Testimony of Tim Brown
Vice President and Chief Architect
CA Security Management

Before the Subcommittee on Research and Science Education
House Committee on Science and Technology

Hearing on
"Cyber Security Research & Development"

June 10, 2009

Good morning Chairman Lipinski, Ranking Member Ehlers, and members of the subcommittee. My name is Timothy Brown. I am the Vice President and Chief Architect for Security Management for CA, Inc. I will testify today on behalf of CA. However, in several instances, I will also draw upon the cybersecurity policy positions of the Business Software Alliance (BSA), an association representing the world's commercial software industry and its hardware partners. CA is a member of BSA and we actively participated in the development of those positions.[1]

CA (www.ca.com) is one of the world's largest information technology management software providers, providing software and expertise support to more than 99 percent of Fortune 1000® companies, as well as United States federal, state and local government entities, educational institutions and thousands of other companies and governmental organizations worldwide. Founded in 1976, CA is a global company with headquarters in the United States, 150 offices in more than 45 countries, and more than 5,300 developers worldwide.

To strengthen relationships among research communities and our company, we established CA Labs in 2005. CA Labs works closely with universities, professional associations and government on various projects that relate to CA products, technologies and methodologies. The results of these projects include research publications, best practices, and new directions for products. We also work with many universities to enable and promote innovation—including funding university research projects in specific areas, working with faculty to enhance curriculum, and providing opportunities to interact with CA research and development experts.

I appreciate the opportunity to testify today on cybersecurity research and development (R&D), cybersecurity in higher education, and public education and awareness of cybersecurity. These three issues, which you raise in the questions you have asked that I answer, are of great importance to CA and to the cybersecurity of our Nation, and I commend you, Mr. Chairman, and Ranking Member Ehlers, for focusing on them. They correspond to three key aspects of cybersecurity: R&D is central to our capacity to provide innovative and secure information technology products and services; university-level

[1] The Business Software Alliance (www.bsa.org) is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cybersecurity, trade and e-commerce. BSA members include Adobe, Apple, Autodesk, Bentley Systems, CA, Cisco Systems, CNC Software/Mastercam, Corel, CyberLink, Dassault Systèmes SolidWorks Corporation, Dell, Embarcadero, HP, IBM, Intel, Intuit, McAfee, Microsoft, Minitab, Quark, Quest Software, Rosetta Stone, SAP, Siemens, Sybase, Symantec, and The MathWorks.

education directly impacts our workforce's ability to both develop and operate secure information technology products and services; and public awareness contributes to a sound foundation of technology and security savvy users.

INDUSTRY AND THE FEDERAL CYBER SECURITY RESEARCH AGENDA

I would like to start by addressing the issue of the role of the private sector in setting the federal cybersecurity research agenda. Specifically, you asked the following question:

> "*How does the private sector provide input regarding its research needs into the process by which the federal research portfolio is developed? Do you believe your needs are adequately addressed by the federal research agenda? How can the federal government more effectively partner with the private sector to address common research needs?*"

As a prelude, let me first say that the recently released Cyberspace Policy Review, announced by President Obama on May 29, reflects cybersecurity concerns understood by virtually all information security professionals. The state of cybersecurity today clearly shows that we need to deliver game-changing security innovations and practices. Cyber criminals, state and non-state actors, and other cyber adversaries move rapidly and adeptly to exploit weaknesses and vulnerabilities in systems, networks, applications and practices. They are successful at taking control of machines and stealing data. Their motivation may be monetary gain or broader, more sinister goals, but they all have the luxury of picking and choosing both targets and methods to take advantage of the weakest links available. They are increasingly sophisticated and technically adept. So today's reality is that we are in a very tactical arms race with our adversaries.

The software industry has raised the bar considerably in the past few years. We have implemented mature, responsible vulnerability disclosure practices, internal secure code training, penetration testing, and code inspection tools. Large software vendors now have security as one of the major architectural components of any software they build and have made important changes to their development processes based on the demand of their corporate customers. The industry has also worked to simplify security and make it more user-friendly.

However, we need to supplement these tactical successes with strategic ones. We face increasing cybersecurity risks emerging from factors such as the extension of the enterprise externally to partners and customers, the rapid pace of technology adoption, the integration of physical devices into a networked environment, and increasingly sophisticated threats. Industry's research efforts are typically directed to product feature development and relatively short-term objectives that have a high probability of success in the marketplace. Game changing, strategic research is a difficult investment because of financial risk and unclear return on investment. Because of this, federal research programs can and should look to longer-term research requirements that prepare us not for the past or present, but for the future, a research agenda that will focus on strategic, systemic and structural cybersecurity issues not addressable by short-term, tactical solutions.

The federal research agenda is laid down in the Federal Plan for Cyber Security and Information Assurance Research and Development (hereafter "the CSIA plan"). I will now address the shortcomings of this plan and of the process by which it was developed. I will also propose solutions to make this agenda more inclusive of the needs of industry. In doing so, I will draw upon the positions of the BSA.

First, while it identifies many worthy cybersecurity R&D priorities, **the CSIA plan does not propose national-level objectives**. Rather, it is an aggregation of the cybersecurity R&D objectives of the federal agencies that fund or conduct cybersecurity R&D. While it is appropriate for these agencies, in support of their individual missions, to have specific cybersecurity R&D objectives, their aggregation does not produce a cohesive picture of the nation's overall R&D needs.

CA and BSA recommend that the objectives of the CSIA plan be established on the basis of a truly comprehensive and holistic view of the cybersecurity needs of the nation. Once a set of comprehensive, national objectives has been identified with the input of government, industry and academia, then the plan can determine what entities – government, industry and academia, whether by themselves or in partnerships – are, or should be, pursuing each of them. The Office of Science and Technology Policy is responsible for coordinating the federal government's efforts surrounding cybersecurity R&D, and should ensure that federal R&D actually supports the nation's strategic cybersecurity goals. President Obama announced on May 29, 2009 the future appointment of a Cyber Security Coordinator in the White House. CA and BSA recommend that the Cyber Security Coordinator provide joint oversight and direction to this effort, alongside OSTP. Once a national framework for R&D has been established, individual agencies should be assigned R&D projects within their areas of expertise.

Second, for the CSIA plan to reflect the cybersecurity R&D needs of the nation, **a wide community of stakeholders needs to play an integral role in the creation of the plan and the identification of its objectives**. CA and BSA recommend that stakeholders, and in particular the owners and operators of critical cyber infrastructure and developers of critical cyber technology, be involved from the earliest stages of the process and throughout the creation of the plan, as well as when the plan's objectives and implementation activities are reviewed. The IT industry is a key stakeholder not only because it owns and operates the critical infrastructure of cyberspace and develops its underlying technology, but also because it invests tens of billions of dollars each year in R&D.

Another important avenue for identifying cybersecurity research gaps is via industry-government partnership initiatives organized jointly by the Department of Homeland Security and industry organizations such as the Information Technology-Information Sharing and Analysis Center (IT-ISAC) and the Information Technology Sector Coordinating Council (IT-SCC).

An extremely timely example of such an initiative is the IT Sector Baseline Risk Assessment, a major report that will be released soon, which results from a multi-year partnership between the IT-SCC, IT-ISAC, industry subject matter experts and DHS. The IT Sector's Baseline Risk Assessment is intended to provide a cyber and all-hazards risk profile that IT Sector partners can use in particular to inform resource allocation for security research and development in core IT functions. Those key functions include producing and providing IT products and services; incident management capabilities; domain name resolution services; identity management and associated trust support services; internet-based content, information and communications services; and Internet routing, access and connection services. With a powerful methodology for assessing risks and identifying necessary mitigation requirements, the Baseline Risk Assessment can serve as a foundation and industry-supported model for developing a strategic cybersecurity R&D agenda and plan of action.

I believe the inclusiveness is very much in line with the recently released conclusions of the White House Cyberspace Policy Review, which states that "*the federal government should*

greatly expand coordination of [NITRD and other R&D-related] strategies with industry and academic efforts."[2]

Third, in addition to contributing to the identification of the overall objectives of the national cybersecurity R&D plan, companies can play a role downstream in the **definition of specific R&D projects** that will contribute to reaching those national objectives. CA and BSA believe that it would be appropriate to facilitate federal support for specific research topics or projects that were not conceived originally by a federal agency, but rather pro-actively suggested to an agency by a company. In such a situation, the company is awarded funding as a "sole source." We believe a mechanism should be found that would make it easier for agencies to act upon such suggestions. Today, such a process is insufficiently used, because of legitimate concerns regarding the fairness of the award process. CA and BSA's goal is to encourage more companies to suggest promising avenues for cybersecurity innovation to the federal government. Naturally, projects pro-actively suggested by private industry should be closely related to the national R&D plan, as well as to the particular part of that plan that was delegated to the agency to which the idea was suggested.

We would like to make it clear that we do not in any way oppose the mechanism by which companies receive federal funding because they submitted proposals in response to a competitive federal solicitation. In fact, CA and other companies actively review and respond to such proposals, and we believe it should continue to represent a large part of the federal R&D funding. We merely want to find a way to ensure that, in addition to this reactive role, companies can play a more pro-active role in the definition of R&D projects.

Fourth, I would like to address the issue of short-term vs. long-term R&D. We believe it is appropriate to include both. As a general rule, however, **CA and BSA recommend that the government focus on long-term and basic cybersecurity research**. We believe it is appropriate for the government to be involved in applied R&D if: the technological solution that is sought is not commercially available; and its absence creates a measurable security gap.

In most cases, when government agencies seek to develop specific technologies, we are concerned that they do not check beforehand whether commercially available solutions provide the same or an equivalent capability. We recommend requiring federal agencies to ascertain whether or not commercial solutions exist—or could be readily adapted—before they invest in an R&D project to develop equivalent capabilities. This would allow the government to better leverage its limited resources. Importantly for industry, it would also ensure that the federal effort focuses more on research that may bring breakthroughs of considerable importance to the cybersecurity of our Nation's infrastructure in the long run, but lacks demonstrated short- or medium-term commercial viability. Commercial companies rarely undertake such research by themselves, but it is an ideal topic for federal research. This recommendation aligns with the White House Cyberspace Policy Review's emphasis on R&D in "*game-changing technologies that will help meet infrastructure objectives.*"[3]

We note, however, that cybersecurity research is underfunded when compared to other research programs. For example:

> "… the president's fiscal year 2009 budget requests $29.3 billion for life science research, $4.4 billion for earth and space sciences, $3.2 billion for the Advanced Energy Initiative, $2.0 billion for the Climate Change Science Program, and $1.5 billion for nanotechnology. The National Information

[2] Cyberspace Policy review, pp.32-33.
[3] Cyberspace Policy review, p.32.

Technology R&D (NITRD) programs will receive $3.5 billion. Cybersecurity will receive about $300 million."[4]

In order to increase cybersecurity for the nation, funding for fundamental and applied research in cybersecurity is required. Keeping current funding levels will result - at best - in maintaining the current level of progress and therefore the current inadequate level of cybersecurity.

Companies have an important role to play in fostering greater engagement with academic institutions and government. For example, CA today works with universities in a number of ways. Through the CA Academic Initiative, colleges and universities can get free access to select CA products, faculty education, professional courseware and technical support. CA also has a strong partnership with Universities for research. For example, CA is working with the University of California Davis and Pacific Northwest National Laboratory on insider threat research and with Dartmouth University on determining the benefits seen by organizations in the deployment of security software.CA is also working with Carleton University in Canada on data leak prevention research. This research is partially funded through the Canadian government's NSERC Strategic Network Grant.

Finally, for federal cybersecurity R&D to best address the needs of industry, it is important that we **facilitate the migration path of technologies developed through federal R&D**, so that they can more quickly and widely contribute to improving our Nation's cybersecurity. This is another issue on which our recommendations are consistent with the direction advocated by the White House in its Cyberspace Policy Review.[5] CA and BSA propose two avenues to ease technology transition onto the marketplace. First, provide greater incentives for industry to participate in federally funded cybersecurity R&D by looking at the status of the intellectual property (IP) it generates. We recommend that Congress explore ways to make such industry participation more appealing through improved IP ownership or licensing, similar to what Congress did for small businesses, non-profits and universities through the Bayh-Dole Act in 1980. Second, the federal government should improve its sharing of the innovations generated by cybersecurity R&D conducted by federal agencies. Too often, those innovations are not shared with industry, where they could benefit the nation as a whole through productization, even with licensing conditions that appropriately reward the agency in question.

SPECIFIC CYBER SECURITY R&D TOPICS

The second issue that you asked that I discuss in my testimony is that of specific topics and gaps in federal cybersecurity R&D:

> "*Does the current range of federally supported research adequately address existing cybersecurity needs as well as new and emerging threats? If not, then what are the current research gaps and priorities?*"

As I discussed above, we need a long-term, strategically-focused, national research agenda developed in partnership between the federal government and industry. As we look to the future, we see a number of trends that will impact both the cyber infrastructure as well as

---

[4] From "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency", December 2008, page 74. This report is available at http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf

[5] Cyberspace Policy review, p.33: "*To enhance U.S. competitiveness, the Federal government should work with industry to develop migration paths and incentives for the rapid adoption of research and technology development.*"

specific cyber functionalities. An understanding of these trends can be useful in informing research planning and prioritization. What are some of these important trends?

- **Increased bandwidth and connectivity to a virtually unlimited number of devices.** The number of devices connecting to the cyber infrastructure continues to grow: desktops, laptops, smart phones, GPS devices, cars, houses and many more to come. The available bandwidth continues to grow both in the cellular environment, the wireless environment and the wired environment. Managing cybersecurity risks in this new world will push our existing security technology beyond its limits given the sheer scale of networked devices and speed of communications.
  - CA recommends federal support for advanced research in the area of threat detection, systems management and security management allowing security controls to scale to this emerging cyber generation.

- **Huge amounts of storage and computing power will be present in the home, in the enterprise and in the network.** More sensitive data in huge volumes will be stored and shared among businesses, government agencies and consumers. The technical disciplines of digital rights management, data leakage protection, and data classification are in their infancy from a technology perspective. Digital rights management is the process of embedding and managing access control within data. Data leakage protection refers to the identification and control of sensitive data. Data classification refers to the process of tagging data to indicate it is sensitive, owned by an individual or part of a larger system, and to associate it with controlling policies.
  - CA recommends federal support for advanced research to move these technologies into the mainstream where data can be tagged appropriately and managed in accordance with policy-driven rules, under the control of the entity or individual responsible for its care.

- **Greater expectations for managing identity risks.** The exponential growth of interconnected applications and systems will require advances in identity management technology. Today's username and password model is inadequate. Stronger forms of authentication are available, but their acceptance and adoption have been slow. Similarly, the lack of a monetization model for strongly validated identities has limited their commercial success.
  - CA recommends federal support for advanced research to help with the development of new technology and new business models that are acceptable to consumers and industry.

- **Emergence of new, interactive social networking applications.** Social networking continues to go through many changes.
  - CA recommends federal support for advanced research to develop models enabling people to collaborate safely and securely, both to share the data they wish to share and to maintain anonymity as needed.

- **Universal business connectivity, collaboration and partnerships.** Businesses no longer operate independently; it is necessary for them to collaborate and share data as well as establish enforceable security policies. For example, a small hospital with 5000 employees typically has 50,000 people in its user directories and collaborates with other hospitals, universities and healthcare providers. Today's technology can support these business and clinical relationships, but more advanced technology is necessary to truly enable a secure and auditable infrastructure as the collaborative environment expands almost exponentially.

- CA recommends federal support for advanced research to enable a federated model where security and responsibility are technically manageable at the scales we expect to occur.

- **User manageability and interaction.** It is becoming more and more difficult for someone to live an unconnected life. Although technology has provided amazing capabilities, the device-human interfaces used to connect and interact with context and applications have not fundamentally changed.
  - Although browsers have greatly improved and are now being embedded in personal devices, as we look to the future CA recommends federal support for advanced research into flexible and manageable technical interfaces, displays and supporting instrumentality that incorporate seamless understanding, manageability and security functionality for users in many different environments and contexts.

- **Increasingly sophisticated cyber adversaries.** As I said at the beginning of this testimony, our cyber adversaries are sophisticated, they move rapidly and adeptly to exploit weaknesses and vulnerabilities.
  - CA recommends federal support for advanced research to create test tools and products that can identify vulnerabilities, logical inconsistencies and inappropriate "back doors." A new generation of tools would give application builders the ability to identify and fix vulnerabilities as well as meet industry security certifications more quickly and reliably.

- **The growing focus on insider threats.** As industry reacts to threats, cyber adversaries look for alternative business models. The insider is one of the most effective.
  - CA recommends federal support for advanced research into insider threat detection and advanced data leakage protection.

Let me now briefly turn to the final two questions you have raised.

CYBER SECURITY IN HIGHER EDUCATION

> *"What is the state of cyber security education? Are future cyber security professionals being adequately trained by colleges and universities to meet anticipated demands of the private sector? If not, what kind of cyber security training is appropriate and necessary for institutions to develop, and for what kinds of students?"*

My comments focus on the education of the technical workforce that will be responsible for the engineering of our applications, the implementation of our systems and the processes necessary to run these systems. Security is an important element to each one of these areas.

Cyber security education should consist of courses in secure coding practices, security architectures and security of complex systems. Colleges and universities have made great progress and security courses are mandatory in many programs. While still inconsistently deployed, there is also a movement within universities to incorporate secure coding practices into programming courses.

The level of security knowledge for graduates has greatly increased, but in many cases it lacks real world experience. The security knowledge tends to focus more on secure coding practices and less on implementation and system design. In order to fill the gap large

software vendors have implemented programs to reinforce security design and secure software development practices to their existing and new employees.

Separate from the issue of developing *secure* systems is that of developing *security* systems and architectures. In this latter case students require more specialized knowledge of security, such as identity and access control, authentication, threat detection and response, cryptographic systems such as public-key cryptography, etc. Knowledge at this level tends to be obtained at the graduate level, and can be broadly categorized as operationally focused (typically the Masters level degrees) and research focused (doctoral degrees).

The National Security Agency has a history of supporting security education through their National Centers of Academic Excellence in Information Assurance Education program, where they certify programs that meet a minimum set of requirements. These programs produce students who have a broad understanding of security and who can perform operational roles ranging from being responsible for the information security of an organization to understanding functional requirements for security-related software.

At the doctoral level, the focus is on longer-term research in order to improve the cybersecurity field. This requires not only students who are interested in cybersecurity research, but also faculty who are active in this field. Government support at this level consists of providing support for students (e.g., through National Science Foundation grants and scholarship-for-service programs) and of supporting faculty research. Such programs should be strengthened.

PUBLIC AWARENESS AND EDUCATION

Allow me to turn to the last topic that you had asked me to address, that of cybersecurity awareness of the general public. Specifically, your question was:

> "*What role can the federal government play in educating the general public about protecting themselves and their networks against cyber threats?*"

To address the need to increase public awareness of cybersecurity, I will draw upon the position of the BSA. CA and BSA believe we need to increase our national efforts to educate and raise awareness of the public about their cyber risks, and how they can protect themselves online, for two reasons. First, to decrease the likelihood that they will become victims of identity theft, and other harms that may befall them online. Second, to decrease the likelihood that consumers' computers will be hijacked to serve as launching pads for larger attacks against businesses, the infrastructure and our government – the botnet phenomenon.[6]

CA and BSA agree with the White House's Cyberspace Policy Review's recommendation that the federal government, in partnership with educators and industry, should develop a national cybersecurity public awareness and education strategy. Its objective should be to educate about the threat as well as about changing public attitudes online, towards greater cybersecurity as well as digital safety and ethics, to promote a responsible and ethical use of the Internet.[7] There are many such efforts: the National Cyber Security Alliance is a partnership between the Department of Homeland Security (DHS), the Multi-State

[6] A bot is a computer that has been infected by a cyber criminal – known as a bot-master – so that the bot-master can control it remotely and use it, along with many other hijacked bot computers, to carry out various types of large cyber attacks, from sending out spam and phishing emails, to disseminating to malicious code, to performing distributed denial of service (DDoS) attacks against banks or government IT systems. The largest networks of botnets (networks of bots) can number in the hundreds of thousands, if not millions.

[7] Cyberspace Policy review, pp. 13-14.

Information Sharing and Analysis Center (MS-ISAC), corporate and non-profit partners to promote cybersecurity awareness for home users, small and medium size businesses, and in primary and secondary education. Information about their year-round campaigns, which culminate in National Cyber Security Awareness Month every October – and I note that Congress has for several years now recognized the October campaign in a resolution of support – can be found at www.staysafeonline.org I also want to mention the www.onguardonline.gov effort led by the Federal Trade Commission, as well as the www.playitcybersafe.com campaign of BSA, which offers tools and educational material for children, parents and educators about how to use the Internet safely and responsibly.

One final comment: educational programs will be most effective when targeted to specific age groups. For example online activities may be very different for 5-10 year olds, 10-13 year olds, 13-17 year olds and people over 18. Each age group has specific needs and should have appropriate messaging and education. The non technical community in all age groups is moving to cyber platforms at an unprecedented rate, and all need to understand the rules and the risks in the context of their work, social and academic life, and environment. This is another area where partnership initiatives are vitally important.

* * * *

Mr. Chairman, Ranking Member Ehlers and members of the subcommittee, I appreciated the opportunity to appear before you to share some thoughts on cybersecurity R&D, cybersecurity education, and public education and awareness of cybersecurity. CA shares the subcommittee's goal of helping to enhance cybersecurity, and we would be happy, together with the Business Software Alliance, to work with you towards this goal.

I would be happy to answer any questions you may have for me.

Thank you.

Timothy G. Brown is the Vice President and Chief Architect for Security Management for CA, Inc. He has overall technical direction and oversight responsibilities for the CA security products. This includes Identity Management, Server Security, Data Leakage Protection, Web Access Management and Single Sign On.

With over 20 years of information security expertise, Brown has been involved in many areas of security including compliance, threat research, vulnerability management, consumer and enterprise identity and access management, network security, encryption and managed security services. In his career, Brown has worked with many companies and government agencies to implement sound and practical security policies and solutions.

Prior to joining CA, Brown spent 12 years at Symantec's CTO office, where he was responsible for companywide technical architecture, integration, gap analysis and technical strategy. Prior to joining the Symantec CTO office, Brown focused on Symantec's enterprise security architecture and the collection, correlation and prioritization of security data. Brown joined Symantec through the company's acquisition of Axent Technologies. At Axent he was responsible for the Identity Management, Single Sign On and multifactor authentication products.

Brown is an avid inventor with 14 filed patents in the security field. He is active in promoting cross industry initiatives and has participated on a number of standards boards.

Brown earned a Bachelor of Science degree in computer science from MCLA and has participated in the Wharton School of Business Executive Education program.