Walker Model Congress 2015

|  |  |
| --- | --- |
| **Committee:****Senate Foreign Relations**  | **Principal Author:****Christopher Benos**  |
| **Bill No:**  | **Delegation: Maggie Lena Walker Governor’s School for Government and International Studies**  |
| **Title of Bill:****An Act to Ensure the Preservation of National Security and Defense.** |

Be It Enacted By The Walker Model Congress

|  |  |
| --- | --- |
| **1****2****3****4****5****6****7****8****9****10****11****12****13****14****15****16****17****18****19****20****21****22****23****24****25****26****27****28****29****30****31****32****33****34** | Preamble: Whereas the U.S. requires a greater electronic infrastructure to secure its national security; whereas online foreign threats, both unsponsored and government-sponsored, have increased by 2000% in the last decade; whereas the U.S. currently has billions of dollars in infrastructure susceptible to cyber warfare. Now therefore:Section 1: Bolster the Federal government’s efforts and capabilities to increase national cyber defense.1. Increase yearly funding for the Research, Development, Testing, and Evaluation section of the Department of Defense’s budget from $79.1 billion to $82 billion. This increase in funding will go towards developing and maintaining a program to combat cyber warfare.
2. The program referenced in Section 1, Sub-Section A, shall be formed by and placed under the authority of the Central Intelligence Agency (CIA). The CIA shall develop new methods for combatting cyber warfare and securing the United States. These methods can include but are not limited to:
	1. the improvement of American satellite/anti-satellite technology;
	2. the development of more effective types of malware, including spyware programs; and
	3. conducting risk assessments (threat, vulnerability, impact) and penetration testing on federal systems.

Section 2: Agencies are required to permit the Secretary of Defense to acquire, intercept, retain, use, and disclose communications, system traffic, records, or other information transiting to or from or stored on a federal system, for the purpose of protecting federal systems from cyber-security threats and mitigating threats to protect the federal government.Section 3: Let the punishment for cyber-crimes be increased from the current minimum of three years, according to federal code §1030A, to a minimum of ten years.Section 4: If the draft were to be reinstated during a time of national crisis, let there be an allocation of troops to the section on Cyber-Security Communication at the Department of Homeland Security. These troops will be selected from the broad pool of drafted highly skilled individuals based upon capabilities and experience in computer and technical fields. Their duties will be managed and directed by the Department of Homeland Security.Section 5: Sections 1 and 2 of this bill shall be funded by the Federal Department of Defense. Section 4 shall be funded by the Federal Department of Homeland Security.. The specific allocation of funds and the funding for Section 3 will be decided by the Appropriations Committee.Section 6: This bill shall go into effect 91 days after passage. |