VANGUARD
Integrity Professionals
Information Security Experts

6625 S. Eastern Avenue Suite 100
Las Vegas, NV 89119

TEL +1.702.794.0014 FAX +1.702.794.0023
www.go2vanguard.com

February 16, 2012

The Honorable Harry M. Reid
Majority Leader
United States Senate
Washington DC 20510

The Honorable Joseph I. Lieberman
Chairman, Committee on Homeland
Security and Governmental Affairs
United States Senate
Washington, DC 20510

The Honorable Susan M. Collins
Ranking Member, Committee on Homeland
Security and Governmental Affairs
United States Senate
Washington, DC 20510

The Honorable John D. Rockefeller
Chairman, Committee on Commerce, Science
and Transportation
United States Senate
Washington, DC 20510

The Honorable Dianne Feinstein
Chairman, Senate Select Committee on
Intelligence
United States Senate
Washington DC 20510

Dear Senators Reid, Lieberman, Collins, Rockefeller and Feinstein:

Vanguard Integrity Professionals strongly supports the recently introduced Cybersecurity Act of 2012.

Vanguard has provided large enterprises and government agencies with the information technology security expertise to protect their critical information technology resources for over 25 years. We are privileged to be currently engaged with NIST, DHS, DOD and other agencies, state governments, as well as many of the largest private enterprise owners of critical infrastructure in the United States, on cybersecurity issues that affect all of us on a daily basis.

We specifically support Title I of the Act. We are fortunate that the United States is one of the rare countries in the world where over 85% of what is defined as the "Critical Infrastructure" is privately owned, rather than government owned. Given today's interconnected and networked world, each entity, regardless of the effectiveness of its own security and compliance implementation, has the level of risk exposure of the least secure business partner that it interconnects with. When each entity in an interconnected world can choose which "best practices" are appropriate for its own risk appetite, interconnected business partners then have the level of information technology risk of the business partner with the greatest willingness to assume risk, or the least knowledge about appropriate information technology security.

The private sector attempts to address this today with complex series of cross contracts that require each connected business partner to certify compliance with another company's security policies. The result is complexity, expense and the multiplication of IT security audits or assessment using each

business partner's different information security policies and standards. In addition, many private sector companies today face a variety of different information security standards, contained in legislation and regulations issued under SOX, HIPPA, GLB, as well as consortium security standards such as PCI DSS, and finally each company's own internal standards and policies. The result is that some parts of the private sector today are sometimes "over audited" or "over assessed" against slightly different standards, with no discernible increase in actual security despite the cost of the audits and assessments.

Title I provides the first steps to ensure that minimum levels of IT security are in place to protect appropriate parts of the critical infrastructure in the private sector. We believe in particular that Section 106(b) and Section 105(e) will result in the wider adoption of appropriate minimum information security standards and implementation of minimum levels of security configuration controls, which may reduce the need for redundant audits and assessments against multiple different standards, and therefore will enable more attention be paid to implementing appropriate security policies and configuration controls.

We strongly support Titles II and III of the Act as well and believe that the improvements to FISMA are needed as soon as possible. The Federal Government needs to improve its implementation of information security as much, if not more, than the private sector critical infrastructure companies. The Act points to the specific NIST minimum standards, guidelines and checklists that will be used to implement and report on the state of the cybersecurity, and help ensure that the weakest link in the chain is as secure as the strongest. Continuous monitoring is a must. We also strongly support designating a central agency to be held accountable and lead both government and industry in cybersecurity implementation and reporting.

Most of the cybersecurity threats that have the greatest impact today can be effectively countered with education and existing technology properly implemented. Once we have done that across the board, all of us in government and industry will be able to focus resources on combatting advanced and evolving threats that need significant attention. The Cybersecurity Act of 2012 is an overdue step in the right direction to protect the critical infrastructure, national security and prosperity of our country. We appreciate the work done by the Senators and the staffers to introduce this Act.

Sincerely,

Steven G. Ringelberg
Chief Operating Officer
Vanguard Integrity Professionals