FROM: SCUSA 71 Roundtable on Security in Cyberspace
TO: National Security Advisor
SUBJECT: Addressing the United States’ Vulnerabilities in Cyberspace

Introduction
Within a matter of years, “Cyberspace” has rapidly transitioned from an optimistic concept, to an emerging field, to where we are today: a national and international security concern that is quickly gaining primacy over traditional security measures. While the United States has led the world in innovation in Cyberspace, other nations are quickly approaching parity, using the technology for purposes not originally envisioned by the researchers and entrepreneurs of the United States. Today, we are at a cyber crossroads, where the United States national interest intersects private corporations financial interests and the world’s international security interests. At this intersection, we find that there are critical vulnerabilities in cyberspace that the National Security Council must address before they are exploited by organizations, both foreign and domestic, whose interests do not perfectly align with the United States’. Many vulnerabilities exist in cyberspace that compromise national and international security including coordination between the public and private sectors, legal and regulatory matters, and multinational actor concerns. To address these vulnerabilities, we recommend two major policy proposals that will work in both the domestic and foreign realms to quickly return the United States government to a position of power.

Public-Private Coordination
The challenges in cyberspace demand a more free-flowing relationship between the private and public sectors. Routinized paths for exchanging personnel between public and private organizations allow for the cross-pollination of ideas and the development of critical relationships between the two sectors that will foster the nexus of security, privacy, and safety. This enables both private and government personnel to take mission-critical objectives from government enterprises and utilize the private sector’s innovative project-based strategies to more holistically solve problems facing United States cyber interests. The expansion of the Defense Innovation Unit model will encourage and create technology that can be utilized for United States objectives across both spheres. Further synchronization will develop a more responsive and agile environment for cybersecurity.

We advocate for the creation of a sponsored sabbatical program that links government personnel to private companies for specific projects. This practice encourages employees from the public sector to learn from counterparts in a more innovative environment. In addition, encourages a project-based workflow that reinforces the flexibility needed to address the dynamic nature of cyberspace. In the other direction, private employees gain specialization and experience with skills aligned with USG interests that are not frequently trained in the private sector. The key step in crafting a robust two-way knowledge flow is permitting members from both sides to return to their previous positions or organizations; doing so gives them the opportunity to share their new experiences and skills with their home organizations. Expanding the Defense Innovation Unit will pave the way for smaller ventures to contribute valuable
developed assets that otherwise would not be available to government enterprises due to existing obstacles for smaller businesses.

**Legal and Regulatory Matters**

There is no consensus on the appropriate norms of behavior that exist for cyberspace. This problem can be addressed by creating stability through industry norms, facilitating diplomatic dialogue, and balancing the United States’s immediate and long-term goal of guiding cyber norms to create a cyber realm that adheres to regulation of appropriate conduct, while preserving different entities’ rights. We recommend that governmental organizations subsidize corporate technological development that advances the policy preferences of the United States. This provides a two-way line of communication between the private sector and the government to facilitate the development of new technology and its implementation in accordance with the United States’ policy, on a domestic and international scale. Additionally, we aim to connect field experts with rising university talent to educate and address current and emerging threats as part of international discussions by drawing on the expertise of both groups, past, present, and future. We affirm our commitment to respect the rights of all governmental and corporate institutions that are involved in cyber activity.

**Multinational**

The “cyber world order” is still in its nascent forms, with few norms or legal frameworks that exist to coordinate a global response to tomorrow’s cybersecurity issues. A lack of cooperation between states means that poor cybersecurity in one state can affect the national security in a whole region. Cybersecurity vulnerabilities in national infrastructure is not a solely national issue; instead, the world must create a global initiative. To improve the United States’ own domestic cybersecurity concerns, we must lead the world in creating a global cybersecurity initiative inclusive of all willing states, not just the United States’ closest allies. Using both national and private industry experts, this “Cyber Health Organization” will emphasize open security standards in cryptography and cybersecurity practices. It will also promote information sharing and response coordination, improving a cyberattack victim’s ability to identify the source of an attack and stop it from proliferating.

**Conclusion**

The pivot to Cyberspace represents one of the most fundamental challenges in policy the United States has faced since the Second World War. The emerging technologies in cyberspace have the opportunity to improve the world writ large, but if we only focus on the opportunities for improvement, we will be destroyed by malicious actors using this same technology against us. The importance of private corporations in cyberspace makes our domestic policy toward them affect our foreign policy toward the world; however, without an educated government workforce, the U.S.’s policy will be feckless. Finally, without these policies, there will quickly be a lack of democratic leadership in this emerging Cyber World Order. The world has yet to codify both the laws and norms of Cyberspace; without effective, dynamic cyber policies, the United States government will soon find that it does not control its own destiny in Cyberspace like it could in the postwar world.