Impact of legislation on internal revenue service

Law

The paper " Impact of Legislation on Internal Revenue Service" is a perfect example of an essay on law. The paper aims to analyze and review the IRS’s information security program and its program evaluation programs in accordance with Cyber Security Legislative Proposal of 2012, the Presidential Policy Directive pertaining to critical infrastructure resilience and security and the Executive Order 13636 relating to the improvement of cybersecurity critical infrastructure. In addition, points of analysis have been chosen from the three sources to better inform the way forward for cybersecurity enforcement in not only government agencies but also private sector entities.

IRS

The IRS’s activities are extensively based on computer systems to enable its mission-related and financial operations. Therefore, ensuring that its computer systems are secure from breach, is key in the protection of taxpayer data and sensitive financial information. Additionally, the effective modernization and development of information systems and applications are necessary in order to cope with the ever-changing business needs and improve the services that they render to the American taxpayer.

The Cyber Security Act of 2012 has been responsible for the ongoing measures in the IRS, of leveraging effective technological advances and modernizing its core business systems to improve overall output and efficiency levels. Specifically, the directive of protecting critical infrastructure in all government agencies and private sector entities has pushed for changes in the internal control system of the IRS. The federal requirements stipulated in the Act have led to the adoption of goals pertaining to electronic tax administration.

A review of the IRS and its information security program and evaluation programs, reveals that there is a deficiency in the IRS internal control system, pertaining mostly to its financial reporting systems. Areas that have been identified as being susceptible to risk include- the security of its employees, the adoption of security measures proposed by the recent legislature, Federal tax information security, enterprise risk management implementation, system development security measures and the security program dealing with enterprise information security. Further analysis of its Customer Account Data and Modernization Program, reveals that further measures need to be implemented.

Points of Analysis

Information sharing relating to cybersecurity is very crucial. The U. S government has embarked on legislature aimed at improving the efficient sharing of information between not only government agencies like the IRS, but also among private entities. The government aims to increase the quality, volume and timeliness of cybersecurity information shared in order to ensure that federal agencies and private sector organizations are able to protect themselves accordingly.

In accordance with the Executive Order 13636 and the Presidential Policy Directive, the Secretary of Homeland Security, the Attorney General and the Director of National Intelligence shall give instructions that match with the requirements of section 12(c), ensuring the timely development of reports on cybersecurity. Sharing of non-classified information with the private sector is very crucial in the war against cyber terrorism as it will assist in early detection and adoption of adequate prevention measures. Additionally, the measure of expanding the use of programs facilitating the application of

experts will be useful in providing advice on the structure, content and the type of information that is key to critical infrastructure operation, ownership and in mitigating cyber risks.

According to Borene, critical infrastructure protection is key to determining whether the United States is secure from cyber-attacks or not. Currently, the U. S is almost entirely run on computer systems meaning that any threat to these systems on a local, state or federal level can have devastating effects on the economy. The critical systems are not just limited to systems and assets but also refer to both virtual and physical systems. Critical infrastructure analysis and identification are essential in curbing the adverse effects of cyber terrorism, national security enforcement, national public safety and health (Borene, 2011).

Another point of the analysis is policy. Currently, the United States has been affected by a number of cyber intrusions in core critical infrastructure, which alludes to the importance of improved cybersecurity in all government agencies and private sector entities. The cyber threat posed on every critical infrastructure is an ongoing threat that represents one of the biggest challenges in national security. This is because the United States' economic and national security is reliant on the efficient functioning of critical infrastructures such as the IRS financial systems.

According to the Cyber Security Legislative proposal of 2012, policy impacts greatly on how the government deals with a number of issues. In terms of cybersecurity, the government's policy is hinged on improving the resilience and security of the country's critical infrastructure while also maintaining a cyber-environment that promotes innovation, efficiency, safety, privacy, confidentiality, sharing of cybersecurity information economic prosperity and

civil liberties. However, this can only be achieved if there is a mutual deal of cooperation between the operators of critical infrastructure and its owners. The creation of Voluntary programs relating to the Critical Infrastructure Cybersecurity is bound to improve levels of cybersecurity in all sectors of the agencies. In accordance with Presidential Policy Initiative, for critical infrastructure resilience and security, the Secretary shall work in coordination with some specific sectors of the federal agencies to develop a voluntary program whose main agenda is to support the development of a Cybersecurity framework for operators and owners of critical infrastructure. The sector agencies shall also report to the President on an annual basis via the Secretary, with reference to developing and reviewing the Cybersecurity framework. Additionally, the Secretary shall be involved in coordinating and managing the creation of incentives aimed at promoting participation in the program. This will assist in not only identifying areas of critical infrastructure most prone to risk but also in the incorporation of security standards in contract administration and acquisition planning.

Conclusion

It is only through cooperation between the federal agencies and the private sector can there be successful measures implemented against cyber terrorism and intrusion. In addition, a common framework and easy access to information between government agencies are key in the prevention and mitigation of cybersecurity risks.