United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

July 1, 2010

Mr. John T. Chambers
Chairman, President and Chief Executive Officer
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134

Mr. Samuel J. Palmisano
Chairman, President and Chief Executive Officer
IBM Corporation
1 New Orchard Road
Armonk, New York 10504

Mr. Lawrence J. Ellison
Chief Executive Officer
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065

Dear Mr. Chambers, Mr. Palmisano, and Mr. Ellison:

On June 24, 2010, your companies wrote to us concerning the Protecting Cyberspace as a National Asset Act, S. 3480. We introduced this bill on June 10, and it was ordered reported by the Homeland Security and Governmental Affairs Committee on June 24 by a unanimous voice vote. This legislation is informed by years of oversight by this Committee and is the result of more than a year of drafting. Our staff spent considerable time working with industry representatives – including representatives from your companies – and the bill, as reported, addresses many of the concerns your companies raised during that time.

We hope that the information provided below will address some of the concerns and misconceptions you have about the bill and its scope.

Section 253. In your letter, you state that developing and implementing a supply chain risk management strategy for federal information technology procurement would "in effect, regulate the information technology sector." This statement is simply not supported by the text of the bill.

As an initial matter, requiring a strategy on supply chain security for federal information technology procurements – which will be developed in consultation with numerous agencies, councils, *and the private sector* – would not regulate the information technology sector writ large. Rather, this section directs the Federal Acquisition Regulatory Council (FAR Council) to use its existing authority over federal government procurements[1] to implement the strategy, in much the same way as efforts already under way at the Department of Defense and Department of Homeland Security (DHS) as part of Initiative 11 of the Comprehensive National Cybersecurity Initiative (CNCI).

Homeland Security Presidential Directive-23 explained the need for supply chain risk management for government information technology procurements:

> Globalization of the commercial information and communications technology marketplace provides increased opportunities for those intent on harming the United States by penetrating the supply chain to gain unauthorized access to data, alter data, or interrupt communications. Risks stemming from both the domestic and globalized supply chain must be managed in a strategic and comprehensive way over the entire lifecycle of products, systems and services. Managing this risk will require a greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions; the development and employment of tools and resources to technically and operationally mitigate risk across the lifecycle of products (from design through retirement); the development of new acquisition policies and practices that reflect the complex global marketplace; and partnership with industry to develop and adopt supply chain and risk management standards and best practices."[2]

We agree with this assessment, which is why section 253 creates a responsible, flexible, and comprehensive approach, in partnership with industry, to ensure that we have greater security built into critical federal networks and systems. We also believe that developing a single, unified, approach to this problem will be less burdensome for industry than myriad agency policies developed ad hoc.

Moreover, to ensure that this section does not place an unnecessary burden on industry, the bill requires the strategy "to the maximum extent practicable, promote the ability of federal agencies to procure authentic commercial off the shelf information and communications technology products and services from a diverse pool of suppliers." This is further echoed in the requirement in subsection (d) that the strategy "be consistent with the preferences for the acquisition of commercial items under section 2377 of title 10, United States Code, and section 314B of the Federal Property and Administrative Services Act of 1949 (41 U.S.C. 264b)." On numerous occasions, your companies have expressed the belief that industry is taking sufficient steps to

---

[1] Indeed, there are three cybersecurity cases currently pending before the FAR Council - FAR Case 2009-032, Sharing Cyber Threat Information; FAR Case 2009-030, Safeguarding Unclassified Information; FAR Case 2008-019, Authentic IT Products.

[2] The Comprehensive National Cybersecurity Initiative. http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

protect its supply chain and guarantee software assurance. Thus, the strategy should be consistent with the internal practices of most IT companies that do business with the federal government.

Your letter also raises concerns that Section 253 would require "all purchases by the government . . . to meet standards approved by NIST." But this requirement is not new; the National Institute of Standards and Technology (NIST) has had responsibility for some time in "develop[ing] standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency."[3] Only recently has the federal government began to leverage NIST's unique relationship with the private sector to help develop interoperable standards that will allow both vendors and agencies to come together and define what "secure" really means. In fact, in July 2007, OMB issued a memorandum to require information technology providers to use the Secure Content Automated Protocol – a technology-neutral, interoperable standard developed by NIST – to certify that their products would not unintentionally alter network security configurations. As such, your concern seems directed at current law and practice – not this provision, which supports NIST's important, ongoing work in this area.

Your letter also expresses concern that Section 253 will undermine the Common Criteria and suggests that instead the "Common Criteria should be reviewed and improved upon, so as to improve its weaknesses without losing its strengths." But your objections, again, are not supported by the text, as section 253 both incorporates international standards and provides a mechanism for recommending improvements where the standards are deficient. Section 253 explicitly requires that the strategy place particular emphasis on "the use of internationally-recognized standards and standards developed by the private sector and develop[ment of] a process, with the NIST, to make recommendations for improvements of the standards." Indeed, this provision was based largely on language recommended by your representatives.

Your letter also asserts that "the expertise in this area does not currently reside at DHS, the agency granted regulatory authority under the bill." First, as we noted above, the strategy is *not* regulatory in nature, as any change to existing procurement regulations will be done by the FAR Council using existing notice and comment procedures. Second, the statement reflects a misreading of the bill – the strategy is not a DHS product; rather, it will be the result of a broad inter-agency effort, as well as a partnership with the private sector, that will be led, but not dictated, by DHS.

Third, and more fundamentally, the responsibility for protecting the American people from a large-scale domestic attack – in any form – is at the heart of DHS's mission. It has responsibility for securing our nation's critical infrastructure, and for protecting the government's "dot-gov" domain. Quite simply, no other agency is as well-positioned as DHS to lead the cooperative effort set forth by Section 253. Any effort to secure our civilian government systems and our critical cyber infrastructure must leverage the mission and resources of DHS – doing otherwise would waste taxpayer resources on duplicative efforts at other agencies and exacerbate coordination challenges. DHS is already the department within the federal government building

[3] 15 U.S.C. 278g–3

partnerships with the private sector to secure our critical infrastructure and key resources, and Section 253 builds on that responsibility and capability.

Lastly, this section of the letter expressed concern that our bill would "circumvent" the authority of the National Security Staff's Cybersecurity Coordinator. We appreciate your expression of support for the concept of an overall federal coordinator for cybersecurity, and assure you that nothing in our bill will undermine the authority of such an office Instead, it would ensure that the Director has sufficient authority to set strategy and policy, oversee its implementation, and resolve inter-agency disputes, including in the development of the strategy that Section 253 would mandate. Our bill would also ensure that the Congress and the public (including industry) have full insight into the activities of the White House office.

Section 242. Our legislation, as your letter notes, creates a National Center for Cybersecurity and Communications (NCCC) within the DHS to elevate our nation's focus on the security of civilian government systems and vulnerable private sector networks, especially those that are most critical to our nation's welfare. The NCCC will serve as a partner with the private sector, relying on voluntary information sharing programs to gain a better understanding of the risk our nation faces from cyber threats. Your letter is correct that the responsibility of the NCCC would include "assist[ing] in the identification, remediation, and mitigation of vulnerabilities to . . . the national information infrastructure."

Among other ways, the NCCC would do so by promoting risk-based best practices established under Section 247 of the new law – best practices developed in consultation with the private sector and based to the maximum extent possible on existing private sector standards. The NCCC – at the request of the private sector – would be available to provide voluntary technical assistance. The programs our bill would establish at the NCCC would form the foundation for a collaborative relationship with the private sector – a relationship built on trust and interaction versus overly burdensome top-down regulatory mandates.

By working in partnership and voluntarily sharing information with the private sector, the NCCC will have a better understanding of the threats and vulnerabilities our nation faces in cyberspace, "situational awareness" of our nation's cybersecurity posture. In your remarks on the NCCC's responsibility to develop this "situational awareness," your letter asserts, incorrectly, that the bill would lead to the "deployment of government monitoring devices on private networks."

It is extremely misleading to argue that our legislation would grant the NCCC any authority to monitor or compel the production of information from the private sector. Indeed, the legislation expressly states – in numerous places – that it would grant no authority to the federal government to conduct surveillance on private networks or compel the production of information. Indeed, in the very section (Sec. 242(f)(1)(C)) cited in your letter regarding "dynamic, comprehensive, and continuous situational awareness of the security status of . . . the national information infrastructure," our legislation makes clear that the NCCC's analysis will be based on "sharing and integrating classified and unclassified information . . . on a routine and continuous basis" with several federal cyber operations centers and the private sector. Moreover, as it relates to the private sector, that section explicitly states that information will be shared with the NCCC from

"any non-Federal entity, including, where appropriate, information sharing and analysis centers, identified by the Director, *with the concurrence of the owner or operator of that entity and consistent with applicable law*." (Emphasis added). Indeed, our legislation carefully distinguishes between the "situational awareness" required under Section 242(f)(1)(C) and the "automated and continuous monitoring" that would be required for federal networks under Title III. It is simply incongruous to interpret section 242, as your letter does, as an authorization to deploy "government monitoring devices on private networks."

Section 248(b). The assertion in your letter that the regulatory authority in Section 248(b) is "apparently unbounded" is equally without merit. Quite to the contrary, our bill specifies that only those systems or assets whose disruption would cause a national or regional catastrophe could be subject to the bill's mandatory risk-based security performance requirements. To qualify as a national or regional catastrophe, the disruption of the system or asset would have to cause:

- mass casualties with an extraordinary number of fatalities;
- severe economic consequences;
- mass evacuations of prolonged duration; or
- severe degradation of national security capabilities, including intelligence and defense functions.

Thus, the bill sets up a process that clearly defines – and limits – the systems and assets that the Secretary of Homeland Security can identify as covered critical infrastructure.

Owners/operators who believe their systems and assets were erroneously identified as covered critical infrastructure will have an opportunity to appeal their coverage through administrative procedures. This will help ensure that only our nation's most critical systems or assets are covered by the risk-based security performance requirements in Section 248. Thus, we do not believe that the scope of covered critical infrastructure is overly broad, and it is simply wrong to claim that the reach of the section is "unbounded." In devising its regulatory structure, our bill appropriately seeks to protect against the most catastrophic risks to our country.

In implementing risk-based security performance requirements, the legislation also builds in flexibility for the owners and operators of covered critical infrastructure. The risk-based security performance requirements applicable to covered critical infrastructure would be developed in collaboration with the private sector and sector-specific agencies. These performance requirements would be targeted only at cyber risks to specific systems or assets that "if exploited or not mitigated, could pose a significant risk of disruption to the operation of information infrastructure essential to the reliable operation of covered critical infrastructure." Moreover, owners and operators would have the ability to choose the security measures that are right for their own systems and networks – so long as they meet the minimum performance requirements applicable to these high-risk systems and assets. In addition to this flexibility, the legislation would provide important incentives for complying with the risk-based security performance requirements – liability limitations for specified civil actions.

Your input on this important legislation is important to our Committee, and both our staff and yours have invested considerable time in this process. While we find the mischaracterizations of our bill in your letter inaccurate and disappointing, we welcome further discussion and hope that we can engage in a constructive dialogue going forward.

Sincerely,

Joseph I. Lieberman
Chairman

Susan M. Collins
Ranking Member

Thomas R. Carper
Chairman, Subcommittee on Federal Financial Management,
Government Information, Federal Services, and
International Security