly 18 million people have gained health coverage as the Affordable Care Act has taken effect. And we have dramatically cut our deficits by almost three-quarters and set our Nation on a more sustainable fiscal path.

Yet while it is important to take stock of our progress, this Budget is not about looking back at the road we have traveled. It is about looking forward and making sure our economy works for everybody, not just those at the top. It is about choosing investments that not only make us stronger today, but also reflect the kind of country we aspire to be – the kind of country we want to pass on to our children and grandchildren.

The Budget makes critical investments in our domestic and national security priorities while adhering to the bipartisan budget agreement signed into law last fall, and it lifts sequestration in future years so that we continue to invest in our economic future and our national security. It also drives down deficits and maintains our fiscal progress through smart savings from health care, immigration, and tax reforms.

The Budget shows that the President and the Administration remain focused on meeting our greatest challenges – including accelerating the pace of innovation to tackle climate change and find new treatments for devastating diseases; giving everyone a fair shot at opportunity and economic security; and advancing our national security and global leadership – not only for the year ahead, but for decades to come.

****

The President has made clear that cybersecurity is one of the most important challenges we face as a Nation. That is why, since 2009, the President has executed a comprehensive strategy to protect and defend the country against cyber threats. The strategy brings all elements of Government together with private industry, academia, international partners, and the public to raise the level of cybersecurity in both the public and private sectors; deter and disrupt adversary activities in cyberspace; improve capabilities for incident response and resilience; and enact legislation that will remove legal barriers to and incentivize cybersecurity threat information sharing among private entities and between the private sector and the Federal Government.

The Budget builds on these achievements by enhancing ongoing work and investing resources and focusing leadership attention on new broader reforms—including fundamental changes to the way that the Federal Government manages cybersecurity risks. The Budget invests over $19 billion, or a roughly 35 percent increase from FY 2016, in overall Federal resources for cybersecurity, to support a broad-based cybersecurity strategy for securing the Government, enhancing the security of critical infrastructure and important technologies, investing in next-generation tools and workforce, and empowering Americans. In particular, this funding will support the Cybersecurity National Action Plan which aims to dramatically increase the level of cybersecurity in both the Federal Government and the country's digital ecosystem as a whole.

The Budget strategically invests in a series of actions outlined in the Cybersecurity National Action Plan (CNAP). Several of these investments are highlighted below.

Strengthening Federal Cybersecurity.

Building upon the Administration's broader efforts to enhance the Nation's cybersecurity, the Government has executed a series of actions to bolster Federal cybersecurity and secure Federal information systems through the 2015 *Cybersecurity Sprint* and the Administration's recently-issued *Cybersecurity Strategy and Implementation Plan (CSIP)*. While these actions addressed immediate concerns, challenges remain. The Federal Government has identified three primary challenges:

- **Outdated Technology** – The Federal Government relies significantly on hard-to-defend legacy hardware, software, applications, and infrastructure, which make it particularly vulnerable to malicious cyber activity, as well as costly to defend and protect.
- **Fragmented Governance** – Governance and management structures are unable to consistently provide effective, well-coordinated cybersecurity across the Federal Government.
- **Workforce Gaps** – Workforce shortages and skill gaps, including training, education, and recruitment and retention of cybersecurity and privacy professionals, are significant.

To meet these challenges, the Budget makes strategic investments to address these challenges:

- **Enhancing Federal IT to Secure Federal Information and Assets –** To address our legacy technology problems, the Budget requests $3.1 billion for the establishment of a revolving fund, the Information Technology Modernization Fund (ITMF), to retire the Government's antiquated IT systems and transition to more secure and efficient modern IT systems, while also establishing long-term mechanisms for Federal agencies to regularly refresh their networks and systems based on up-to-date technologies and best practices. A project review board, comprised of experts in IT acquisition, cybersecurity, and agile development, will review agency business cases and select projects for funding to ensure prioritization of projects with the greatest risk profile, government-wide impact, and probability of success. The board will identify opportunities to replace multiple legacy systems across government with a smaller number of common platforms – something that is difficult for agencies to do when acting on their own with limited insight into other agencies' operations. As a result, the ITMF will achieve a far greater and more rapid impact than if the funds were allocated directly to agencies. The ITMF revolving fund will be self-sustaining by requiring agencies to repay the initial investments through efficiencies gained from modernization, ensuring the fund can continue to support projects well beyond the initial infusion of capital. Seed funding of $3.1 billion would address an estimated $12 billion worth of modernization projects over 10 years. Ultimately, retiring or modernizing vulnerable legacy systems will not only make us more secure, it will also save money.

- **Streamlining Governance and Securing Federal Networks** – This Budget lays the foundation for shifting to more effective approaches to Federal cybersecurity by supporting investments in common IT solutions for small agencies, more secure enterprise-wide email systems, and common cybersecurity tools and services. The Budget includes $746 million for DHS to lead implementation of the Continuous Diagnostics & Mitigation program to assist agencies manage cybersecurity risks on a near real-time basis, and deployment of the National Cybersecurity Protection System to enable agencies to detect and prevent evolving cyber

threats. Using the purchasing power of Government acquisitions, GSA will pilot efforts to better coordinate and centralize IT networks and system acquisitions for smaller agencies. The Budget will continue funding for important efforts to strengthen enterprise-wide email system investments, migrating to stronger, more secure systems that reduce risk of intrusion.

- **Strengthening the Cybersecurity Workforce –** There is a shortage of skilled cybersecurity experts and privacy professionals throughout the IT industry as a whole, and that shortage is more acute within the Federal Government. To address this shortage, the Administration will enhance student loan forgiveness programs for cyber experts joining the Federal workforce. The Budget invests an additional $62 million for the following initiatives:
    - Establishing a CyberCorps Reserve program, which will offer scholarships for Americans who wish to obtain cybersecurity education and serve their country in the civilian Federal Government,
    - Developing a Cybersecurity Core Curriculum that will ensure cybersecurity graduates who wish to join the Federal Government have the requisite skills, and
    - Providing grants to academic institutions to participate in the National Centers for Academic Excellence in Cybersecurity Program.

Securing the Digital Ecosystem.

The Federal Government also has a responsibility to protect the nation from threats in cyberspace. Our Nation's critical infrastructure is increasingly under threat from disruption by cyber means. Such disruption could have severe adverse impacts on our national security, economic security, and public health and safety. Citizens and businesses should have the tools they need to protect themselves. Accordingly, the 2017 Budget sustains and expands on the Administration's previous work in this area as part of actions to secure the Digital Ecosystem, as outlined in the National Action Plan for Cybersecurity.

- **Outreach to the Private Sector** – The private sector is primarily responsible for operating the nation's critical infrastructure. The Budget include $174 million across a range of Federal agencies and programs to support ongoing, proactive efforts to improve the cyber security posture of the private sector.
- **Research and Development** – Our success in addressing cybersecurity challenges depends on continued investment in innovative science and technologies. The Budget includes $318 million to support ongoing R&D efforts.
- **National Security and Cyber Threats --** The Budget includes $682 million for the Department of Justice to investigate cyber intrusions that pose serious threats to national security and the Nation's economic stability and to prosecute the offenders. The Budget also includes $213 million for the DHS National Cybersecurity and Communications Integration Center to identify, assess, and respond to cyber threats.