National Security & Homeland Security Councils
Review of National Cyber Security Policy

Submission of the Business Software Alliance
March 19, 2009

Question # 1: What is the federal government's role in protecting critical infrastructure and information networks against a nation state attack?

The information technology (IT) industry has demonstrated a genuine commitment to working with the government in the critical infrastructure protection partnership. We have invested resources in this partnership, including industry subject matter experts, through such groups as the Critical Infrastructure Partnership Advisory Council (CIPAC), the sector coordinating Councils (SCC), the Information Sharing and Analysis Centers (ISAC), and others.

The role the government should play in protecting critical infrastructure and information networks is that of a true partner with industry. Specifically, the government needs to:

1. Closely, openly and transparently partner with industry to develop national cyber security strategy and policy.
2. Share threat information with industry.

Government-industry partnership in developing national cyber security policy

Our experience has been that the process by which the government has engaged the private sector has been at times extremely successful, and at other times much less effective.

In particular, we have often struggled to learn about aspects of the Comprehensive National Cybersecurity Initiative (CNCI) – both at the classified and unclassified level – and have often been brought into consultation only after key conclusions had already been reached. Government engagement with industry has also often been selective, rather than open and transparent – again, both at the classified and unclassified level. This challenge has been compounded by the over-classification of national cyber security initiatives and of the policy-making process.

It is of great importance to industry that the government make the process of national cyber security policy-making open and transparent, so that industry participation is as broad and deep as possible, both at the classified and unclassified level. It is also of great importance that classification be the exception

rather than the norm, as it should be reserved for areas that genuinely require confidentiality.

Sharing of threat information by the government

- *Current situation*

To date, sharing of information about threats, vulnerabilities and attacks between industry and government has largely been one-way, with industry sharing information with the government.

The government, however, has shared relatively little of the information that it gathers through its intelligence collection and investigative capabilities. This means that industry is lacking threat information that the government possesses that very likely would enhance its situational awareness, incident response and mitigation, and resilience.

This has been compounded by the fact that much of the information sharing takes place in the context of bilateral relationships between individual companies and the government. Greater emphasis needs to be placed on multilateral, sectoral or cross-sectoral information sharing mechanisms.

- *Solution*

The federal government needs to share with the private sector its threat information. The collection and sharing process should be:

- Coordinated across government.
- Equally open to all industry participants that comply with applicable rules (see next bullet).
- Governed by clear rules and standard operating procedures, which lay out the rights, roles and responsibilities of all government and industry participants.
- Focused on producing information that is actionable, i.e. timely and specific.

- *Required resources*

We understand that working with industry to establish the processes and trust to share information will require overcoming persistent and systemic resistance among certain government agencies. This will not happen without engagement from government's most senior leaders.

The government agencies taking part in this information sharing will need appropriate direction, legal authority, and resources, and be assigned specific roles and responsibilities. Existing structures between government and industry may

need to be adapted to share information in a trusted environment, but those structures provide a foundation from which to build.

- *Benefits of enhanced information sharing*

If the threat and vulnerability information that is shared with industry is specific, timely and actionable, it would improve situational awareness and give the companies that receive this information the opportunity to improve the security of their operations and information networks. Until an ongoing mechanism is in place and actually used to share government threat information with industry, it would be premature to address the issue of whether some form of regulation is needed.

Question # 2: What thresholds do we recommend for defining and reporting cyber incidents, and to whom does it get reported?

We believe that setting definitions and thresholds, and the corresponding mechanisms for reporting incidents must be done through a collaborative and ongoing process between government and industry.

This would ensure that the definitions, thresholds and reporting mechanisms reflect industry practices, rapid technological changes, the evolving threat environment and the operational experience gained in the context of the government-industry partnership. This process should also seek to enhance trust and the value of government-industry information sharing, by correcting the following problem: after companies report incidents, there is no standard or required feedback loop to inform them of how the government used the reported information.

Defining what constitutes a "cyber incident" is a first step that should be taken jointly by government and industry. It is important to note that this definition may have sub-definitions and varying triggers for reporting, based on the type of incident (e.g. product, internal environment, cyber crime, etc.) and its severity.

Question # 3: What changes are needed for the partnership to work? How can it lead to more action and accountability? Are existing government structures effective for public-private partnership engagement?

The answer provided above to Question # 1 addresses many of the changes that are needed for the partnership to work more effectively and lead to more action and accountability.

We believe that the existing Critical Infrastructure Partnership Advisory Council (CIPAC) framework is the right one for primary engagement with the private sector. Much work is being done under the CIPAC umbrella, and we do not want to lose that momentum. The sector risk assessments, which have been developed and are now being piloted, are a good example of this.

We would again note that government agencies often engage the private sector in an ad hoc manner, and the engagement is often based on bilateral relationships between specific agencies and specific companies or sets of companies. As a result, they are often redundant, or in some cases conflicting, and do not effectively leverage the CIPAC framework. Government can and must make more effective use of these collaborative mechanisms.

Question # 4: How do we increase security while preserving prosperity and innovation?

We believe that security, prosperity and innovation are not distinct goals that need to be balanced. In fact, they are interdependent. Therefore, we recommend that our national cyber security policy pursue three objectives that foster greater security, prosperity and innovation:

1. Preserve the global commercial off-the-shelf (COTS) model;
2. Enhance U.S. leadership in cyber security policy;
3. Create and implement a national cyber security research and development (R&D) plan.

- Preserve the global COTS model

We strongly believe that it is in the government's interest to ensure that policies preserve and foster industry's continued ability to develop and produce COTS technology through global supply chains.

Our industry's use of this business model yields many important benefits for agencies across the government. Our globally competitive, commercial technology industry offers to its government customers the most diverse and innovative set of solutions, at the lowest cost possible. This supports fundamental objectives of the Obama administration:

- Promoting the widespread use of transformative technologies by civilian agencies;
- Maintaining the superiority of U.S. defense and intelligence agencies; and
- Remaining fiscally responsible, by relying on the R&D investments of the private sector, and thus freeing up scarce dollars for government-specific R&D.

Simply put, the government cannot reach its security goals by compromising its access to commercial solutions and processes, nor can it technologically or financially afford it. Thus, the real issue centers on the need to prioritize security requirements relative to needs for the products to be delivered. Rather than imposing overbroad security requirements, government needs to be selective and limit them to high-criticality systems. Regulations or procurement rules would run counter to this objective and harm the global COTS model if they:

- Imposed technology-specific requirements about the integrity, reliability and trustworthiness of technology;
- Favored specific technology development models or processes;
- Were not based on transparent criteria developed in coordination with industry;
- Did not provide vendors fair opportunities to address concerns; and/or
- Drive divergent requirements from country to country.

➢ Enhance U.S. cyber security policy leadership

U.S. leadership in cyber security policy contributes to reaching the goals of improving security and helping commercial IT companies thrive in the global economy.

This leadership critically depends on U.S. cyber security policies that, while robust, are either developed in collaboration with our international partners, or are promoted internationally. The ultimate goal must be to produce a globally convergent, not divergent, policy framework. To reach this goal, the U.S. government needs to develop, and provide sufficient resources to implement a more comprehensive international cyber security strategy, and actively involve industry in its development and implementation.

➢ Create and implement a national cyber security R&D plan

Currently, we have disparate government and industry efforts, but no comprehensive, coordinated vision for cyber security R&D. Our nation needs a national cyber security R&D plan that:

- Identifies requirements, objectives and resources;
- Is developed collaboratively by the government and industry, because of the role that industry should play in implementing that plan, either on its own or in the framework of federal funding;
- Is not classified, but rather opened widely to input from stakeholders;
- Clarifies the ownership and licensing of the intellectual property (IP) created as a result of R&D activities supported by federal dollars. Currently, the status of that IP is unclear, which is a significant disincentive to industry participation;
- Directs the government's own cyber security R&D efforts (R&D either funded or performed by the government) toward: long-term and basic research; and applied R&D of specific security technologies or solutions that are not commercially viable and whose absence creates a measurable security gap.

Conversely, the government does not need to devote its scarce scientific, technological and financial resources to competing with industry to develop technologies or solutions that are commercially viable.