[H.A.S.C. No. 111–128]

# PRIVATE SECTOR PERSPECTIVES ON DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY AND CYBERSECURITY ACTIVITIES

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

HEARING HELD
FEBRUARY 25, 2010

U.S. GOVERNMENT PRINTING OFFICE
58–308 WASHINGTON : 2010

SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES

LORETTA SANCHEZ, California, *Chairwoman*

ADAM SMITH, Washington
MIKE McINTYRE, North Carolina
ROBERT ANDREWS, New Jersey
JAMES R. LANGEVIN, Rhode Island
JIM COOPER, Tennessee
JIM MARSHALL, Georgia
BRAD ELLSWORTH, Indiana
PATRICK J. MURPHY, Pennsylvania
BOBBY BRIGHT, Alabama
SCOTT MURPHY, New York

JEFF MILLER, Florida
FRANK A. LoBIONDO, New Jersey
JOHN KLINE, Minnesota
BILL SHUSTER, Pennsylvania
K. MICHAEL CONAWAY, Texas
THOMAS J. ROONEY, Florida
MAC THORNBERRY, Texas

KEVIN GATES, *Professional Staff Member*
ALEX KUGAJEVSKY, *Professional Staff Member*
ANDREW TABLER, *Staff Assistant*

# CONTENTS

## CHRONOLOGICAL LIST OF HEARINGS

### 2010



### THURSDAY, FEBRUARY 25, 2010

### PRIVATE SECTOR PERSPECTIVES ON DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY AND CYBERSECURITY ACTIVITIES

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS



WITNESSES



APPENDIX

# PRIVATE SECTOR PERSPECTIVES ON DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY AND CYBERSECURITY ACTIVITIES

---

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES,
*Washington, DC, Thursday, February 25, 2010.*

The subcommittee met, pursuant to call, at 2:06 p.m., in room 2118, Rayburn House Office Building, Hon. Loretta Sanchez (chairwoman of the subcommittee) presiding.

## OPENING STATEMENT OF HON. LORETTA SANCHEZ, A REPRESENTATIVE FROM CALIFORNIA, CHAIRWOMAN, SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES

Ms. SANCHEZ. Good afternoon. Before we begin, this is my first subcommittee hearing as chairwoman for this subcommittee, and I would like to share that I am extremely honored to be serving in this new role, and I look forward to working with the subcommittee members and staff.

I would like to welcome you all and thank you for joining us today to discuss cybersecurity, a high priority issue for the Department of Defense [DOD] and for the security of this nation as a whole and, I think, on an individual basis a high priority for many people who value their privacy.

Today our witnesses will be providing us with private sector perspectives on the Department of Defense's information technology [IT] and cybersecurity activities. Cybersecurity is an issue that I have been following very closely for many years, including in my role as vice chair of the Homeland Security Committee. Cyber threats have only recently received, I think, the attention that we should have been giving them the entire time, particularly within the defense community. DOD is continually working to gain a better understanding of cybersecurity and how to best protect this nation's cyberspace.

There have been many mainstream discussions in the press regarding cybersecurity lately, in particular because of the Google incident. However, there have been a number of high profile events against the DOD and others, including cyber attacks against Estonia and Georgian government forces, reports of intrusions into contractor networks to exfiltrate data on the F–35 Joint Strike Fighter, intrusions in to the networks that control our electricity grid, and intrusions on Pentagon e-mails as well.

Those are only a few of the incidents that we know of. Many people are unaware that our systems, especially our defense networks, are attacked on a daily basis. In the Department of Defense there are more than 15,000 different computer networks which are operated across 4,000 military installations around the world. We must protect those systems and ensure that information on them is only available to authorized personnel, and we must not only be prepared to respond quickly and effectively to cyber attacks but we need to invest what is necessary in particular resources to protect our systems.

That is why it is important that the government engage the private sector as a partner in cybersecurity and not simply as the technology provider that you have been for such a long time. There is a vast array of intellectual capital and expertise in the private sector. I should know because I am from California and a lot of the cyber people live there.

It is not consulted on key strategic questions, even though some of those decisions have as much impact on industry as on government, because sometimes government becomes the standard and then others take from them.

We should recognize that the private sector is very much a part of the DOD family, and we should treat it that way. DOD works with countless defense industries, and these industries must also be held responsible for handling classified and sensitive unclassified information appropriately.

While DOD may find it difficult to engage with industry, that is not the case for Congress, and we feel that gaining insight from the private sector is essential. We hope that the witnesses today will share their views on a broad range of topics to further inform our awareness of these issues as we work with the DOD to craft an appropriate strategy for defending and operating our cyberspace.

I feel the views of our private sector witnesses are a valuable complement to those views that we have within the DOD. For example, understanding the implications of how the recent QDR addressed the issue of cyberspace would be, I think, valuable to us and we would love to hear the thoughts on the proposed directions for the new established Cyber Command that the DOD has set.

A major focus of this subcommittee is on the science and technology [S&T] programs of the DOD, so getting an outside view on the proposed research agenda would also be valuable. And with a proposed increase of more than $70 million in new funding for computer science and security research in the S&T budget this year I would like to better understand, from a private sector perspective, if we are investing in the right thing.

If not, what should we be investing in and how much would that cost us? Because I believe we must better protect our information networks before we experience more situations where state and non-state actors are able to infiltrate our systems and not only steal data on our weapons system but also put lives in danger by disrupting military operations on our front lines.

[The prepared statement of Ms. Sanchez can be found in the Appendix on page 25.]

So let me quickly introduce our three witnesses. Today we have Mr. Phil Bond, who is the president and CEO [Chief Executive

Officer] of TechAmerica; Mr. David Bodenheimer, who is a partner of Crowell and Moring; and Dr. Fred Schneider, a professor of computer science at Cornell University.

All written testimony submitted by the witnesses will be included in the hearing record. Also, a reminder for subcommittee members that we will be adhering to the five-minute rule for questions. Once again, I want to thank our witnesses for being here, and I would now like to yield to my ranking member from Florida, Mr.—oh, Mr. Miller is not here.

Who are we ranking? Okay. Sorry.

Mr. Conaway, from Texas? From Texas——

Mr. CONAWAY. Yes, ma'am. Madam Chairman, your situational awareness is magnificent, yes.

Ms. SANCHEZ. From Texas?

Mr. CONAWAY. Texas.

Ms. SANCHEZ [continuing]. Will be filling in for Mr. Miller, and we will hear the opening statement from your side.

**STATEMENT OF HON. K. MICHAEL CONAWAY, A REPRESENTATIVE FROM TEXAS, SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES**

Mr. CONAWAY. Well, Madam Chairman, thank you very much, and welcome to the chair of the subcommittee. Looking forward to seeing you in your new role. It will not be long before none of us will remember Adam Smith and the role he played for a number of years as chairman. So congratulations, and look forward to working with you.

Rather than read Jeff Miller's statement—Jeff is on the floor working on the Intel reauthorization bill, which I will have to go as well in a few minutes, but I would ask unanimous consent to submit his written opening statement for the record and—if that is all right?

Ms. SANCHEZ. Perfect. I am sure Mr. Miller wrote something that is very, very good and we will put it in the record. And if you will yield back——

[The prepared statement of Mr. Miller can be found in the Appendix on page 27.]

Mr. CONAWAY. All right, yield back.

Ms. SANCHEZ [continuing]. I would again ask our witnesses one at a time to summarize your written testimony. We did receive it, and I think we even received it on time, which is great. And we will ask you to summarize in five minutes. We try to adhere to the five-minute rule here.

And we will begin with Mr. Bond.

**STATEMENT OF PHILLIP J. BOND, PRESIDENT AND CEO, TECHAMERICA**

Mr. BOND. Thank you, Chairwoman Sanchez and members of the committee. Privilege to be here on behalf of TechAmerica and representing some 1,200 member companies across the country.

Let me begin by thanking the chair and the members of the committee for raising these important issues and holding the hearing. Our members in our association share the panel members' concerns about these vital topics and the need to apply technology to every

aspect of national security, from the basement offices in the Pentagon to the warfighters in the battlefield.

We share a commitment to protecting these critical networks and infrastructure from attacks and disruption. Today I want to focus on two fundamental themes here: IT, which includes the procurement thereof; and then cybersecurity, including information assurance.

We believe that the inability of our IT acquisition process to keep pace with innovation indeed threatens our warfighters' technical advantage, and notably our adversaries are not tied up in the same red tape. Deputy Secretary Lynn put it well when he said: With IT technology changes faster than the requirements, faster than the budget process, faster than the acquisition milestone process. For all these reasons the normal acquisition process does not work for information technology.

To solve that problem, we recommend first that DOD should build a new cadre of acquisition professionals, people dedicated solely to purchase of large systems, much as is done in the private sector. The Department also needs greater flexibility in budgeting. We cannot afford to wait too much time in a world where cycles are so short.

There also is a need to restore and enhance commercial IT products and their use. There is an inadequate supply of STEM-carrying [Science, Technology, Engineering and Mathematics] degree workforce out there and that is a long-term challenge. Another long-term challenge is basic research. We are certainly supportive of substantial increases in basic research scheduled for DOD in the coming year.

On the second broad theme of cybersecurity and the related topic of information assurance, let me acknowledge the critical natures the chair mentioned about the collaboration between DOD and the private sector. In our view, DOD's dialogue with the private sector has been incomplete so far in this area—certainly engaged with the Defense Industrial Base, with system integrators that are a part of TechAmerica, but the vast majority of the commercial software development world is not a part of that conversation and needs to be. They have not been formally involved.

Related to any of these kinds of discussions about the collaboration on information assurance and—is a discussion of supply chains—excuse me. Again, here, government needs to work with industry to understand the global deployment, the benefits of it, and the risks of it. And then once you assess the risk, share the risk so that the very best minds in the private sector can help.

We would encourage some specific steps refocusing and reforming the existing certification processes, identifying commercial sector best practices and tools to expand their use within the government realm. We also would recommend creating a governance structure for assurance. We underscore the need to accelerate—accelerate the efforts in this regard.

Now, I want to suggest one idea in particular that we, as an association, have begun to explore, which is—the threat to national security is real. And perhaps there are other models we can use to bring the best of the private sector into collaboration with the best of the public sector.

So if you think of the Reserve model, which allows reservists to keep their civilian jobs, come in and do service—do their national service—and perhaps have the government salary supplemented by the private sector. But that legal framework might well apply so that leading cyber companies could donate talent on tours of duty, much like reservists, and really help the national security.

Finally, we think it is important to underscore that the leadership of DOD and the warfighter ultimately traces itself back to our leadership in the private sector in innovation and believe that therefore the Department should take an interest in the private sector leadership of American companies.

Let me make one other point quickly in summing up, which is that we note there are many efforts in information assurance and global supply chain assurance. So we encourage the administration to look at a single authority to consolidate and coordinate those.

And finally, Madam Chair, we would ask that the subcommittee consider a strategic review of Title X to see if in this information age there aren't some antiquated authorities that just have not kept up with the pace of technology that could be updated for the good of our nation's security.

Thank you.

[The prepared statement of Mr. Bond can be found in the Appendix on page 29.]

Ms. SANCHEZ. Thank you, Mr. Bond.

And now we will hear from Mr. Bodenheimer.

## STATEMENT OF DAVID Z. BODENHEIMER, PARTNER, CROWELL AND MORING, LLP

Mr. BODENHEIMER. Chairwoman Sanchez and members of the committee, thank you for your leadership on cybersecurity issues. Without cybersecurity we cannot maintain military superiority or economic security, and a vital key to cybersecurity is a robust public-private partnership. Quite bluntly, government and industry will either succeed together or fail separately.

I am David Bodenheimer, a partner in the law firm of Crowell & Moring, where I head the homeland security practice, specialized in government contracts, and work on ABA [American Bar Association] committees focusing on cybersecurity issues. Today I appear in my personal capacity to talk about cybersecurity, a topic that keeps me busy during the day and awake at night.

I will not dwell on the threat today. Nearly everybody agrees that the cybersecurity threat is imminent, relentless, and catastrophic, and it is getting worse. The cyber barbarians are stealing our secrets and our technology, they are plundering our databases and private information, and they are hacking into our critical infrastructure systems.

The real question is not the threat, but what we do about it. I have six points, six suggestions—Winston Churchill would say that is five too many, but let me see how many I cover—six areas where the Department of Defense and the private sector must work in tandem.

Number one: We must supercharge the public-private partnership. With the same urgency that we mobilized the industrial base in World War II, we need a public-private partnership to attack to-

day's cybersecurity threat so it does not become tomorrow's digital Pearl Harbor.

With the Defense Industrial Base Initiative, DOD has made a fine start with its pilot program for bilateral partnerships. Now we need to move from limited partnership to full partnership. Instead of a bilateral model with a few companies we need a bigger tent with more private sector players and broader participation. Additionally, full partnership should involve a two-way exchange of information before the decisions and strategy are cast in concrete.

Number two: We need more effective information-sharing. If we cannot connect the dots our cyber defenses are just another Maginot Line begging for a cyber ambush from the rear.

Too often the public sector gets information that is too little, too late, and too classified. For effective information-sharing the private sector needs timely data exchanges with context and analysis, two-way sharing not a one-way pipeline, and less classification with greater access.

Number three: We need clear, firm, and consistent cyber standards. Working to inconsistent cyber standards works about as well as serving two masters. It just doesn't work very well.

Multiple inconsistent standards drive industry crazy, and it is not just a military versus civilian standard issue. Sometimes even the Army, Navy, and Air Force don't agree. Getting clear, firm, and synchronized standards would give us better cyber defense at a lower cost.

Number four: We must encourage development of breakthrough technologies. The Department of Defense, specifically DARPA [Defense Advanced Research Projects Agency], brought us the Internet. We need that same big-brain research to deliver breakthrough technologies for cybersecurity that can leapfrog our cyber enemies, but at a cost we can afford.

Innovation can be energized in other ways as well, such as technology clearinghouses, DARPA prizes, and private fellowships. For cybersecurity, the more brains the better.

Number five: We need to stimulate cyber defense through liability safe harbors. Getting sued and penalized is a surefire way to shut down information-sharing and technology innovation.

For effective cybersecurity the private sector must share information not only with the Department of Defense but also its industry partners. To encourage that sharing we need safe harbors so that industry partners can meet minimum security standards and are not penalized with antitrust suits and other sanctions for cooperating.

Safe harbors can also accelerate innovation, such as we have with the SAFETY Act. We need to expand that so it also applies to companies in the cyber industry as well.

Number six: We need to assure due process and dispute resolution. In every partnership, partners sometimes disagree. In the government contracts business, pulling the plug on a government contractor that is connected to the DOD systems is effectively a cyber death sentence.

A private party should not be unplugged when someone else is responsible for a security breach. A disputes resolution process—perhaps a cyber board of appeal of independent IT experts—would

allow government to do its job while assuring due process for private sector in the event of such disputes.

As an old Navy guy I am proud to appear before this historic committee. We thank you for your leadership on this issue and welcome your comments.

Thank you.

[The prepared statement of Mr. Bodenheimer can be found in the Appendix on page 44.]

Ms. SANCHEZ. Thank you so much to the gentleman.

And now, Dr. Schneider for five minutes or less.

**STATEMENT OF DR. FRED B. SCHNEIDER, SAMUEL B. ECKERT PROFESSOR OF COMPUTER SCIENCE, CORNELL UNIVERSITY, COMPUTING RESEARCH ASSOCIATION**

Dr. SCHNEIDER. Thank you for inviting me here to testify. I want to focus on cybersecurity research and education. Military and civilian computing systems need to tolerate failures and to withstand attacks, but they don't. They are not trustworthy. And our dependence on these systems is increasing both for peace time and war time operations, often with system users ignorant of what they depend on and the risks of that dependence.

Moreover, we operate in a reactive mode and we improve defenses only after they have been penetrated. We thus prepare to fight the last battle rather than the next one. This means attackers always win round one.

We need to move beyond this reactive stance to a proactive one. In short, we must build systems whose trustworthiness derives from first principles.

The proactive approach requires having a science base for cybersecurity. Since we don't have one we need to develop one. But doing that will require making significant investments in research and the investments will have to be made on a continuing basis, for without continuity few will be inclined to make the intellectual commitment necessary to enter the field.

Unfortunately, cybersecurity will never be a solved problem. We are not going to find a magic bullet solution. Attackers grow evermore sophisticated. The systems themselves change as do the deployment settings, bringing new opportunities for attack and disruption.

So what research needs to be done? There have been 19 studies by federal agencies since 1997 each concerned with that question, each offering some kind of cybersecurity research agenda. And there is remarkable agreement among them all, so it is time to move beyond the list-making phase and embark on execution.

I will offer two observations about the conduct of cybersecurity research, though. First, when the work is classified it cannot engage many of the country's top researchers, it necessarily receives less scrutiny by a diverse community of experts, and it will be slow to impact the civilian infrastructure on which even the military so depends.

Second, cybersecurity once was funded by a diverse ecology of agencies and instruments—DARPA, MURI [Multidisciplinary University Research Initiative], AFOSR [Air Force Office of Scientific Research], ONR [Office of Naval Research], ARO [Army Research

Office], all within DOD, plus NSF [National Science Foundation], DHS [Department of Homeland Security], and some others. This diversity was valuable because different agencies have different needs, goals, cultures, and style.

But the diversity has been eroding. Getting that restored should be a priority, and it would undoubtedly bring better value for research dollars spent.

I earlier made the observation that today's systems are not as trustworthy as they need to be. The number of adequately trained cybersecurity professionals is obviously a factor here.

To start, universities need to hire more faculty and to teach cybersecurity courses and to expand their programs. Significant increases in research funding will promote this.

In addition, employers need incentives to hire system developers who have adequate training in cybersecurity. Government policies can help here but they can also cause grave damage. Some have advocated a cybersecurity credential for system developers as a forcing function.

The medical profession is a useful point of departure as it, too, is concerned with matters of life and death. Here, obtaining a credential requires far more than passing an exam. It requires years of postgraduate study in which the curriculum has been set by the most respected thinkers and practitioners in the field.

Second, credential-holders are required to stay current through courses sanctioned by the institution that issues credentials. Finally, the threat of legal action, such as malpractice litigation against a credential-holder incentivized professionals to engage in best practices. Eliminate any of these three aspects and I have grave doubts that the—about the success of the resulting scheme.

In closing, let me observe that the armed forces have a long and distinguished record of supporting research and education in cybersecurity and in systems trustworthiness, but our adversaries are now overtaking those early modest investments. We must now move from a reactive mode to a proactive one, which means creating a science base and significantly ramping up our research, and while we need to create a workforce that is up to the challenges of today and tomorrow, we need to be thoughtful about any policy incentives we impose to promote that.

Thank you.

[The prepared statement of Dr. Schneider can be found in the Appendix on page 72.]

Ms. SANCHEZ. Thank you, gentlemen.

I will remind my colleagues that we are going to work under the five-minute rule, and I will begin by asking questions.

Once again, thank you for being with us.

Dr. Schneider, you said we need to develop a science basis for cybersecurity, and then you spoke about how the medical profession trains and takes 10, 12, 15 years sometimes before they go out and really do their work. What would you envision would be a science-based cybersecurity pod?

What would it look like? Who would fund it? Would it be at some universities? How would we get the cross-pollenization of different things going on?

Dr. SCHNEIDER. There is an active research community in universities, and I would expect that most of the revolutionary ideas would come from that community. By a science base I would hope we come up with laws, like physical laws, that are independent of technology, independent of specific application problems, but that inform all our decisions about how to build systems.

And like we see in the medical profession, there is applied research, there are people who develop drugs, and there is basic medical science research. And without this basic medical science research we don't understand the mechanisms under which diseases operate, and therefore we don't have a chance of developing palliatives or cures.

And so really, medical research progresses on two planes. There is a basic research that builds a foundation and it enables specific research problem—topics to depart and address specific diseases, and I would expect that to happen in this setting as well.

Ms. SANCHEZ. Thank you.

Gentlemen, we just passed the cybersecurity bill in the House maybe about two or three weeks ago, and one of the amendments that I put onto it was to make it a little bit easier for academia to, in particular, respond and work with us at the government level, at the DOD level, to—with respect to the security clearances and this type of thing. What do you think are the major walls that are in place from having the public sector, the working public sector, the people who are commercializing some of this—actually doing their own basic research most of the time and commercializing, but also taking basic research we have and doing things.

What would you say are some of the barriers to working with our Defense Department or other departments of our federal government with respect to information-sharing and thought-sharing, and what would you say it is from the academic perspective from our universities and research centers?

And any of you can answer, or all of you, or——

Dr. Schneider.

Dr. SCHNEIDER. So, the risk of doing this is it might make visible to our adversaries what is working and what is not working, and that is primarily the concern about revealing classified data to a broader community. On the other hand, it seems pretty clear that we overclassify content with respect to cybersecurity. And there is a grave risk that academics and others who don't have access to this information will solve the wrong problem.

Mr. BOND. Let me add to that if I can. This is one of the reasons why we advocated this potential review of Title X to look at a number of things through that prism, because in a networked world we can bring people and ideas together more easily—academics with government, private sector and public sector. There are a number of rules, regulations, laws, authorities in place built in earlier times for good reasons and rationales of the time but which today represent large and small obstacles to just that collaboration.

If I can, with the analogy used earlier to the medical research efforts, the difference is you can't really talk to the disease or even the particle if it is really, really basic kind of physics research you are doing, but in this case we can talk to not only leading—leading thinkers and leading companies are talking to some of the folks

who are engaged in this kind of gray world between perpetrators and the rest of the world. So there are collaborations and conversations. We can learn more about what the adversary is doing, bring that through academic and private sector partners so that we get to that forward-looking agenda that Dr. Schneider talked about in his testimony.

Ms. SANCHEZ. Mr. Bodenheimer.

Mr. BODENHEIMER. I would agree that there are, indeed, legal barriers to the information-sharing between DOD and the private sector. There was a recent report in the U.S. STRATCOM [Strategic Command], which identified about 23 different laws bearing upon the public-private partnership in information-sharing. About ten of those have a direct effect upon the information-sharing issues.

We need a dual-pronged approach. One, as Mr. Bond said, we do need to look at some of those laws to determine whether there needs to be additional authority for DOD to share the information with the private sector. In addition, there are models for sharing the information, such as in the U.S. STRATCOM report, by using a nonprofit organization to receive the information and effectively serve as a clearinghouse.

I also agree with Dr. Schneider that overclassification has been an issue. I think that we do need some institutionalized methods, such as technology clearinghouses, with restrictions on access but still access so that industry and the Department of Defense can, in fact, work together.

Ms. SANCHEZ. I see that my time is up, and I am going to pass on to Mr. Marshall, my colleague from Georgia. Georgia?

Mr. MARSHALL. Thank you, Madam Chair. Congratulations on heading up the committee.

You note that there aren't a lot of members present, and it is not that we are all over attending the health care summit or watching the health care summit. We are certainly busy and we tend to focus on things that we think we might, you know, add some value to, and that might explain why so few of us are here.

I am a former law professor, you know, reasonably well-educated. I use computers all the time, and it is very difficult for me to follow a lot of—your suggestions actually are fairly straightforward and so I can follow the suggestions, I just don't have a sense of—enough of a sense of the problem, of the structure we currently have that is attempting to address this problem, and whether that structure that we currently have—those individuals who are currently doing this who have expertise I don't come close to having nor will I ever have—are the right experts to have. Are they appropriately structured? Do they have the appropriate authorities?

So I have to assume that you all are here because you do have some familiarity with how we, the government, are currently structured to try and analyze, understand this issue and then make recommendations to Congress concerning how we should proceed—make recommendations to Congress for how we should proceed. I fully accept Secretary Lynn's statement and your description of the urgency of this. There is no doubt in my mind that this is critically important; I just have no clue what direction to go in.

So with your familiarity with our structure can you tell me whether or not you are kind of comfortable with who is there, how they are organized, and what they are doing to try and tackle these issues that you are addressing today?

Mr. BOND. Let me take a first stab at your question, which I think is a good one and I note the attendance as well, which I think tells us in the industry something about our need to be better in terms of educating and engaging policymakers on this——

Ms. SANCHEZ. Mr. Bond.

Mr. BOND. Yes.

Ms. SANCHEZ. I might note for the record that the intel authorization is—intelligence authorization bill is up on the floor and many of the members who tend to be on this committee are interested in some of the matters there, so it could very possibly be—yes, and you know, we were shut down for two weeks here so everybody is trying to catch up. So it could be a matter of the timing as well as a matter of the fact that the intel bill is on the floor that we may not see some of the people here. But I know everybody is interested in it, and it is a very complicated, very difficult issue to get our hands around, but it is not because of you three.

Mr. MARSHALL. If I could reclaim my time here, it is definitely not because of the three of you, but I have been on this committee now for a while, and we have had hearings like this in the past, and they are typically not very well attended. And it is not because we aren't alarmed; it is not because we don't worry about this problem. It is because we don't really understand it very well.

And so we are hoping that we are appropriately organized, that we have the right people in the government organized appropriately to try and listen to folks like you and come up with the right suggestions for us, whether it is change the law, increase funding here or there, and that is my question: Do you feel like we do have those folks in place and that they are going to—and who are they, and how are they—are they appropriately organized, they are going to make the right recommendations?

Mr. BOND. I think there is an awful lot of talent across the government applied against some of these things, and indeed, as I tried to point out in my testimony, sometimes too much talent.

So if there are 12 different efforts on the same topic—that was what is behind our recommendation that the administration maybe look at a coordinator to bring those together; that was in information assurance. We also have the challenge of legal prohibitions on co-locating private sector and public sector folks together to work on some problems, and this challenge cries out for exactly that kind of thing.

Mr. MARSHALL. Okay, so you, having said that, are there—does Bill Lynn, for example, or the people who are advising him concerning these issues, do they agree? Have they made a suggestion to us the we modify the law in a certain way that would then permit them to do the kind of collaboration that they think is advisable and that you have in mind maybe?

Mr. BOND. On that last specific point, not that we are aware of. We have had direct conversations with Secretary Napolitano about it from a DHS perspective, so I know that she is aware of that, and

Phil Reitinger over there has identified that as something he would like to address. So those kind of discussions are going on, certainly.

Another one I would mention that is a specific challenge, I think, to Capitol Hill is the speed of innovation is so much faster than the speed of legislation that issues around budget flexibility, the color of money and when that money dies, how much flexibility you can have to respond quickly in a fast-changing technology environment, those would be challenges here with that branch of government that has the power of the purse.

Mr. BODENHEIMER. I would like to add to what Mr. Bond said. One of the things that we do see is a divided structure within DOD and the civilian agencies. One of the things that Congress has done well is to bring both from the Senate and the House side the staffs together into cyberjams, and it would be great to see a model like that, you know, within DOD and the civilian side as well.

We need to bring together the standards that we see on the DOD side with those on the civilian side and the IC [intelligence community] in a way that we have a single set of standards. We need the government—the executive agency speaking with a single voice.

Mr. MARSHALL. Just to sort of give you an idea of how far behind you I am, I—a single set of standards. What does that mean? You just want to stop it all, so, I mean, that is how basic my—there is a standard of acceptable—there is an acceptable level of——

You don't really need to tell me. I have never going to have that kind of expertise. I just want to know that the right people are in place doing the right things.

Dr. SCHNEIDER. So, the good news is you have some very good people. The bad news is they are not working in a context in which they can get the job done. And I am a professional computer scientist; I am going to become an amateur governmentist and point something out.

The Defense Department is dependent on lots of stuff that is highly vulnerable—the power grid, the communications infrastructure in the public sector as well as stuff that they operate themselves. There are some obvious things to make this better. You could imagine a staged plan where you start addressing short-term things, you worry about 10-year-out problems, and you worry about investing in research long-term.

If you go into the Pentagon and look around you will find nobody who is doing this, but what is worse is you will not find anybody who believes this is his or her job. There is nobody who feels it is job number one to create a program and to execute on it.

With the appointment of Howard Schmidt in the White House you could argue for the nation at large there has been some movement in this direction, but the Defense Department cannot depend on the efforts for the nation at large. Your needs are slightly different; your needs are more critical, and there needs to be somebody there. The people exist but nobody has that job.

Mr. MARSHALL. Why don't we just go back and forth? There are only two of us.

Okay. My impression jives with what I think I heard from a few of you, and that is that the technology that we use for most of our systems lags behind a little bit, and I think in part it is because of the process that we go through in order to develop it, and then

the concerns that we have concerning changing it. You know, so we change it here, how is it going to be compatible there? If we make this change how are we going to train people, et cetera?

And I wonder, is there an accepted mechanism for us to evaluate the effective—it would be very helpful if there were some way to—an accepted way where, you know—not going to be a lot of argument about this—to evaluate the talent and productivity of the folks that we have that are developing our software?

We have got a lot of software engineers out there that we are relying upon, I guess people who could be working for Google or Microsoft or what have you but they happen to be working for us on software for UAVs [Unmanned Aerial Vehicles], on software for communication, et cetera, in addition to cybersecurity stuff. How do we evaluate whether or not they're as talented as they need to be and productive as they need to be?

Mr. BOND. Let me take a first stab at that. It strikes at some fundamental issues, so I appreciate the question.

Much of the talent does come through private sector partners on a lot of the large projects and there are a number of metrics in the—from the very initial stages through contract performance and other things. I would take the question, if I could, and try to get back to you on how far down the chain those go to individual engineers and how much transparency there may be there.

So with your——

Mr. MARSHALL. No, no, that would be great.

Mr. BOND [continuing]. Forbearance we will try to take that and get back to you with something.

[The information referred to can be found in the Appendix on page 105.]

Mr. MARSHALL. And Dr. Schneider, if you would, I mean, the committee staff here is great and they have been really working on this issue for some time, and so if you could, if you would get back with committee staff on that. And then, Dr. Schneider, in your case, your thoughts concerning the absence of a mission within the Pentagon, people specifically tasked to these kinds of issues, if you could—it may be that it is in your testimony. If it is not, if you could share that with us in writing that would be very helpful if you could detail that.

And I am sorry, I interrupted—other thoughts about how we evaluate, or, you know, do we have the right talent pool, is it appropriately productive?

Mr. BODENHEIMER. One of the things that we need to do is to make cyber sexy to the people that are in the software business. For example, my nephew is an IT wizard. He has no interest in becoming involved in cybersecurity because there are so many other opportunities, and I think part of it is a marketing job and part of it is a credentialing job to make cybersecurity professionals stand out. That would make a difference.

Dr. SCHNEIDER. I am curious about your interest in evaluating the quality of people since ultimately we really want to evaluate the quality of the artifacts they produce. And if, for example, we could evaluate the quality of what they built—how secure it was—then we would have an easy way to determine how good the people who built it are. Certainly when you are going to buy a car you

read Consumer Reports or something and they discuss the car, they don't discuss the engineers.

The bad news is, we don't really have a way to measure security. We don't have a way to measure security or return on investment from defenses, and this isn't—and this is a hard fundamental problem. It is not something we are going to crack in the near term. It is something everybody appreciates is a big difficulty.

There is a famous quote that says, "If you can't measure something you really don't understand it," and the field is well aware of this. And this is a fundamental disconnect.

And the reason it is a difficult problem is because you don't know what to measure it against. You would like to measure it against some hypothetical attacker, but as soon as you deploy a defense the attacker gets wise and now you don't know what to measure it against because the attacker may go in any number of directions.

So this is the sort of problem that has eluded the field for some time. This is one of the reasons I have been advocating for the kind of science base, because I think that is the only hope for getting these measurements. But I think in the limit, we really want to be able to evaluate artifacts and not evaluate people.

Mr. BOND. I would, if I could, just quickly observe, too, there are a number of private sector-based efforts to measure the reliability and kind of fundamental code within software programs to increase your understanding of the assurance and reliability of that, and I wanted to acknowledge and then agree with Dr. Schneider's point, too, that one way of measuring that is to look at the overall product, and is it working, and the different levels of certification and other things.

Approaches to information assurance have tended to look at it that way: Okay, let us break it down by level of sensitivity, and therefore greater certification or greater assurance as you climb up that stack. So each would have a different metric assigned to it.

Ms. SANCHEZ. Gentlemen, what effect does having all these former—these legacy systems in the Department of Defense and sort of trying to hold on information and bring it forward and move on—I mean, this is one of the reasons why we have had at least hardware, in particular, sort of encumbered, if you will, in the sense of trying to bring forward these legacy systems. How does that impede us, or are we at the point where we could just do a sort of data dump and move forward into the next generation of whatever hardware and software will look like?

Are we in the process of doing that or are we still—I am thinking in particular to the DOD. Are we still encumbered with that? And I say that in the very naivest terms because I know, you know, if we have a fire in some warehouse where the files of our veterans are we could lose—I mean, there have been cases where we lose everything we know about them, basically, and we have to reconstruct from what they might have on hand. How does the legacy issue affect an ability for us, from the DOD standpoint, to move forward into this new arena?

Mr. BOND. I will take a first shot at that: I think that in the rapid changing environment that we are in, the information age, legacy systems are something that everybody deals with, and perhaps government more than many others because government, to

a large extent, is in the information business with its citizens and everything else, so I think that is a constant. And large and small companies deal with it every day, too. At my association I am sure most of my employees think our systems are too old and would like something new and so forth, so that is a constant.

What it takes me back to, though, is the recommendation—and this is really why we need a panel of some experts to help on these large-scale things, because it is like a multilevel chess game, you have a lot of things you have to factor in. How you are going to move information from the legacy systems, how much of those are interoperable? Is the new system going to be backward-compatible as you look at the next challenge and next generation?

These are exactly the kinds of things that private sector companies are dealing with all the time and could help the agency deal with, but I think to best assist that would be kind of an expert panel that can help on these, because these are very large, complex systems, old and new, that the Department needs to keep that warfighter at the very front on the edge.

Mr. BODENHEIMER. Let me address that from an acquisition standpoint. Many of these systems are in the process of being replaced through various ERP [Enterprise Resource Planning] procurements within the Department of Defense, you know, replacing the stovepipe systems and the legacy systems.

I think one of the most important things we can do is make sure that the contracts for replacing those old systems include the requirements for information assurance and information security in them. And in addition, I think that we need to take a hard look to determine whether the existing DOD standards—for example, the defense information assurance certification and accreditation program, DIACAP—is the right standard, is a sufficient minimum standard for applying to updating these legacy systems.

Dr. SCHNEIDER. New systems are more secure than old systems, but if you read the newspapers the front page is about attacks against new systems. I don't believe that moving to today's new systems is going to appreciably change how vulnerable DOD is to cyber attacks.

I think the only way to change things is to build systems differently, and that requires a different force field, whether it is economic policy, legislative, that changes the equation about how people are prepared to make investments when they build the system, whether they are prepared to spend more time testing the system, whether they are prepared to sacrifice complexity, because complexity gives attackers an edge. But just upgrading our systems to the latest is not going to appreciably change the vulnerability of DOD systems.

Mr. MARSHALL. I am certain that software engineers, as they develop products, have security in mind as they do so. How could you not? I mean, it is just sort of—it is all around you and your packages, your product is not going to be as attractive in handling—you are not going to—it won't be as attractive to the market, if the market is something that wants security, if you can't somehow establish the security.

Within the private sector when large software packages are being developed does the company go so far as to actually have red teams

that are trying to figure out ways to attack the product, to destroy the product, to—you know, what are the—it is not just relying on the software engineer who is designing the product to come up with security that is adequate, but actually trying to attack it. Do we have that?

I guess, Dr. Schneider, if we don't have anybody within DOD that is really specifically charged with the responsibility of worrying about these security issues we probably don't have red teams that are actually out there trying to penetrate or systems.

Dr. SCHNEIDER. No, actually DOD has some of the finest red teams in the world. What we don't have in DOD is somebody who is worried about the road map and making investments and executing on a plan to move the field and move DOD forward so that DOD is less vulnerable to all of the attacks that exist today——

Mr. MARSHALL. Well, if we have got the best red team in the world we are obviously concerned about cybersecurities, and yet we are not appropriately structured because we are not—we don't have the right mindset or the right division of responsibilities, or our attention isn't drawn to this adequately as we develop systems? Is that what you are saying?

Dr. SCHNEIDER. Yes, sir.

Mr. MARSHALL. And yet, here we are. It is national security. We know cybersecurity is an issue. It is hard for me to believe that we wouldn't have cybersecurity in mind as we develop our software products.

Dr. SCHNEIDER. Yes, sir. It is very disturbing.

Mr. MARSHALL. So you have made the statement that, in fact, we have this lack. How do you, you know—because frankly, if the chairlady here was convinced there was such a lacking this committee would be moving forward with whatever needs to be done in order to make sure that that gets fixed. So would DOD agree?

If we went to the folks in DOD who are principally responsible for this at maybe the undersecretary level and we said, "Geez, you know, Dr. Schneider says we are not structured appropriately. We don't have the right mindset. The products that we are producing are inadequate because of this failing." Would they say, "Yes, that is true"?

Dr. SCHNEIDER. I couldn't put words in their mouth, but I believe there are people who see it this way, yes.

Mr. BOND. If I can, I probably see it a little bit differently. I do think DOD is moving exactly that direction with the Cyber Command. There is a senior official in charge of information assurance, which goes to the supply chains and so forth. And I think in recent years, to your basic point, that there has been a greater emphasis and understanding of the need to build security into software even though companies certainly test, because their reputation and their brand is going to be at risk and can be—somebody can choose another product with the click of a mouse.

But that said, there is much greater awareness just in the last few years, nationally and throughout the software community—the entire high tech community—to put more attention and effort into building security in from the very beginning so that it is not just patches and things you bolt on the edge of your network or onto the software, but you build it in from the very beginning. And so

that should continue to increase because the risk and importance is only growing, but I do observe that in the last few years I think both the private sector and DOD and the public sector generally have been moving in that direction.

Ms. SANCHEZ. And I think that we have seen that, in particular working on the homeland side, with respect to the civilian side of the federal government. We certainly have seen a bigger impetus to—a momentum to try to get that done, and obviously also coming out of the White House and their cybersecurity czar.

Did you have a comment——

Mr. BODENHEIMER. Yes, Chairwoman. One of the things that I think DOD would agree upon is we do need the regulations—the acquisition regulations—out in public with comment and discussions. This is one area that the Department of Defense has shown leadership. They have prepared a set of acquisition regulations specifically addressing the information security issues. That puts DOD ahead of a number of other agencies which have not issued those regulations.

I think it would be a great thing to get those regulations through OMB and out into the public so we can comment and get those regulations improved and as good as they can be. It would then provide a gold standard for other agencies to use that as a model for acquisition.

Ms. SANCHEZ. Let me ask you, what is the role of the Defense Security Service in working with industry to secure industry unclassified networks? Do they have a role in any of this?

Mr. BOND. If I can——

Ms. SANCHEZ. Mr. Bond.

Mr. BOND [continuing]. I would just volunteer to get you more detailed input from some of our member companies——

Ms. SANCHEZ. That would be great.

Mr. BOND [continuing]. On exactly their perspective and what they would have the chair know about that.

Ms. SANCHEZ. I would like to see that. Great.

Do you have any more questions, Mr.——

Mr. MARSHALL. Yes, I do.

Mr. Bond, were you the one that suggested Reserve officers—Reserve—has that proposal been kicked around with DOD?

Mr. BOND. This is something that arose out of a conversation between CEOs and chief information security officers out in Silicon Valley with Secretary Napolitano where she talked about her—the challenge that agency has in getting enough skilled professionals in to meet the cybersecurity needs of DHS and the palpable frustration of everybody else around the table that they want to help defend their country and they feel like they can't. They want to give executives to the government for a short period of time; they want to supplement their salary or do whatever they can to try to help defend their country and they feel like they can't.

And so we began to look and talk to others in government about models that might already exist that would be a good framework that policymakers could quickly understand and the reservist model suggested to us seems to be one that everybody can understand quickly and say, "Okay, great. You keep your civilian job, you get to supplement the government salary, and you get to come back

to your civilian job. But in the meantime, go help defend your country."

Ms. SANCHEZ. And it sounds like a great idea. We ran into this on Homeland, actually, having been on Homeland since the inception of that committee, in just trying to fill the cybersecurity czar position over there in the Homeland Department. I would—and I am estimating—but having lived through it I would guess that 50 percent of the time that position was vacant, and that the other 50 percent of the time—I am talking about the first 5 years' worth—I believe we had six czars, and that the median stay of that—those czars might have been 6 or 7 months.

And the biggest problem we found was how do we pay them for what they are worth to come over and do that? And in fact, we had one of them who was supplemented, I believe through a university, maybe MIT [Massachusetts Institute of Technology] or one of the others that was a Northeastern University.

And there was a total outcry when the newspapers came out with the fact that they were funded by the university and only taking the $160K, or whatever, that we were paying the czar but had a total compensation package of $400 because—$400,000 because they were being subsidized by some university who, by the way, the deanship of that university or the flagship of that university was a private company. And therefore wasn't it amazing that this czar guy was considering that the best stuff was coming from, oh, by the way, the company that was funding the university's program that was basically funding—you know, I mean, you can imagine the iterations of what we went through with this.

So the answer is, the reservist model is a new thing for me to think about, but it is very difficult to figure out how we do that—and that is one of the things we have to think through if we do take a look at that—because, without naming names but more or less my—what I remember of the situation was people didn't stay very long because they weren't paid. If they were paid from the outside it was a problem.

These people came, they stayed for a while. What did they do when they left? They came back and they were the contractors to the Homeland Department to bring in, you know, other people's goods trying to sell us. So it is a very—it is a very slippery slope on how we get people to come in and give us good information, do the patriotic thing to their country, and at the same time not be partial to whatever it is their company is selling.

Mr. BOND. Couldn't agree more on exactly some of the challenges. I think one of the things that appeals to many of the executives involved about the reservist model is that it could be more widespread, so it is not about what any one individual and how they are gaming the system. The American people understand the reservist concept as well, and it could be a range of talent, too—it might be mid-level; it might be senior level folks for a while—but could be a range, and that therefore maybe that might be enough to get over some of those obstacles you identified.

I guess it does, in my mind, two other things: One, it underscores that this really is urgency. This is about national security and if we are serious about it then we should bring more people and talent to bear on it. And it goes to a point that was raised earlier

about making cybersecurity a little bit sexy, you know, that no matter where you work in the industry you can spend some time helping defend your country might be very appealing.

Ms. SANCHEZ. Thank you.

Mr. MARSHALL. Could I ask——

Ms. SANCHEZ. I will allow one more question.

Mr. MARSHALL. Pardon me?

Ms. SANCHEZ. I will allow you one more question.

Mr. MARSHALL. You are all familiar with how software programmers and others—you know, mid-level and higher level—the reservists typically come in for a brief period, leave for a brief period. How long do you think they would have to come in in order to be effective?

Mr. BOND. Well, I——

Mr. MARSHALL. On average.

Mr. BOND. This is——

Mr. MARSHALL. Too much in the weeds?

Mr. BOND. Well, no. I just think the answer would vary. I think just, you know, there might be longer tours of duty, there might be particular talents that you want to bring in, a shorter term on a project. So I think it probably would vary.

But also it is very much something notionally that some leaders in the space have talked about and have not had the benefit of enough thought and research yet to be a full-bodied proposal to you. But I think it does underscore how much the industry wants to help and how frustrated that they are.

Mr. MARSHALL. You know, it would be great—if you are representing 1,200 companies you obviously have resources. I think it would be wonderful if you could pull some folks together and explore this with some detail and get it to us, get it to DOD, you know, get it to whoever. And I think the chair listed some of the concerns that we would have; no doubt there are others out there as well. But the potential seems fairly obvious to me.

Dr. Schneider, I hear you when you say we should be looking at the quality of the product. I did mention productivity as well as talent, and in this arena, just like many others, obviously the talent of the workforce has a lot to say or to—a major effect on the quality of the product that you wind up getting, let alone productivity.

And so I hear Mr. Bond saying, and I think all of you would agree, that, you know, to the extent that we can organize ourselves in a way that brings to the table the best talent that the country has to offer to try to tackle this problem that affects both national security and—at a public level and a private level—then we ought to be doing that if there is a way to do that.

And I don't have to—I will never be an expert in this area, and I don't have to be an expert in this area in order to understand that we need to fund it, and if the right people are in place giving us advice concerning how to go about funding it then we will do it.

Mr. BOND. Well, I will commit to you that we will get back to you. Next week in San Francisco is the world's largest cybersecurity trade show. We will have a number of the CEOs who are affiliated with our association meeting at that and I will convey your message to them and we will get back to you with some thoughts.

Mr. MARSHALL. Thank you.

Ms. SANCHEZ. Gentlemen, thank you so much for being before our committee. As is the usual course of business, members will have some—a few days to ask some additional questions in writing and put them to you. We hope that you would answer them fairly quickly for our committee.

And with no other questions out there we will close the committee. Adjourned.

[Whereupon, at 3:09 p.m., the subcommittee was adjourned.]

# A P P E N D I X

THURSDAY, FEBRUARY 25, 2010

## PREPARED STATEMENTS SUBMITTED FOR THE RECORD

THURSDAY, FEBRUARY 25, 2010

**Statement of Terrorism, Unconventional Threats and Capabilities**
**Subcommittee Chairwoman Loretta Sanchez**
**Private Sector Perspectives on Department of Defense**
**Information Technology and Cybersecurity Activities**

February 25, 2010

"Before we begin, since this is my first TUTC Subcommittee Hearing as Chairwoman, I would like to share that I am extremely honored to be serving in this new role and I look forward to working with the Subcommittee Members and staff. I would like to welcome you all and thank you for joining us today to discuss cybersecurity-- a high priority issue for the Department of Defense and for the security of the nation as a whole.

"Today, our witnesses will be providing us with private sector perspectives on the Department of Defense's information technology and cybersecurity activities. Cybersecurity is an issue I have been following very closely as a member of the House Armed Services Committee and as the Vice-Chair of the Homeland Security Committee.

"Cyber threats have only recently received the attention they deserve, particularly within the defense community. DOD is continually working to gain a better understanding of cybersecurity and how to best protect this nation's cyberspace. There have been many mainstream discussions in the press regarding cybersecurity, in large part because of the publicity around the hacking attacks on Google.

"However, there have been a number of high profile events against the DOD and others, including cyberattacks against Estonian and Georgian government forces, reports of intrusions into contractor networks to exfiltrate data on the F-35 Joint Strike Fighter, intrusions into the networks that control our electricity grid, and intrusions on Pentagon email networks.

"In December, hackers reportedly were able to access information that included details about the South Korean and US strategy if we were to go to war with North Korea. These are only a few instances that we know of. Many people are unaware that our systems, especially our defense networks, are attacked on a daily basis.

"In the Department of Defense, there are more than 15,000 different computer networks which are operated across 4,000 military installations around the world. We must protect these systems and ensure that information on them is only accessible to authorized personnel.

"We must not only be prepared to respond quickly and effectively to a cyberattack but we must invest in the necessary resources to protect our systems. This is why it is important that the government engage the private sector as a partner in cybersecurity, and not simply as a technology provider.

"There is a vast array of intellectual capital and expertise in the private sector that is not adequately consulted on key strategic questions, even though decisions will typically have as

much of an impact on industry as it will on government. We should recognize that the private sector is very much part of the DOD family, and should be treated that way.

"DOD works with countless defense industries and these industries must also be held responsible for handling classified and sensitive unclassified information appropriately. While DOD may find it difficult to engage with industry, that is not the case for Congress, and we feel that gaining insight from the private sector is essential.

"We hope that the witnesses today will share their views on a broad range of topics to further inform our awareness of these issues as we work with the DOD to craft an appropriate strategy for defending and operating in cyberspace. I feel the views of our private sector witnesses will be a valuable complement to the views of the DOD.

"For example, understanding the implications of how the recent QDR addressed the issue of cyberspace, will be incredibly valuable, as would thoughts on the proposed direction for the newly established Cyber Command.

"A major focus of this subcommittee is on the science and technology programs of the DOD, so getting an outside view on the proposed research agenda would also be valuable. With a proposed increase of more than $70 million in new funding for computer science and security research in the S&T budget this year, I would like to better understand, from a private sector perspective, whether we are investing in the right areas. If not, where should we be investing this new funding?

"We must better protect our information networks before we experience more situations where state and non-state actors are able to infiltrate our systems and not only steal data on our weapons systems but also put lives in danger by disrupting military operations on the frontlines.

"Once again I would like to thank all of our witnesses for being here today and I look forward to hearing your testimonies. I will now yield to the Ranking Member from Florida, Mr. Miller for his opening statement. Thank you."

**Miller Opening Statement for Hearing on "Private Sector Perspectives on Department of Defense Information Technology and Cyber-security Activities"**

February 25, 2010

**Washington, D.C.**—House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities Ranking Member Jeff Miller (R-Florida) today released the following prepared remarks for the subcommittee's hearing to gather private sector perspectives on the Department of Defense information technology and cyber-security activities:

"I would first like to recognize the outgoing chairman, Adam Smith, for the exemplary work he has done as chairman of this subcommittee. Given the challenges and threats that exist in the world today, he pushed an aggressive schedule for the subcommittee that did much to inform the members and guide the decisions we made as a subcommittee. Although he has moved to chair the Air and Land Forces Subcommittee, I am glad that he will remain involved here. I would also like to welcome my Armed Services Committee colleague, Loretta Sanchez, as the new chairwoman. I look forward to working closely with you on the wide range of very important, and timely, issues that we handle on this committee.

"Recent events highlight the timeliness of this hearing on cyber-security. Earlier this month, the Director of National Intelligence, Dennis Blair, testified before the House Intelligence Committee and said, 'Sensitive information is stolen daily from both government and private sector networks, undermining confidence in our information systems.' He highlighted that this malicious activity is increasing in scale and sophistication, and the Department of Defense is one of the main targets of these cyber-intrusions and attacks.

"I fully believe that cyber-warfare is a reality that must be given full consideration. The potential impact of malicious activity is far reaching. State and non-state actors are always trying to gain an asymmetric advantage against our highly capable, and technically advanced, military. The exfiltration of F-35 data from a government contract's system and the massive attack on the Office of the Secretary of Defense that forced a shutdown of their system are only a few examples of recent incidents. Cyber-space is an increasingly important operational battlespace that needs to be understood.

"The Department of Defense is not alone, however. The attacks on Google reminded us all that the threat is shared between the government and private sectors. Shortly afterwards, the Kneber bot was discovered and revealed the reach of malicious cyber activity. Identified almost two years after the bot attack is believed to have first begun, this malicious botnet is estimated to have compromised almost 75,000 systems in more than 2,400 corporations and governments around the world. Criminal organizations, individual hackers, and groups affiliated with state governments are all believed to operate against private sector targets – from large businesses like Google to a private citizen's on-line banking account. Financial losses from cyber-theft have been estimated to be in the millions, if not higher, and the vulnerabilities in basic infrastructure systems like the electrical grid, transportation, and water management systems could be compromised with devastating affect by a cyber-attack.

"Much of the discussion regarding cyber-security necessarily centers on the technical means to defend and counter malicious activity. Advances in these areas are critically important, but adapting our thinking about cyber-space is also needed. Government, military, and business strategy must adapt its framework to take full advantage of all of the potential gains, and to avoid the many pitfalls, that accompany operations in cyber-space.

"Further, many have pointed to a legal system that has not kept pace with advances in technology and the evolving world of cyber. Identifying and prosecuting people suspected of criminal cyber activity is difficult at best. Concerns about privacy and civil liberties arise when the discussion shifts to counter-terrorism and intelligence operations in the cyber realm. We have tried to tackle these issues with changes to the Foreign Intelligence Surveillance Act, but we have still not fully addressed the problem given its scope and changing nature. Increased use of social networking sites, funds transfers from cell phones, and autonomous botnets like the Kneber bot are just a few of the challenges.

"We can learn much from the private sector, and with that I welcome today's witnesses. I hope that they will help us to understand how the private sector views the issue of cyber-security, in all its complexity and nuance. I will be very interested in what technologies you view as being keys to cyber-operations into the future, how the private sector approaches security, what challenges exist in maintaining an industrial and technological edge, and what legal issues concern you regarding operations in cyber-space. I look forward to your testimony."

TechAmerica
WHERE THE FUTURE BEGINS

TechAmerica.org

1401 Wilson Boulevard
Suite 1100
Arlington, VA 222094
P 703.522.5055

Testimony of

Philip J. Bond
President and CEO
TechAmerica

on

Private Sector Perspectives on Department of Defense Information Technology and Cybersecurity Activities

Presented to the Subcommittee on Terrorism, Unconventional Threats and Capabilities of the House Armed Services Committee

February 25, 2010

Chairwoman Sanchez, Ranking Member Miller and Members of the Subcommittee, I am Phil Bond and I serve as President and CEO of TechAmerica.[1] TechAmerica is the leading voice for the U.S. technology industry, which is the driving force behind productivity, growth and jobs creation in the United States, as well as the foundation of the global innovation economy. Representing approximately 1,200 member companies of all sizes and 16,000 more through an affiliation with the 40 local and regional technology groups belonging to the Technology Councils of North America, TechAmerica is the industry's largest advocacy organization. Collectively, our companies employ millions of America workers serving the public and commercial sectors of the economy.

We are pleased to present to you today the technology sector's perspective on the various aspects of Department of Defense (DoD) Information Technology (IT) and Cyber security activities. TechAmerica shares with the panel Members here today the goal of improving the security of our nation through the use and deployment of technology to every aspect of our National Security apparatus, from the back offices of the Pentagon to the warfighter in the battlefield. We are also committed to protecting the critical networks and infrastructure of our nation from attacks and disruption. The committee posed several questions to inquire about industry perspectives on information technology and cybersecurity activities and, because these are such expansive topics, I will divide my comments into two sections.

## Information Technology

### IT Acquisition

TechAmerica believes that we should place emphasis on reform of the IT acquisition processes used at the Department, and for that matter, the entire Federal government. Not doing so threatens the technological edge our warfighters have because of the inability of current processes to keep up with the pace of innovation. Our adversaries both in the battlespace and in cyberspace are not hindered by the red

[1] TechAmerica is the leading voice for the U.S. technology industry, which is the driving force behind productivity growth and jobs creation in the United States and the foundation of the global innovation economy. Representing approximately 1,500 member companies of all sizes from the public and commercial sectors of the economy, it is the industry's largest advocacy organization and is dedicated to helping members' top and bottom lines. It is also the technology industry's only grassroots-to-global advocacy network, with offices in state capitals around the United States, Washington, D.C., Europe (Brussels) and Asia (Beijing). TechAmerica was formed by the merger of AeA (formerly the American Electronics Association), the Cyber Security Industry Alliance (CSIA), the Information Technology Association of America (ITAA) and the Government Electronics & Information Association (GEIA). Learn more at www.techamerica.org.

tape slowing DoD technology acquisitions. To quote Deputy Secretary of Defense Bill Lynn:

> "…[W]ith IT, technology changes faster than the requirements process can keep up. … It changes faster than the budget process and it changes faster than the acquisition milestone process. For all these reasons, the normal acquisition process does not work for information technology."[2]

While such conditions are the result of many factors – ranging from the perpetuation of Cold War-era acquisition policies developed at a time when most technology was not even thought of yet to the drawdown of the acquisition workforce – they need our attention now to make sure that America does not lose its technological advantage.

TechAmerica was asked by the sister panel to this Subcommittee, the Defense Acquisition Reform Panel (DARP), to offer suggestions regarding IT Acquisition and I attach a copy of those suggestions to my testimony for your review and action. We identified four areas where we thought the Armed Services Committee would be able to contemplate and propose legislative solutions.

These are: Acquisition Workforce for IT, Budget Flexibility for IT Programs, Development and Management of Major Automated Information Systems, and Access to Commercial IT Products and Services.

- Acquisition Workforce for IT. DoD does not currently have sufficient organic acquisition resources and capabilities to effectively acquire information technology. In addition to other on-going acquisition workforce enhancement efforts, TechAmerica believes that the Department should establish a cadre of acquisition professionals dedicated solely to the acquisition of information technology products, services and systems. This practice is common in commercial companies that acquire large volumes of complex IT products, services, and systems. Such specialists develop and maintain a thorough knowledge of the products they acquire and an understanding of their companies' purchasing processes. Conversely, government procurement professionals are expected to be proficient in their knowledge of the acquisition rules and regulations that guide their actions.

[2] Defense IT Acquisition Summit, November 12, 2009

- Budget Flexibility for IT. Unfortunately, the acquisition approach for acquiring major automated information systems (MAIS) is beginning to mirror the more traditional MDAP acquisitions. While one can debate whether overseeing and managing large MAIS programs in a manner similar to MDAPs is desirable or not, the need to rapidly acquire information technology to meet warfighters needs in an era where technology cycles are measured in months rather than years is more comparable to rapid contingency contracting than to a traditional MDAP acquisition.

  Successful rapid acquisition requires flexibility in budgeting, as there is no time to wait years to program for funds under the current budget process. By the time funds are obtained to start a program, technology may have leapfrogged by two generations calling into question the approach taken in the original request. Addressing this funding dilemma is critical if DOD is going to leverage the rapid changes occurring in the information technology sector. Combatant commanders should have the ability (not contingent on an ongoing war) to rapidly tap into funding sources for information technology to meet urgent needs of the warfighter.

  Moving beyond the immediate needs of the combatant commanders, the need to refresh technologies and implement a more incremental IT acquisition approach also requires a more flexible budgeting approach. One such approach was outlined by the Defense Science Board in its March 2009 report on the Acquisition of Information Technology as "level of effort" funding. However, current "color of money" issues that distinguish between R&D, Procurement, MILCON, and O&M funds will make it difficult to implement "level of effort" funding, make little sense in funding incremental IT operations and modernization and serve as a barrier to successful IT acquisition.

- Improving the Way DoD Develops and Manages Major Automated Information Systems. As noted above, the government workforce needs material improvement that will take years, not months. In the meantime, the government must continue to acquire IT. TechAmerica recommends three actions that can be taken to improve the process during these years of transition and beyond in the most difficult IT procurements, large transformative IT programs. These are:
  - Authorize the creation of an expert panel to provide objective, professional oversight. This panel would be called upon to provide reasoned, professional assistance and oversight when necessary and give government employees making such judgments protection from second-

guessing by various oversight bodies. Drawn from a pool of respected and objective leaders in IT program management and business transformation, 3-member panels would engage when a program determined that expert help was needed or an oversight entity questioned the appropriateness of IT-related decisions.

- IT Projects should be Limited in Scope, but Scalable to Serve as Solid Foundations for Following Phases. We support the Defense Science Board's (DSB) recommendation that IT projects be limited in scope to simplify the procurement and to allow functionality to be added in useful increments. Called spiral development by the DSB, TechAmerica would place more emphasis on designing each segment or phase to schedule and cost that the DSB might.

  As noted by the DSB and the Acquisition Advisory Panel, DoD and the government as a whole has a requirements development process that needs vast improvement. For IT procurements, the requirements process is not quick enough to stay current with advances in technology. Thus, expecting requirements to accurately capture the technology available in the time the work is done is unrealistic. Until the government workforce that defines IT requirements gets the resources and training required and gains necessary experience, there is little question that requirements may need to be changed and likely scaled back during a program, to meet schedules and budgets.

- Focus on Program Level Engagement First. TechAmerica endorses the DSB's call for "enhanced stakeholder engagement," but would focus immediately on engagement at the program level, building toward enterprise level engagement. We further recommend that selected major IT programs would have assigned during the initial concept development phase and continuing through delivery under the contract, a single manager with a dedicated, stable team representing all major stakeholders. For example, when the Department of Defense intends to acquire an IT system directly affecting warfighting, the team would include at least: (1) the Combatant Commands; (2) DoD or Service CIO office; (3) the Comptroller; (4) government relations; (5) DCAA[3] (6)

[3] This is a significant departure from normal separation of program and audit functions but the assigned auditor could be from a different branch or a different audit organization from DCAA. Costing and pricing considerations need to be represented but not so as to bind subsequent auditors.

Acquisition office; (7) the affected service (if it is a joint program, representatives from each affected service.); (8) Logistics, if there would be any material impact on logistics (many IT programs are delivered and then maintained through hardware and software updates with little other logistical impact); and (9) other stakeholders, such as CECOM if communications were being modified.

- Restore and Enhance Access to Commercial IT Products and Services. We note that it is widely recognized that IT technology refreshment cycle times are turning over much more rapidly than in the past, certainly far more quickly than is the case for major weapons systems. Yet, the acquisition processes used to acquire IT systems and major weapons systems fundamentally are the same. Additionally, the Department (and the Federal government as a whole) has seen a significant decrease in its influence in the Commercial IT market space. DoD, by far the department with the largest IT budget[4], accounts for slightly more than .1% of dollars spent globally on IT[5]. Its presence is further diluted because of the decentralization of buying activities for commercial IT. Indeed, although DoD spends a considerable amount of its budget on IT, the average contract action has declined in size from nearly $2.5M in 2000 to $204K in 2007[6]. This reduction in size and the corresponding decentralization of buying activity also reflect the reality that DoD and the Federal government also have diminished influence on the innovations that are introduced in the commercial market, as well as the functionality that those innovations incorporate.

  The last two decades have brought a significant amount of statutory and regulatory change to the acquisition of products and services for Government use, including the enactment of laws such as the Federal Acquisition Streamlining Act of 1994 (FASA), the Federal Acquisition Reform Act of 1996 (FARA), and the Services Acquisition Reform Act (SARA). The main thrust of these statutes and other broad acquisition reform tools has been to enable a transition in the federal acquisition space from a system based on Government unique requirements under strict design specifications to one centered on the acquisition of commercial items to meet the Government's needs.

---

[4] FY2011 Budget Submission by President Obama, DoD request is $36.5.

[5] Gartner Says Worldwide IT Spending to Grow 4.6 Percent in 2010

[6] Structure and Dynamics of the U.S. Federal Professional Services Industrial Base, 1995-2007, Center for Strategic and International Studies, February 2009

Like all large institutional processes growing to maturity, however, FAR Part 12 has become burdened with added regulatory and process requirements over time, resulting in the layering of more formal acquisition processes onto the framework of commercial item acquisition (for example, cost element documentation requirements). This has led to a reduction in the efficient use of commercial item acquisition. This impact has been felt most acutely and notably in the ability of the Department and government as a whole to acquire commercial Information Technology (IT) products, services and systems at a pace timely enough to meet government's requirements and still be state of the art.

To the extent that such government acquisition processes vary from those found in the commercial marketplace, they serve as a real and significant deterrent for entry into the Federal market, particularly for small- and mid-sized businesses that frequently do not have the resources to pursue opportunities because of the compliance burden. Some of the government unique acquisition requirements include, but are not limited to: False Claims Act, Trade Agreements Act, Cost Accounting Standards, Truth in Negotiations Act, Audits by the General Accountability Office (GAO) and the Defense Contract Audit Agency (DCAA), suspension and debarment, Administrative Contract Oversight, organizational and personal conflicts of interest, constrained dialogue, bid protests and the delays they cause within the process.

TechAmerica recommends that Congress take a fresh look at IT Acquisition with the creation, funding and staffing of an IT Acquisition review panel similar to the DoD Advisory Panel on Streamlining and Codifying Acquisition Laws (the Section 800 Panel). That panel, funded administratively and staffed with a cross-section of recognized experts from industry and government, embarked on a comprehensive review of the entire acquisition system and yielded the recommendations that led to many of the reforms embodied in the Federal Acquisition Streamlining Act and the Clinger-Cohen Act. We believe the process would be well served by a similar exercise for IT Acquisition.

Finally, we have identified three acquisition models for consideration by the Subcommittee as pilots that could improve the way we acquire IT. These are: the traditional design-bid-build approach for construction authorized under the Brooks Architects-Engineers Act; the two-phase design-build construction procurement process implemented under FAR subpart 36.3; and, a Joint

Solutions Procurement Process used by the Canadian province of British Columbia to acquire sophisticated IT systems. TechAmerica believes all three hold promise as ways that DoD and the Federal government can reform the options for efficient and timely acquisition of information technology.

**Science, Technology, Education and Math (STEM) training**

TechAmerica is fully aware of the very concerning decline in STEM-educated graduates and is concerned that we are not doing enough to ensure a pipeline of graduates in these critical disciplines. Such a decline threatens our innovation economy and standing in the global marketplace. Studies have identified that our society and culture have lost the challenges for educational excellence that emerged as part of the space race of the 1960s, to the point where students today are actively discouraged from considering STEM curriculums and careers by counselors and parents. Sadly, there is a perception that such educations do not lead to successful careers and financial stability.

There is some movement on this front, but much more needs to be done, particularly at the K-12 levels. Because of the cultural leaps and bounds that technology has afforded the post-boomer generations, we believe that more attention should be given to the use of that technology to communicate with and engage students. Many programs rely upon traditional mentor-protégé arrangements at the secondary and post-secondary levels. While these programs are effective, they are also limited in scale and numbers; too limited to meet the needs of our nation. Impressions are formed far earlier in the formative mind and we must engage students through technology at an early age for STEM careers.

In the near term, we encourage the Subcommittee to express support for reauthorization of the America Competes Act as an incubator for education programs in STEM. We also ask that Congress support the large increases in basic research in the FY2011 budget proposal, which will help spur the next wave of America innovation and train the next generation of scientists, technologists, engineers and mathematicians. For DoD, that is an increase of about 16% to $1,999 million.[7] Congress must contribute to a national effort to encourage students to pursue STEM educations.

**Research & Development**

[7] Task Force on American Innovation

A stronger, permanent R&D tax credit is still a badly needed incentive for spurring future research and development in the United States. Companies cannot adequately depend on credits that expire, making temporary credits an ineffective incentive for the technology industry. By comparison to other countries where R&D incentives are far more compelling, the United States is losing its ability to attract research and development activities to its shores.

In the near term, we encourage the Subcommittee to express support for reauthorization of the America Competes Act as an incubator for education programs in STEM. We also ask that Congress support the large increases in basic research in the FY2011 budget proposal, which will help spur the next wave of America innovation and train the next generation of scientists, technologists, engineers and mathematicians. For DoD, that is an increase of about 16% to $1,999 million.[8] It has been many years since Government played a significant role in research & development and these increases are an encouraging sign that trend may be reversed.

## Cybersecurity and Information Assurance

Threat Sharing

TechAmerica has for some time now expressed concerns about the incomplete dialogue that DoD has with industry regarding IA threats. Historically, their focus has been on the systems integrator community (defined as the Defense Industrial Base or DIB) and, while those companies are members of TechAmerica and an indispensible community to engage for any discussions on IA threats, the vast majority of the tech sector is not formally engaged in threat sharing activities with DoD. Such a lack of dialogue leaves an incomplete picture for both the Department and industry. It is difficult to envision a thorough discussion on IA threats when commercial software developers and original equipment manufacturers are not formally part of the conversation.

Recently, the Department extended the Defense Industrial Base initiative (DIB/IA), which heretofore been a relatively limited effort to protect unclassified DoD information that resides or transit on a DIB information system or network through the release of Instruction 5205.13. This memorandum assigns responsibilities for fourteen separate DoD entities and subagencies and will have a broad and significant

[8] Task Force on American Innovation

impact on industry and its' ability support the Department to meet mission goals. As noted above, it is our hope that the Department will engage all of industry to effectively implement this new effort.

To promote a more robust and thorough dialogue and better protect the security interests and infrastructure of the National Security community, TechAmerica would recommend that the Subcommittee consider developing report language for the FY11 Defense Authorization Act. That language would require the expansion of DoD's threat sharing activities to formally include all of the industry elements comprising the tech sector as part of the implementation activities of Instruction 5205.13.

Certification & Accreditation

In July of last year, TechAmerica applauded the release of a Memorandum establishing reciprocity for certification and accreditation (C & A) for information systems across the Department. Industry has long had concerns about the lack of coordination between the C & A processes at DoD, particularly when companies would be forced to test the same device to the same or very similar standards or criteria for different testing entities. Such testing is frequently very expensive for companies and can take months to complete. Repetitive testing also delays the acquisition of technology products, frequently delivering second or third generation old products to the warfighter. It is our hope that the Department will engage industry to participate in the development of a reciprocally accepted C & A process and a DoD APL. We also hope that the Subcommittee will monitor this process as it develops to ensure that services and agencies do not seek to preserve independent certification and accreditation processes, thereby negating any efficiencies that reciprocity would have achieved.

Global Supply Chain Assurance

In 2007, TechAmerica collaborated with the Center for Strategic and International Studies to release a report[9] regarding industry recommendations for demonstrating assurance in the global supply chain. Those recommendations are still valid in this discussion. They include:

**1. Assess the risk (and share the assessment).** Inserting malicious code into software during the production process (whether overseas or in the United States) is only one of several attack options available to opponents.

[9] Foreign Influence on Software: Risks and Recourse, CSIS, March 2007

Responsibility for collecting information about opponents who are considering such attacks and the form these attacks might take should be assigned to the Intelligence Community, and the information shared among agencies and with appropriately cleared company representatives. Government and industry can develop formal processes to improve the exchange of information about threats and vulnerabilities to inform and coordinate their risk assessments.

**2. Focus on assurance, not location.** In the past, it was safe to assume that technology produced in the United States by a U.S. firm did not contain intentional vulnerabilities. This assumption no longer holds. Even if the technology is manufactured in the United States, the global nature of business means that this alone does not guarantee trustworthiness. An American company is likely to have employees from a broad range of countries. Foreign intelligence agencies could take advantage of the increasing internationalization of business to insert or recruit insiders, including U.S. citizens, with access to software production in the United States. Moreover, the borderless nature of information networks – one of its great attributes – means that malicious actors can be anywhere to access their targets anywhere, even in the U.S., if the appropriate protections are not in place.

The place where companies make software is not the key variable. Since 2000, many companies have made security a central element of their design and production processes for software. A strategy that takes advantage of the best procedures adopted by leading software manufacturers to make their products more secure has a better chance of succeeding than a strategy that attempts to determine security by looking at location.

**3. Avoid one-size-fits-all solutions.** The government already has processes for producing software with high assurance levels for very sensitive applications, such as command-and-control or intelligence. Cleared personnel working in secure facilities and following strict guidelines write this software. This provides software that is more trustworthy, but it is too expensive and too limiting to scale across government.

Building on existing efforts, an effective strategy will map software assurance levels and requirements to the sensitivity of the function and networks they support. Federal requirements could scale progressively from routine applications to the most sensitive, with requirements increasing to match sensitivity.

**4. Refocus and reform existing certification processes.** There are already several security certification processes for software products, such as the Common Criteria, but these processes do not ensure that certified software products are capable of resisting hostile attack. The United States can lead an effort that engage the industry to streamline these certification processes, reduce their cost, and buttress them with best practices and software assurance tools.

**5. Identify commercial-sector best practices and tools and expand their use**. Many companies already have extensive software assurance procedures as part of their production processes. The processes include a sequence of internal reviews for performance and security, testing, external testing and red-teaming, and the use of software review tools (some commercial, some proprietary and developed by the software company itself) to find vulnerabilities or errors. These practices offer the building blocks for an approach that is most likely to succeed in reducing the risk of distributed production. Extending these best practices would improve software assurance and security overall and reduce risk from hidden malicious code.

As part of this effort, the government could provide incentives and support for building better software assurance tools. As software programs continue to grow in size, investment in R&D for better tools will become more important for preliminary checks of the millions of lines of code found in many products.

**6. Create a governance structure (or structures) for assurance.** Companies may be taking extensive steps to improve software assurance, but if these steps are unknown or unmeasured, they cannot increase trust. Finding ways to overcome this is a crucial step for increasing trust in software products used for national security and critical infrastructure applications. It is essentially a governance problem. Traditional approaches to governance—command-and-control or regulations—do not work as well as they once did, or they may increase assurance at an unacceptable cost. An alternative solution is to create public-private partnerships to improve assurance. Whether this structure is formal or informal (and there are a number of existing groups that could be consolidated to serve this purpose), the objective would be to identify and share the best practices developed by software companies and shape requirements and procedures for better software assurance.

**7. Accelerate information assurance efforts.** Even if there were no foreign participation in IT production, networks would still be insecure. Networks involve thousands of different devices, some running older legacy code, others

running unpatched programs, and all facing the possibility that they are vulnerable because of a configuration error found in a separate network to which they connect but do not control. In this environment, knowing who has accessed information, and whether they have changed it, copied it, or transferred it offers a more efficient way to improve security. Greater attention to accountability and transparency in information use—monitoring and safeguarding data at rest—can help manage risk. Emerging technologies for information assurance, use control, and better authentication and authorization can counterbalance network and software vulnerabilities by allowing networks to control who can access information and what they can see and do with it.

**8. Promote leadership in IT innovation.** Globalization and distributed production are unavoidable, but the United States can take steps to keep itself at the forefront of technology. Technological innovation is good for the economy and for national security. Innovation makes life more difficult for opponents. All of an opponent's work to "rig" one technology is wasted if a new technology appears and supplants it. Innovation can improve assurance processes, tools, and overall network and information security. Measures that improve the climate for innovation in the United States (such as increased funding for IT-related R&D) also help build a skilled domestic workforce, so that the United States does not find itself relegated to low-end functions or working off some other nation's designs.

TechAmerica members have identified over a dozen various efforts across the Federal government that are purported to be addressing aspects of assuring the global supply chain. An unavoidable element of the technology that the Department acquires and deploys on a daily basis is that it is sourced from a global industry. While industry is willing to help develop the mechanisms to provide greater assurance in the supply chain, government must commit to sharing the risks and liabilities as part of that effort. Several of the government efforts seek to revise the acquisition process to place liability – even unlimited liability – on the vendors of hardware, software or services. Such a lopsided assignment of risk is unworkable and would only serve to cut the government off from the critical technologies it needs. Industry believes a more workable framework for sharing risk will include a demonstration of assurance in the products and services offered to the government, coupled with revised acquisition behavior on the part of government procurers.

TechAmerica is leading the industry response to the Federal Acquisition Council regarding their proposal on supply chain assurance offered as an Advanced Notice of Proposed Rulemaking on "Authentic IT". While the FAR Council has held public

hearings and sought out industry participation in formulating a solution to this problem, other efforts have not been so transparent. A recent effort by the National Institute of Standards and Technology, with participation from DoD and DHS, among other agencies involved a draft Special Publication was not vetted with industry until almost ready for publication.

Industry is very concerned that without oversight and coordination, government risks creating multiple, potentially conflicting requirements for the demonstration of assurance for hardware, software and services. These conflicts could unintentionally prevent companies from bringing their innovations to the public sector market, create significant barriers for small and mid-sized companies or drive other companies from the market because of an inability to accept the financial ramifications on their business model. The Subcommittee should seek to encourage the Administration to identify a single authority to consolidate and coordinate the various efforts addressing this issue.

Legal Challenges

There are a number of laws and regulations that prohibit or discourage information sharing and operational collaboration between industry and government that are in need of attention from Congress. Many of our policies and their statutory foundations were crafted before the Internet was invented and certainly before it became the ubiquitous resource it is today. Others are unintentionally restrictive because the drafters could not contemplate the technologies and capabilities that we now enjoy in the age of innovation.

The Subcommittee should consider a review of relevant portions of Title 10 for such antiquated authorities that inhibit the ability of the National Security community to protect our Nation's information systems, infrastructure and networks. Additionally, the Subcommittee should consider coordinating with other committees to address similar disconnects between the United States and our global partners. Such an undertaking would not be easy, but will be a necessary endeavor if we are to have success securing Cyber space for our Nation.

# Phillip J. Bond

## President, TechAmerica

Phillip J. Bond is the President of TechAmerica and holds responsibility over the Association's policy and communications. In 2008 as the President & Chief Executive Officer of the Information Technology Association of America (ITAA), a position he held since 2006, Bond partnered with Christopher W. Hansen -- then President & CEO of AeA -- to form TechAmerica. As President & CEO of ITAA, Bond helped to also drive the April 1, 2008 merger with the Government Electronics and Information Technology Association (GEIA).

Mr. Bond is also President of the World Information Technology and Services Alliance (WITSA), a network of industry associations representing 70 high-tech trade groups around the world. Bond is a highly accomplished executive in both government and industry. Prior to joining ITAA, he served as Senior Vice President of Government Relations for Monster Worldwide, the world's largest online career site, and General Manager of Monster Government Solutions.

From 2001 to 2005, Bond was Under Secretary of the U.S. Department of Commerce for Technology and, from 2002-2003, served concurrently as Chief of Staff to Commerce Secretary Donald Evans. In his dual role, Bond worked closely with Secretary Evens to increase market access for U.S. goods and services and further advance America's technological leadership at home and around the world. He oversaw the operations of the National Institute of Standards and Technology, the Office of Technology Policy, and the National Technical Information Service. He also worked to transform the Technology Administration into the pre-eminent portal between the federal government and the U.S. technology industry. During that time, Bond was recognized in Scientific American magazine in its list of the Top 50 Tech Leaders of 2003.

Bond joined the Administration from the private sector, where he served as Director of Federal Public Policy for the Hewlett-Packard Company, and previously as Senior Vice President for Government Affairs and Treasurer of the Information Technology Industry Council.

From 1993 to 1998, Bond served as Chief of Staff to Congresswoman Jennifer Dunn (R-WA). He was Principal Deputy Assistant Secretary of Defense for Legislative Affairs from 1992 to 1993. Earlier, Bond was Chief of Staff and Rules Committee Associate for Congressman Bob McEwen (R-OH) from 1990 to 1992. From 1987 to 1990, he served as Special Assistant to the Secretary of Defense for Legislative Affairs.

He is a graduate of Linfield College in Oregon. Bond and his wife, Diane, have two daughters and reside in Fairfax Station, Virginia.

**Statement**

**of**

**David Z. Bodenheimer, Esq.**

**Partner**
**Crowell & Moring LLP**
**Washington, DC**

**Before the**

**House Armed Services Committee's**
**Subcommittee on Terrorism,**
**Unconventional Threats and Capabilities**

**Concerning**

# Private Sector Perspectives on Department of Defense Information Technology and Cybersecurity Activities

**February 10, 2010**

**Introduction**

Ms. Chairwoman Sanchez and Members of the Committee. Thank you for holding these hearings today to seek Private Sector Perspectives on Department of Defense Information Technology and Cybersecurity Activities. The Department of Defense has long been on the leading edge in advancing technology, harnessing information, and developing acquisition policy. Never has there been a more critical time for the Department of Defense to demonstrate its leadership than now on cybersecurity. The stakes are simply too great to wait.

And industry must be an essential partner in hardening our defenses against cyber attack. As Director of National Intelligence Dennis Blair aptly stated in the 2010 Annual Threat Assessment, "acting independently, neither the US Government nor the private sector can fully control or protect the country's information infrastructure."[1] Quite bluntly, the Defense Department and industry will either succeed together – or fail separately.

For this vital partnership between the Defense Department and industry, what are the critical ingredients? Among other needs, the essentials include:

- Effective Information Sharing. To connect the dots effectively, cybersecurity information sharing must be a two-way street, with much broader industry participation and more carrots – and fewer sticks – for industry information sharing.

- Cyber Standards – Clear, Firm, and Consistent. The Defense Department should seize the opportunity to define clear, firm, and consistent cybersecurity standards that become the gold standard on which other agencies and industries can converge.

- Breakthrough Technologies. For effective cybersecurity that we can trust and afford, breakthrough technologies remain indispensable, requiring a combination of more R&D funding, public-private innovation rewards, and technology clearinghouses to bring the best and brightest to building our cyber defenses.

- Liability Limitations. Just as Congress fostered technology advances through the SAFETY Act's liability limitations for anti-terrorism technology, such protections should be shaped to encourage greater technology development and broader information sharing for the cybersecurity industry.

---

[1] Office of the Director of National Intelligence (ODNI), *Annual Threat Assessment of the US Intelligence Community for the House Permanent Select Committee on Intelligence*, p. 2 (Feb. 3, 2010) (http://www.dni.gov/testimonies/20100202_testimony.pdf).

I am David Bodenheimer, a partner in the law firm of Crowell & Moring LLP in Washington, DC where I lead the Homeland Security practice and specialize in government contracts. As part of this practice, I have advised clients, published articles, and lectured extensively on cybersecurity and government contract matters. In addition, I serve as Co Vice-Chair of the ABA Cybersecurity Committee and Co-Chair of the ABA Homeland Security Committee. Prior to entering private practice, I served six years (1982-88) as a civilian attorney for the Department of the Navy where I handled a broad spectrum of government contract matters in the field, at the Commands, and as Assistant to the General Counsel. However, I appear before your Committee today in my personal capacity and the views that I express are my own.

## I. Why We Must Act Now to Protect Our Information Assets

Simply waiting for the cyber apocalypse or digital Pearl Harbor is not an option. Virtual unanimity exists that we need to take action now – if not last year.

- Senators Rockefeller and Snowe. "We need to act now – the time to combat cyber terror was yesterday."[2]
- President Obama. "The status quo is no longer acceptable."[3]
- Industry. "Quite frankly, the bad guys are winning."[4]
- CSIS Cyber Report. "America's failure to protect cyberspace is one of the most urgent national security problems . . . ."[5]

No real dispute remains about the gravity of the threat or the urgency for taking action to guard our information assets. By any measure, the record of cyber attacks, security breaches, and compromised data is alarming. These threats strike at our national security, economic well-being, and personal privacy.

---

2 "Chairman Rockefeller and Senator Snowe's Statement on the Obama Administration's Cybersecurity Review," Senate Committee on Commerce, Science, and Transportation (May 29, 2009).

3 "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House Office of the Press Secretary (May 29, 2009).

4 *Agencies in Peril: Are We Doing Enough to Protect Federal IT and Secure Sensitive Information? Hearings Before Senate Subcomm. on Federal Financial Management, Government Information, Federal Services, and International Security of the Comm. on Homeland Security & Governmental Affairs*, 110th Cong., p. 28 (Mar. 12, 2008) (statement of Mr. Tim Bennett, Cyber Security Industry Alliance).

5 CSIS Commission on Cybersecurity, *Securing Cyberspace for the 44th Presidency*, p. 11 (Dec. 2008) (hereinafter CSIS Commission Report).

National Security Threats. As its "one central finding," the CSIS Commission on Cybersecurity warned that the "United States must treat cybersecurity as one of the most important national security challenges it faces."[6] In January 2009, former DNI Director Mike McConnell "equated 'cyber weapons' with weapons of mass destruction when he expressed concern about terrorists' use of technology to degrade the nation's infrastructure."[7] Recent history has already underscored the gravity and reach of this threat.

- 2007 Foreign Intrusions. "The damage from cyber attack is real. In 2007, the Departments of Defense, State, Homeland Security, and Commerce; NASA; and National Defense University all suffered major intrusions by unknown foreign entities."[8]

- 2008 Malware Attack. "In one of the most serious cyber incidents to date against our military networks, several thousand computers were infected last year by malicious software – malware."[9]

- Presidential Helicopter. "The U.S. Navy is investigating how an unauthorized user in Iran gained online access to blueprints and other information about a helicopter in President Obama's fleet."[10]

- 360 Million Attacks. "Last year the Pentagon reported more than 360 million attempts to break into its networks."[11]

- Russian Cyber Attacks. "And last year we had a glimpse of the future face of war. As Russian tanks rolled into Georgia, cyber attacks crippled Georgian government websites."[12]

---

6 CSIS Commission Report, p. 15 (Dec. 2008).

7 Congressional Research Service (CRS), "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations," CRS Report R40427, p. 3 (Mar. 10, 2009) (hereinafter CRS CNCI Report).

8 CSIS Commission on Report, p. 12 (Dec. 2008).

9 "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House Office of the Press Secretary (May 29, 2009).

10 "Source in Iran Sees Plans for President's Chopper," *USA Today* (Mar. 2, 2009).

11 "Subcommittee Chairman Lipinski's Floor Speech on H.R. 4061," House Subcomm. on Science and Technology (Feb. 3, 2010) (http://science.house.gov/press/PRArticle.aspx?NewsID=2736).

12 "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House Office of the Press Secretary (May 29, 2009).

Economic Damage. Cyber attacks also steal our critical technology and trade secrets, sapping the economic power that fuels our military might. As stated in the President's Cyberspace Policy Review, "[o]ur digital infrastructure has already suffered intrusions that have allowed criminals to steal hundreds of millions of dollars and nation-states and other entities to steal intellectual property and sensitive military information."[13] For such security breaches, the economic stakes are enormous:

> According to a 2009 report from McAfee, the 2008 overall losses from data theft and breaches from cybercrime may have cost businesses as much as $1 trillion globally in lost intellectual property and expenditures for repairing the damage last year. Respondents estimated that they lost data worth a total of $4.6 billion and spent about $600 million cleaning up after breaches.[14]

Even these losses pale in comparison to the catastrophic economic damage that could result from an attack on America's critical infrastructure, such as the power grid or financial system.[15]

Personal Impact. Security breaches also strike with the unpleasant personal force of a punch in the gut, violating privacy and stealing identities. Since 2005, the Privacy Rights Clearinghouse has reported 345,124,400 records with sensitive personal information being compromised in security breaches – with over 80 million records compromised within the last 6 months.[16] Service men and women, veterans, and their families have been hit particularly hard.

- 26 Million Veterans. "In May 2006, the Department of Veterans Affairs lost an unsecured laptop computer hard drive containing the health records and other sensitive personal information of approximately 26.5 million veterans and their spouses."[17]

---

[13] President's Report, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, p. i (May 2009).

[14] *Do the Payment Card Industry Data Standards Reduce Cybercrime? Hearings Before the House Subcomm. on Emerging Threats, Cybersecurity, and Science and Technology of Comm. on Homeland Security,* 111th Cong. (Mar. 31, 2009) (statement of Chairman Thompson) (http://homeland.house.gov/SiteDocuments/20090331141926-86082.pdf).

[15] CRS CNCI Report, p. 3 (potential for "strategic damage to the United States"); Wright, "The Spymaster: Can Mike McConnell fix America's Intelligence Community," *The New Yorker,* p. 51 (Jan. 21, 2008) (". . . McConnell then said, 'If the 9/11 perpetrators had focused on a single U.S. bank through cyber-attack and it had been successful, it would have an order-of-magnitude greater impact on the U.S. economy'").

[16] Privacy Rights Clearinghouse, "Chronology of Data Breaches" (Feb. 4, 2010) compared with 262,442,156 records compromised through June 11, 2009 (http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP).

[17] S. REP No. 111-110, p. 3 (Dec. 17, 2009).

- 2008 Walter Reed Breach. "In June 2008, the Walter Reed Army Medical Center reported that officials were investigating the possible disclosure of personally identifiable information through unauthorized sharing of a data file containing the names of approximately 1,000 Military Health System beneficiaries."[18]

- Navy CIO Victimized. "The personal identifiable information of the Navy chief information officer has been compromised, again. And, it isn't just the second or third or fourth or even fifth time Robert Carey's PII has been exposed, but the sixth instance."[19]

- Defense Secretary Hacked. "The Secretary of Defense's unclassified e-mail was hacked."[20]

In summary, cyber assaults threaten our military might, economic power, and personal well-being. And it will get much worse – perhaps cataclysmically so – if treated as a middle-of-the-inbox inconvenience rather than as the clear and present danger now hanging over our collective heads.

## II. Why Public-Private Partnerships Are Critical to Cyber Defense

Hardly anyone disputes the paramount importance of public-private partnerships, particularly given that the bulk of our critical information assets reside in the hands of the private sector. More than many agencies, the Defense Department has made great strides in recognizing the need for private-sector involvement though the use of bilateral understandings struck with some military contractors. The time is ripe for the Defense Department to expand these private-sector relationships into a full public-private partnership.

### A. The Need for Full Public-Private Partnerships

For at least three reasons, the Defense Department and its contractors must band together to succeed in defending our cyber assets and security: (1) nearly everyone agrees that public-private partnerships are essential to effective cyber defense; (2) the private sector holds the

---

[18] Government Accountability Office (GAO), "Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses," p. 9 (GAO-09-546) (July 2009).

[19] Chabrow, "Navy CIO's PII Exposed for Sixth Time," *Government Information Security News* (Jan. 4, 2010) (http://blogs.govinfosecurity.com/posts.php?postID=404&rf=010510eg).

[20] *Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Response: Hearings Before Senate Comm. on Commerce, Science, and Transportation,* 111th Cong., p. 8 (Mar. 19, 2009) (statement of Dr. James Lewis).

overwhelming majority of critical information infrastructure; and (3) public-private partnerships have been the model for success during past national crises.

### 1. The Consensus on the Need for Public-Private Partnership

Virtually every top official, cybersecurity expert, and major review has reached the same conclusion – public-private partnerships are vital to any successful cybersecurity strategy. Even a short sample reflects this consensus.

- President Obama. "Third, we will strengthen the public/private partnerships that are critical to this [cybersecurity] endeavor."[21]
- Senator Rockefeller. "We need a coordinated public-private response. Currently, this does not exist."[22]
- Representative Lipinski. "Improving the security of cyberspace is of the utmost importance and it will take the collective effort of the Federal government, private sector, our scientists and engineers, and every American to succeed."[23]
- DNI Director Blair. "Acting independently, neither the U.S. government nor the private sector can fully control or protect the country's information infrastructure."[24]
- CSIS Report. "The U.S. government should rebuild the public-private partnership on cybersecurity to focus on key infrastructures and coordinated preventive and responsive activities."[25]

---

[21] "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House Office of the Press Secretary (May 29, 2009).

[22] *Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Response: Hearings Before Senate Comm. on Commerce, Science, and Transportation,* 111th Cong., p. 2 (Mar. 19, 2009) (statement of Sen. Rockefeller).

[23] "Subcommittee Chairman Lipinski's Floor Speech on H.R. 4061," House Subcomm. on Science and Technology (Feb. 3, 2010) (http://science.house.gov/press/PRArticle.aspx?NewsID=2736).

[24] Blair, "Director of National Intelligence's Annual Threat Assessment," *Government Info Security* (Feb. 2, 2010) (http://www.govinfosecurity.com/articles.php?art_id=2154&rf=011610eg).

[25] CSIS Commission Report, p. 6 (Dec. 2008).

- Industry. "[G]overnment and industry must develop a much more thoughtful, fundamental and contemporary relationship to address their mutual (not just government's) cyber security needs."[26]

- Experts Generally. "The key strategy improvements identified by cybersecurity experts [include]: . . . Bolster public-private partnerships through an improved value proposition and use of incentives."[27]

While this list could be much longer, the conclusion would remain the same – the public and private sectors must be partners in the quest for an effective and affordable cybersecurity strategy. Without a partnership, even the most elegant solution will fall short, leaving both the public and private sector exposed to ever more devastating cyber attacks.

### 2. The Private Sector's Information Infrastructure

Even without such a consensus, the need for public-private partnership would still be inevitable. Neither the public nor private sector control the entire information infrastructure, yet the public and private networks are both intertwined and interdependent. In its report, the CSIS Commission summed up the rationale for why the public and private sectors must be partners in securing cyberspace:

> Securing cyberspace requires government and the private sector to work together. The private sector designs, deploys, and maintains much of the nation's critical infrastructure. This is important because unlike certain other elements of national security, cyberspace cannot be secured by the government alone. There is a bifurcation of responsibility (the government must protect national security) and control (it does not manage the asset or provide the function that must be protected).[28]

### 3. The Historical Success of Public-Private Partnerships

During the bleakest of times, the United States military and its contractors have teamed up to defeat foes that literally threatened the survival of the free world. In 1946, Army Chief of Staff Eisenhower described the effectiveness of this partnership during World War II:

---

[26] Internet Security Alliance, "The Cyber Security Social Contract Policy Recommendations for the Obama Administration and 111th Congress," p. 3 (2008).

[27] GAO, "Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats," p. 15 (GAO-10-230T) (Nov. 17, 2009).

[28] CSIS Commission Report, p. 43 (Dec. 2008).

> The armed forces could not have won the war alone. Scientists and business men contributed techniques and weapons which enabled us to outwit and overwhelm the enemy. Their understanding of the Army's needs made possible the highest degree of cooperation. This pattern of integration must be translated into a peacetime counterpart which will not merely familiarize the Army with the progress made in science and industry, but draw into our planning for national security all the civilian resources which can contribute to the defense of the country.[29]

Some may say that the threat is not the same as during World War II. In some ways, today's threat is even greater because the cyber barbarians can now strike at the heart of America in ways that the Nazis and Japanese could not in the 1940s.

> [Cybersecurity is] about protecting our Nation's critical infrastructure from cyberattacks that could severely impact commerce and the economy in absolutely devastating ways.
>
> * * *
>
> For example, private-sector IT systems control virtually all of this critical infrastructure; traffic lights, rail networks. It would be very easy to make train switches so that two trains collide, affect or disrupt water and electricity, or release water from dams, where the computers are involved. How our money moves, they could stop that. Any part of the country, all of the country is vulnerable.[30]

The magnitude of this cyber threat explains why two Directors of National Intelligence "Mike McConnell, under President Bush, and Admiral Blair, under President Obama, both said that the number-one security threat to the United States of America was cybersecurity, or cyberterror . . . ."[31] In short, just as the public-private partnership worked during World War II, the time is right to do so again to forestall a digital Pearl Harbor.

### B. The Need for Expanding Defense Partnerships

Through its Defense Industrial Base (DIB) initiative, the Defense Department has established a pilot program for partnering with a portion of the defense industry. In testimony before this Subcommittee last year, Deputy Assistant Secretary Robert Lentz summarized the Defense Department's DIB program:

---

29 Nagle, *A History of Government Contracting*, p. 464 (1992).

30 *Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Response: Hearings Before Senate Comm. on Commerce, Science, and Transportation*, 111th Cong., p. 2 (Mar. 19, 2009) (statement of Sen. Rockefeller).

31 *Id.*, p. 1.

> In early 2008, the Department initiated a DIB Cyber Security and Information Assurance (CS/IA) pilot program to address cybersecurity risks to DIB unclassified networks that support DoD programs. The DIB CS/IA pilot has five major components: a binding bilateral DoD-DIB company framework agreement to facilitate CS/IA cooperation; threat and vulnerability information sharing; DIB network incident reporting; damage assessments; and DoD acquisition and contracting changes, including proposed changes to Defense Federal Acquisition Regulation Supplement (DFARS). The DoD-DIB legal framework provides the mechanism to exchange relevant threat information in a timely manner, provides intelligence and digital forensic analysis on threats, and expands Government to Industry cooperation while ensuring that industry equities and privacy are protected.[32]

While this pilot program represents a valuable start, the Defense Department now needs to move forward with a full public-private partnership. Key characteristics of this full partnership include the following:

- Broad Industry Partnership. Rather than the current bilateral model involving only a few companies, a full partnership requires broad industry participation for greater transparency and robust sharing of options, ideas, and strategy.[33]

- Timely, Two-Way Partnership. Full partnership should involve two-way exchanges before decisions have been made and strategy has already been set.[34]

---

[32] *Cyberspace as a Warfighting Domain: Policy, Management and Technical Challenges to Mission Assurance: Hearings Before House Subcomm. on Terrorism, Unconventional Threats and Capabilities of Comm. on Armed Services,* 111th Cong. (May 5, 2009) (statement of Robert Lentz).

[33] Business Software Alliance, "National Security & Homeland Security Councils Review of National Cyber Security Policy," p. 1 (Mar. 19, 2009) ("Government engagement with industry has also often been selective, rather than open and transparent. . . . 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").

[34] *Id.*, p. 2 (sharing "has largely been one-way"); *see also* Intelligence and National Security Alliance (INSA), "Critical Issues for Cyber Assurance Policy Reform: An Industry Assessment," p. 2 ("Create an effective public/private partnership [that will] insure that industries receive timely information that will enable them to react to attacks").

- Multi-Sector Partnership. By partnering with other sectors, DoD could leverage expertise across industries and agencies, reduce duplication caused by bilateral agreements, and benefit from existing partnerships.[35]

## III. What the Private Sector Needs for Enhancing Cybersecurity Efforts

Given the escalating pace and magnitude of cyber attacks, both the public and private sectors need a new paradigm to build better cyber defenses more rapidly and cost-effectively. For this effort, five factors are key to elevating and maintaining these cyber defenses:

- Improve information sharing;
- Establish clear, firm, and consistent cybersecurity standards;
- Accelerate breakthrough cyber technologies;
- Limit liability to encourage more information sharing and technology innovation; and
- Develop mechanisms to resolve disputes fairly and quickly.

### A. Effective Information Sharing

Just as the homeland security mission hinges upon information sharing ("connecting the dots"), effective cybersecurity requires real-time, two-way information sharing between the public and private sector. However, current information-sharing arrangements have consistently fallen short of what the private sector needs to fight back against cyber attacks.

- Insufficient Data. "When provided to DIB members, US Government indications and warning (I&W) intelligence frequently lacks context, is too heavily focused on domain and IP blacklisting, provides little or no finished analysis and is generally too old to constitute actionable information."[36]
- One-Way "Sharing". "To date, sharing of information about threats, vulnerabilities and attacks between industry and

---

[35] Business Software Alliance, "National Security & Homeland Security Councils Review of National Cyber Security Policy," p. 4, Question # 3 (Mar. 19, 2009) (Government engagement is "often based on bilateral relationships between specific agencies and specific companies or sets of companies" and "they are often redundant").

[36] Internet Security Alliance, "The Cyber Security Social Contract Policy Recommendations for the Obama Administration and 111th Congress," p. 19 (2008).

government has largely been one-way, with industry sharing information with the government."[37]

- Untimely Sharing. "Speed and timeliness of information sharing needs significant improvement for the achievement of a successful desired degree of protection and attribution."[38]

- Over-Classification. "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."[39]

To maximize the effectiveness of information sharing with the private sector, the following three steps should be taken.

1. Engage in two-way information sharing by providing timely, actionable information, while minimizing the amount and level of classification.

2. Expand information sharing to include the broader defense industry base, rather than limiting such sharing to selected contractors with bilateral agreements.

3. Employ a carrot rather than stick approach, encouraging information sharing through incentives, rather than penalizing those who share bad news of breaches or threats.

### B. Clear and Consistent Cybersecurity Standards

As a nearly universal concern, the lack of clear, firm, and consistent standards for cybersecurity has troubled the private sector. As one expert put it, "we have not brought the full power of the Federal Government to bear on the problem, and what power we did bring was applied in a fragmented and incoherent manner."[40] In another instance, the guidance has been described as "ad hoc," "redundant," and sometimes "conflicting":

---

[37] Business Software Alliance, "National Security & Homeland Security Councils Review of National Cyber Security Policy," p. 2, Question # 1 (Mar. 19, 2009).

[38] INSA, "Critical Issues for Cyber Assurance Policy Reform: An Industry Assessment," p. 3.

[39] Business Software Alliance, "National Security & Homeland Security Councils Review of National Cyber Security Policy," pp. 1-2, Question # 1 (Mar. 19, 2009).

[40] *Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Response: Hearings Before Senate Comm. on Commerce, Science, and Transportation,* 111th Cong., p. 7 (Mar. 19, 2009) (statement of Dr. James Lewis).

> 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 [Critical Infrastructure Partnership Advisory Council] framework.[41]

A number of examples illustrate how the public and private sector can collaborate successfully to develop workable, effective standards.[42] To assure that the private sector's investment in cybersecurity compliance is directed towards cost-effective solutions, a clear, consistent, and firm set of standards is critical.

### C. Breakthrough Cybersecurity Technologies

While technology is not the sole answer for achieving real cybersecurity, major advances in such technology will be critical not only for countering the ever-more sophisticated cyber threats, but also for achieving such success at a cost that the public and private sectors can bear over the long haul. To this end, President Obama stated that "we will continue to invest in cutting-edge research and development necessary for the innovation and discovery we need to meet the digital challenges of our time."[43]

For such breakthrough technologies, the investment in innovation needs to be focused in areas where market forces are less likely to drive the private sector to produce the needed technologies. Research targets include the following:

- Long-Term Research. "We need to apply more funding and support to research. And the research can't be near-term, let's-come-up-with-a-patch-for-the-latest-botnet-or-the-latest-firewall-problem, but long-term research as to how to fundamentally redesign some of the systems we're using and the security involved."[44]

---

41 Business Software Alliance, "National Security & Homeland Security Councils Review of National Cyber Security Policy," p. 5, Question # 3 (Mar. 19, 2009).

42 INSA, "Critical Issues for Cyber Assurance Policy Reform: An Industry Assessment," p. 3 (citing the Capability Maturity Model Integration (CMMI)).

43 "Remarks by the President on Securing Our Nation's Cyber Infrastructure," The White House Office of the Press Secretary (May 29, 2009).

44 *Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Response: Hearings Before Senate Comm. on Commerce, Science, and Transportation,* 111th Cong., p. 29 (Mar. 19, 2009) (statement of Dr. Eugene Spafford).

- Basic Internet Protocols. "There needs to be Research and Development; especially in areas such as the development and implementation of new secure basic protocols for the Internet, which will not be undertaken in the private sector due to the lack of a viable business plan for implementing them profitably."[45]

- Research Coordination. "Cyber security research and development efforts in the US must be better coordinated; only through information sharing and collaboration can effective solutions emerge."[46]

- Over-Classification. "Over-classification hurts many efforts in research and public awareness."[47]

In addition to a greater focus upon cybersecurity research, other options for stimulating technology innovations include techniques embodied in the Homeland Security Act, such as agency requests for, and reviews of, "unique and innovative technologies" and the establishment of a technology "clearinghouse" for collecting and disseminating information to other agencies, as well as the private sector. *See* Pub. L. No. 107-296, § 313(b).

### D. Liability Limitations and Other Incentives

The risk of lawsuits inevitably influences corporate decision-making. For cybersecurity, potential legal liability may discourage information sharing and technology development. Given the importance of both activities to the successful hardening of cyber defenses, legal safe harbors need to be considered in order to encourage greater information sharing and cyber innovation.

#### 1. Enhancing Information Sharing

For information sharing, two factors create disincentives for making disclosures to the Government and sharing critical data with other industry partners. First, the Defense Department should explore incentives to encourage the private sector to identify security problems promptly and cooperate fully with the Defense Department to resolve such problems. In the past, some defense contractors have felt that the Defense Department's response to bad news has tended too

---

45 Internet Security Alliance, "The Cyber Security Social Contract Policy Recommendations for the Obama Administration and 111th Congress," p. 16 (2008).

46 Institute for Information Infrastructure Protection, "National Cyber Security Research and Development Challenges," p. 5 (2009); *see also* CSIS Commission Report, p. 9 (recommending "overall coordination of cybersecurity research and development").

47 *Cybersecurity: Assessing Our Vulnerabilities and Developing an Effective Response: Hearings Before Senate Comm. on Commerce, Science, and Transportation,* 111th Cong., p. 32 (Mar. 19, 2009) (statement of Dr. Eugene Spafford).

much towards the stick rather than the carrot, thus discouraging prompt disclosures in the future. To encourage disclosure, the Defense Department should consider a combination of incentives, safe harbors, and liability limitations as mechanisms to encourage – rather than discourage – disclosing problems, sharing information, and serving as real partners to defend our information assets.

Second, the effectiveness of information sharing would be multiplied exponentially if the private sector could share not only with the Defense Department, but also with other industry partners. However, the specter of antitrust investigations and lawsuits hangs over such intra-industry cooperation. To encourage information sharing within industry, the Defense Department should consider working with industry and other agencies to define standards and safe harbors that would encourage industry cooperation leading to innovative ideas and technologies to enhance cybersecurity.

#### 2. Fostering Technology Innovation

For homeland security, Congress recognized that protections against liability lawsuits could spur the development of anti-terrorism technologies:

> The Select Committee [on Homeland Security] believes that technological innovation is the Nation's front-line defense against the terrorist threat. Unfortunately, the Nation's products liability system threatens to keep important new technologies from the market where they could protect our citizens. In order to ensure that these important technologies are available, the Select Committee believes that it is important to adopt a narrow set of liability protections for manufacturers of these important technologies.[48]

Consistent with this legislative purpose, Congress enacted the SAFETY Act to spur the development of anti-terrorism technologies. *See* 6 U.S.C. §§ 441-44. However, this Act only covers acts of terrorism, leaving questions about its protection for other cyber attacks, such as those sponsored by nation-states and organized crime. To accelerate the fielding of new cyber technology, Congress should consider extending liability protections to the private sector producing such innovations necessary to defend against increasingly dangerous and sophisticated cyber attacks.

### E. Dispute Resolution

As information systems become ever more interconnected, the Defense Department will inevitably find the need to cut off a contractor's access to the DoD network due to security breaches or inadequate security safeguards. Such actions are entirely consistent with the overall objective of protecting the security of military information assets.

---

[48] H.R. REP. NO. 107-609, Pt. 1, p. 118 (July 24, 2002).

At the same time, a contractor should not be disconnected from the DoD network if the fault lies elsewhere. In today's interconnected information world, pulling the plug on a defense network connection may effectively put a contractor out of business – *i.e.*, an information death sentence equivalent to default termination or blacklisting. Due to the serious nature of such actions, the courts and administrative forums have traditionally treated them as forfeitures that have been consistently disfavored in the law. *See, e.g., Bell Helicopter Textron,* ASBCA No. 21192, 85-3 BCA ¶ 18,415 at 92,429 ("Every reasonable presumption is against a forfeiture"); *Bozied v. Brookings,* 638 N.W. 2d 264 (S.D. Sup. Ct. 2001) ("Forfeitures are considered odious in the law"); *McQueen v. Brown,* 775 A.2d 748 (N.J. Super. Ct. 2001) ("equity abhors a forfeiture").

One remedy would be to establish an administrative board with deep expertise in information security matters that could provide a prompt hearing and resolution for contractors severed from the government network. Long ago, the Defense Department opened such a forum for defense contract disputes that contractors could bring before the Armed Services Board of Contract Appeals (ASBCA). Such due process would be equally appropriate to protect contractors in the event of an unfair or improper termination from the military information network.

**Conclusion**

Thank you for your leadership on the Defense Department's information technology and cybersecurity initiatives that directly affect one of the most visible and vital components of America's critical infrastructure.

This concludes my statement and I would be happy to answer any questions you might have.

DC1WDMS: 10361727_1

crowell moring

# biography | David Bodenheimer

**David Z. Bodenheimer**
Partner
dbodenheimer@crowell.com

**Washington**
1001 Pennsylvania Avenue, N.W.
Washington, DC 20004-2595
Phone: 202.624.2713
Fax: 202.628.5116

**Practice Areas**
- Government Contracts
- False Claims/Qui Tam
- Homeland Security
- Privacy & Data Protection

**David Z. Bodenheimer** is a partner in the law firm of Crowell & Moring LLP in the DC office where he heads the Homeland Security Practice and specializes in Government Contracts, False Claims Act, Privacy, and Cybersecurity. For more than 25 years, he has found solutions for clients whenever and wherever problems arise in doing business with the Government.

**Government Contracts.** Mr. Bodenheimer represents all sizes of technology clients (computer hardware and software, major weapon systems, biodefense, satellite and space services, and military avionics and equipment). He litigates, counsels and resolves the full range of issues that clients confront in selling to the Government. Highlights include the following:

- **Defective Pricing.** Counseling on TINA cost and pricing matters, teaching the Defective Pricing course, and litigating major cases define the core of his defective pricing practice. *See, e.g., Wynne v. United Technologies Corp.*, 463 F.3d 1261 (Fed. Cir. 2006), *affirming* 05-1 BCA ¶ 32,860 and 04-1 BCA ¶ 32,556 (defeated $299 million defective pricing claim after 33-day trial and Federal Circuit appeal).

- **Protests.** His 25-year protest experience spans all forums (court, GAO, and agency), with the best ones being successfully resolved through agency corrective action without a decision, while others have established precedents in key areas. *See, e.g., Health Net Federal Services, LLC*, Nov. 4, 2009, 2009 CPD ¶ 220 (winning protest against $16 billion award after 5-day hearing, establishing key precedents on unfair competitive advantage, price realism, past

performance, and staffing); *AT&T Government Solutions, Inc.*, Aug. 28, 2008, 2008 CPD ¶ 170 (establishing contractor's due process rights of notice, opportunity to respond, and right to mitigate organizational conflicts of interest (OCIs)); *DRS C3 Systems, LLC*, Feb. 26, 2008, 2008 CPD ¶ 103 (winning protest on past performance evaluation of $65 million shipboard display award); *IBM Corp.*, June 4, 2007, 2008 CPD ¶ 64 (prevailing on protest against cost and price evaluation of $125 million financial management system); *Gentex Corp. v. United States*, 58 Fed. Cl. 634 (2003) (sustaining protest against misleading and unequal discussions on $400 million award for aircrew helmets for nuclear, biological, and chemical protection).

- **False Claims Act (FCA) & Investigations.** He defends fraud investigations and subpoenas (DCIS, AFOSI, Army CID, DOD IG, NSF IG, and Postal IG) relating to battlefield contracting, ethics rules, defective pricing, labor charging, progress payments, cost claims, government property, and postal equipment. His FCA litigation includes a pending decision on a $600 million FCA claim after a 2-month trial, as well as public decisions. *See, e.g., United States ex rel. Ackley v. International Business Machines,* 76 F. Supp. 2d 654 (D. Md. 1999) (briefed and argued jurisdictional dismissal of *qui tam* relator's fraud claims); *Peoples v. Eagle-Picher Indus., Inc.*, No. 96-5009-CV-SW-GAF (W.D. Mo., Jan. 31, 2003) (briefed and obtained disqualification of *qui tam* relator's counsel, ultimately leading to dismissal of FCA case).

- **Prime/Sub Disputes and Issues.** He advises both prime and subcontractors on software and data rights, trade secret and procurement integrity breaches, teaming agreements, specialty metals requirements, and flowdown terms. He litigates prime/sub disputes in both federal court and international arbitrations. *See, e.g., O'Gara Satellite Systems, Inc., vs. Telenor Satellite Services, Inc.*, No. AW 04 CV 3841 (S.D. Md. 2005) (achieved no-cost resolution of lost-profits claim for satellite services after judicial mediation); *McDonnell Douglas Corp. vs. SCI Corp.*, No. 91CV2077 (E.D. Mo. 1996-97) (conducted 2 weeks of courtroom cross-examination relating to A-12 prime/sub contract, leading to successful resolution and withdrawal of default termination).

- **Counseling & Compliance.** Mr. Bodenheimer supports clients in a broad spectrum of areas, developing strategies for resolving organizational conflicts of interests (from protests to mitigation plans), conducting compliance reviews (defense, healthcare, and

postal industries), defending against default terminations and cure notices, supporting convenience termination settlements, protecting software and technical data rights, preparing claims and requests for equitable adjustment (REAs), and addressing a host of cost, pricing, and profit issues.

**Homeland Security.** Mr. Bodenheimer serves as the head of the firm's Homeland Security practice, where he focuses upon the intersection of this practice with other Crowell & Moring groups such as Government Contracts, Transportation, Privacy, and International.

- **SAFETY Act.** He has developed SAFETY Act due diligence procedures, untangled complex insurance issues, advised on applications, prepared regulatory comments, testified before Congress, and supported legislative and regulatory enhancements to the SAFETY Act.
- **International Sales.** When contractors seek to sell anti-terrorism technology abroad, he has developed strategies for limiting liability exposure, advised on privacy and security implications, and analyzed other international risks.
- **Acquisition Challenges.** For the unique challenges of Department of Homeland Security (DHS) contracting, he has addressed issues relating to inverted corporations and organizational conflicts of interest, commented on special acquisition risks relating to requirements definition, and testified before Congress on TSA regulatory exemptions that have since been legislatively revoked.
- **Homeland Security Privacy.** For privacy issues arising out of Homeland Security technology (including passenger screening, identity authentication, and data mining), Mr. Bodenheimer has prepared extensive analyses of privacy requirements, advised on risk mitigation strategies, and assisted with preparation of policies, procedures, and Privacy Impact Assessments (PIA).
- **ABA Committee.** As Co-Chair of the ABA Science and Technology Section's Homeland Security Committee, he supports ABA activities, publications, and panels on the latest developments, risks, and opportunities in the homeland security arena.

**Privacy & Information Security.** In the privacy and information security arena, Mr. Bodenheimer handles emerging dilemmas arising out of data sharing, information technology (IT) interoperability, cybersecurity, and privacy concerns in the homeland security, postal service, and healthcare industries. His privacy and cybersecurity counseling spans the Privacy Act, Federal Information Security Management Act (FISMA), DIACAP, NIST, USA PATRIOT Act, electronic workplace monitoring, state security

biography

## David Bodenheimer

breach notification laws, HSPD authentication and biometrics, and federal electronic surveillance. He currently serves as a Vice Chair of the ABA Public Contract Law Section's Cybersecurity Committee.

Prior to joining Crowell & Moring LLP, Mr. Bodenheimer worked for the Department of the Navy from 1982 to 1988 in various positions, including Assistant to the General Counsel, where he handled default termination litigation, suspension and debarment, foreign military sales, major claims and disputes, NATO negotiations, and bid protests (GAO, agency, and district court actions).

**Education**
University of North Carolina, B.A., 1978
University of North Carolina, M.B.A., 1982
University of North Carolina Law School, J.D., 1982

**Affiliations**

- **Admissions to practice.** Bars of District of Columbia and North Carolina; United States Court of Appeals for Federal Circuit; United States Court of Federal Claims; United States District Courts (DC and MD).
- **American Bar Association (ABA).** Co-Chair, Committee on Homeland Security, Science and Technology Section; Member, Public Contracts Law Section.
- **International Association of Privacy Professionals (IAPP).** Member and Certified Information Privacy Professional.
- **Intelligence & National Security Alliance (INSA).** Member.

**Publications**
"SAFETY Act Liability Protection for Service Contractors in the Homeland Security Business: Why It's Important and How to Get It," *CSA Service Contractor*, p.14 (Winter 2007). Co-Authors: Linda S. Bruggeman and David Z. Bodenheimer.

"Government's Defective Pricing Claim in the Great Engine War Flames Out at the Federal Circuit," *The Government Contractor*, Vol. 48, No. 36 (October 4, 2006). Author: David Z. Bodenheimer.

"When Cyber Barbarians Storm the Security Walls: The Mounting Risks of Security Breaches to Federal Agencies & Contractors," *BNA Federal Contracts Report*, Vol. 86, No. 12 (October 3, 2006). Author: David Z. Bodenheimer.

biography | David Bodenheimer

"Pulling the Plug on the Nation's Power Grid: Cyberthreats and Homeland Security Challenges," *The SciTech Lawyer*, Vol. 2, No. 4 (Spring 2006). Author: David Z. Bodenheimer.

"When Homeland Security Goes Abroad: The Global Collision of Privacy & Anti-Terrorism Laws," *BNA's Federal Contracts Report*, Vol. 85, No. 16 (April 25, 2006). Co-Authors: David Z. Bodenheimer and Kris D. Meade.

"Country Q&A: United States Data Protection," *Practical Law Company, Vol. 2: Data Protection* (2006-07). Co-Authors: Gaela Bailey, David Z. Bodenheimer, Benjamin T. Butler, Christopher Calsyn, Robin B. Campbell, Charles C. Hwang, Kris D. Meade, Jeremy Rhyne and John Stewart.

"'False' or 'Inaccurate' Estimates," *Briefing Papers*, No. 5-13 (December 2005). Author: David Z. Bodenheimer.

"The Strange Notion of Estimates as Fraud: Will Weather Predictions Be Next Under the False Claims Act?," *The Procurement Lawyer*, Vol. 4, No. 40 (Summer 2005). Author: David Z. Bodenheimer.

"Privacy vs. Information Sharing: The Gathering Storm Over Homeland Security and How Contractors Can Reduce Their Risks," *Federal Contracts Report*, Vol. 83, No. 21 (May 25, 2005). Author: David Z. Bodenheimer.

"Competition Trumps Defective Pricing Claim in the Great Engine War," *The Government Contractor*, Vol. 47, No. 8, pp47-48 (February 23, 2005). Author: David Z. Bodenheimer.

"Homeland Security Now and Later: Emerging Issues and New Perils in Contracting," *The Clause*, Vol. XIV, Issue 4 (November/December 2003). Author: David Z. Bodenheimer.

"The SAFETY Act Interim Regulations: Will They Fulfill the Homeland Security Mission By Stimulating Innovations in Antiterrorism Technology?," *Federal Contracts Report*, Vol. 80, No. 16 (November 4, 2003). Author: David Z. Bodenheimer.

"Technology for Border Protection: Homeland Security Funding and Priorities," *Journal of Homeland Security* (August 2003). Author: David Z. Bodenheimer.

"Finding Dollars for Biodefense: Opportunities and Challenges for Biotech Firms," *Genetic Engineering News*, Vol. 23, No. 10 (May 15, 2003).

biography

## David Bodenheimer

Author: David Z. Bodenheimer.

"Is the SAFETY Act Safe? Homeland Security and the Politics of Tort Liability," 45-17 *The Government Contractor* 181 (April 30, 2003). Author: David Z. Bodenheimer.

"Biotechnology Sellers Beware: The Risks and Opportunities of Doing Business with the Government," 22 *Biotechnology Law Report* 88 (April 2003). Author: David Z. Bodenheimer.

"Economic Price Adjustment Clauses: Pricing Pretzels and Pitfalls," *Gov't Cont. Audit Rep.* 16-20 (Fall 2002). Co-Authors: David Z. Bodenheimer and J. Chris Haile.

"The A-76 Commerical Activities Panel Report: Irreconcilable Differences Meet Mission Impossible," 78 *Fed. Cont. Rep.* (BNS) 187 (August 6, 2002). Author: David Z. Bodenheimer.

"Putting Teeth into the False Claims Act's Pre-Complaint Disclosure Requirements for Relators," *The Procurement Lawyer*, Vol. 4, No. 37 (Summer 2002). Author: David Z. Bodenheimer.

"Profits in Government Contracting: The Continuing Tug of War," *Gov't Cont. Audit Rep.* 12-16 (November 2001). Author: David Z. Bodenheimer.

"Damages Under the False Claims Act: Is the Sky the Limit?," *Gov't Cont. Audit Rep.* 16-20 (September 2000). Author: David Z. Bodenheimer.

"The New Battleground: Defective Pricing Invades Competitive Procurements," *Gov't Cont. Audit Rep.* 16-20 (December 1999/January 2000). Author: David Z. Bodenheimer.

"Past Performance: The Sequel," 8-3 Topical Issues in Procurement Series, 37 *Cont. Mgmt.* (September 1997). Author: David Z. Bodenheimer.

"Responsibility of Prospective Contractors," *Briefing Papers* 97-9 (August 1997). Author: David Z. Bodenheimer.

"Contractors Caught in the Cross Fire of Appropriations Law," 2-5 *Government Contract Audit Report* 14-16 (June 1997). Author: David Z. Bodenheimer

"Cost Realism Analysis: The Myth of Unfettered Agency Discretion," 58

*BNA Federal Contracts Report* 24 (July 13, 1992). Author: David Z. Bodenheimer.

**Speeches & Presentations**

"Cybersecurity: Escalating Threats, Morphing Duties & Intensifying Oversight," ABA Cybersecurity Committee, Washington, DC (Jan. 11, 2010). Speaker: David Z. Bodenheimer.

"Cybersecurity: Titanic Threats and Escalating Duties for Agencies and Contractors," ABA Annual Conference, Chicago, IL (Aug. 2, 2009). Moderator & Speaker: David Z. Bodenheimer.

"Cybersecurity: Opportunities & Pitfalls for Selling in the US Marketplace," Enterprise Ireland Forum, Washington, DC (June 16, 2009). Presenter: David Bodenheimer

"U.S. Technology Marketplace: Opportunities & Pitfalls for Selling to the U.S. Government," Canadian Technology Forum, Washington, DC (June 10, 2009). Speaker: David Z. Bodenheimer.

"Bid Protests and Competition 25 Years After CICA," Crowell & Moring Ounce of Prevention Seminar (OOPS) (May 2009). Co-Speakers: Thomas P. Humphrey, David Z. Bodenheimer, John E. McCarthy Jr. and Puja Satiani.

"Securing our Critical Infrastructure: Money, Technology, and Homeland Security Opportunities," Crowell & Moring Security Roundtable (October 2, 2008). Speaker & Moderator: David Z. Bodenheimer.

"Cyber on the Hill: Congressional Initiatives and Oversight for Emerging Cybersecurity Issues," Crowell & Moring Security Roundtable (August 5, 2008). Speaker & Moderator: David Z. Bodenheimer.

"Investing in Intelligence: Cutting-Edge Solutions for the National Security Mission," C&M Security Breakfast Series (May 13, 2008). Speaker & Moderator: David Z. Bodenheimer.

"Cyberspace and Homeland Security: Vulnerability and Opportunity," Crowell & Moring Homeland Security Breakfast Series, Washington, DC (Jan. 24, 2008). Moderator and Speaker: David Z. Bodenheimer.

"Homeland Security Technology: Where the Technology is Going & the Money is Flowing," Crowell & Moring Homeland Security Breakfast Series, Washington, DC (Nov. 15, 2007). Speaker & Panel Moderator: David Z.

biography

## David Bodenheimer

Bodenheimer.

"Future of Homeland Security Technology," Crowell & Moring Homeland Security Breakfast Series, Washington, DC (Sept. 18, 2007). Moderator: David Z. Bodenheimer.

"Cybersecurity: Old Targets, New Strategies," ABA Annual Conference, Public Contract Law Section, San Francisco (Aug. 12, 2007). Moderator: David Z. Bodenheimer.

"Playing by Its Own Rules: TSA's Exemption from the Federal Acquisition Regulation, and How It Impacts Partnerships with the Private Sector," Testimony before the House Homeland Security Subcommittee on Management, Investigations and Oversight, 110th Cong. (Aug. 1, 2007). Witness: David Z. Bodenheimer.

"Government Contract Claims: The Expanding Litigation Battlefield on Estimates in False Claims Act suits and Defective Pricing Actions," ABA Public Contract Law Section and Center for CLE Teleconference, Washington, DC (March 2007). Speaker: David Z. Bodenheimer.

"Discussion with Stewart Baker (DHS Assistant Secretary for Policy): Biodefense, Cybersecurity, and Technology Issues in Homeland Security," ABA Science and Technology Section's Committee on Homeland Security, Washington, DC (January 2007). Moderator: David Z. Bodenheimer.

"Helping Business Protect the Homeland: Is the Department of Homeland Security Effectively Implementing the SAFETY Act: Testimony Before the House Homeland Security Subcommittees on Management, Integration & Oversight and Emergency Preparedness, Science & Technology, 109th Cong. (Sept. 13, 2006). Witness: David Z. Bodenheimer.

"IT Homeland Security Risks & Opportunities: Technology, Privacy & Cybersecurity," BNA 4th Annual Homeland Security Contracting Opportunities Conference, Washington, DC (May 2006). Presenter: David Z. Bodenheimer.

"Privacy & Cybersecurity Dilemma in Balancing the Homeland Security Mission to Gather & Share Information," BNA 3rd Annual Homeland Security Contracting Opportunities Conference, Arlington, VA (May 2005). Presenter: David Z. Bodenheimer.

"Border & Transportation Security: Emerging Issues & Practical Perils in Contracting," BNA 2nd Annual Contracting with DHS Conference (May

biography

## David Bodenheimer

2004). Presenter: David Z. Bodenheimer.

"Defective Pricing & False Claims Act," Federal Publications Seminar - Washington, DC (Septempber 2003-present). Speaker: David Z. Bodenheimer.

"Pricing of Adjustments in Administration of Government Contracts," The George Washington University Law School (1997 and 1998). Speaker: David Z. Bodenheimer.

**DISCLOSURE FORM FOR WITNESSES**
**CONCERNING FEDERAL CONTRACT AND GRANT INFORMATION**

**INSTRUCTION TO WITNESSES:** Rule 11, clause 2(g)(4), of the Rules of the U.S. House of Representatives for the 111th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants) received during the current and two previous fiscal years either by the witness or by an entity represented by the witness. This form is intended to assist witnesses appearing before the House Armed Services Committee in complying with the House rule.

**Witness name: David Z. Bodenheimer**

**Capacity in which appearing:** (check one)

_X__Individual

___Representative

**If appearing in a representative capacity, name of the company, association or other entity being represented:**_____

**FISCAL YEAR 2009**

| federal grant(s) / contracts | federal agency | dollar value | subject(s) of contract or grant |
|---|---|---|---|
| None | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**FISCAL YEAR 2008**

| federal grant(s) / contracts | federal agency | dollar value | subject(s) of contract or grant |
|---|---|---|---|
| None | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**FISCAL YEAR 2007**

| Federal grant(s) / contracts | federal agency | dollar value | subject(s) of contract or grant |
|---|---|---|---|
| None | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Federal Contract Information:** If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) with the federal government, please provide the following information:

Number of contracts (including subcontracts) with the federal government:

Current fiscal year (2009): None;
Fiscal year 2008: None;
Fiscal year 2007: None.

Federal agencies with which federal contracts are held:

Current fiscal year (2009): None;
Fiscal year 2008: None;
Fiscal year 2007: None.

List of subjects of federal contract(s) (for example, ship construction, aircraft parts manufacturing, software design, force structure consultant, architecture & engineering services, etc.):

Current fiscal year (2009): None;
Fiscal year 2008: None;
Fiscal year 2007: None.

Aggregate dollar value of federal contracts held:

Current fiscal year (2009): None;
Fiscal year 2008: None;
Fiscal year 2007: None.

**Federal Grant Information:** If you or the entity you represent before the Committee on Armed Services has grants (including subgrants) with the federal government, please provide the following information:

Number of grants (including subgrants) with the federal government:

Current fiscal year (2009): None;
Fiscal year 2008: None;
Fiscal year 2007: None.

Federal agencies with which federal grants are held:

Current fiscal year (2009): None;
Fiscal year 2008: None;
Fiscal year 2007: None.

List of subjects of federal grants(s) (for example, materials research, sociological study, software design, etc.):

Current fiscal year (2009): None;
Fiscal year 2008: None;
Fiscal year 2007: None.

Aggregate dollar value of federal grants held:

Current fiscal year (2009): None;
Fiscal year 2008: None;
Fiscal year 2007: None.

# United States House of Representatives
# House Armed Services Committee
# Terrorism and Unconventional Threats and Capabilities Subcommittee

## Hearing on:
## *Private Sector Perspectives on Department of Defense Information Technology and Cybersecurity Activities*

Dr. Fred B. Schneider
fbs@cs.cornell.edu
(607) 255-9221

Samuel B. Eckert Professor of Computer Science
Cornell University
4115C Upson Hall
Ithaca, New York 14853

February 19, 2010

**Testimony of Fred B. Schneider**
**Samuel B. Eckert Professor of Computer Science**
**Cornell University, Ithaca, New York**
**February 19, 2010**

Good afternoon Chairwoman Sanchez, Ranking Member Miller, and distinguished members of the Committee. I appreciate this opportunity to comment on cyber security research and education. I am Fred B. Schneider, a Computer Science professor at Cornell University and Chief Scientist of the NSF-funded TRUST[1] Science and Technology Center, a collaboration involving researchers at U.C. Berkeley, Carnegie-Mellon University, Cornell University, Stanford University, and Vanderbilt University. Today, I come before you as a representative of the Computing Research Association, an organization devoted to the mission of strengthening research and advanced education in computing, and comprised of more than 200 academic departments of computer science, computer engineering, and schools of information; 20 industrial computing research labs; and 6 affiliated professional societies.

I have been a Computer Science faculty member since 1978, actively involved in research, education, and in various advisory capacities for both the private and public sectors. Besides teaching and doing research at Cornell, I am a member of the DoD Defense Science Board (DSB), the Dept. of Commerce Information Security and Privacy Advisory Board (ISPAB), the Computing Research Association's board of directors (where I chair of the CRA Government Affairs committee), and a council member of the Computing Community Consortium. I also co-chair Microsoft's TCAAB external advisory board on trustworthy computing.

---

Our nation's increasing dependence on computing systems that are not trustworthy puts individuals, commercial enterprises, the public sector, and our military at risk. Increased data on-line, increased networking, and increased computing all mean increased exposure. These computing systems need to work as we expect—to operate despite failures and despite attacks. They need to be *trustworthy*.

The risk is particularly problematic for our armed forces, where computing systems have become integral to the success of virtually all aspects of peace-time and war-time operations, ranging from situational awareness and logistics management all the way to command and control of weapons systems. We thus unwittingly are creating new and weakly-defended targets for our adversaries to exploit. Moreover, users of our cyber-enabled systems are often unaware of just how dependent they have become on computing and just how vulnerable they are to attack.

[1] Team for Research in Ubiquitous Secure Technology.

In addition, computer systems and networks are increasingly being interconnected in subtle and unexpected ways, resulting in surprising and hidden dependencies of one system on another. Cyber-security of military systems often depends on the trustworthiness of private-sector and/or public-sector systems. The success of military operations then becomes hostage to the security of these other systems. For example, mission-critical functionality could depend on the Internet or could co-exist on computers that also host mundane administrative functions. These interdependencies create paths that enable attackers to compromise some system that is not seen as critical, and thus is not well protected, as a means to reach a critical asset that might actually be well protected. The recent trend towards outsourcing computation in third-party "clouds" will only make the problems worse.

The growth in attacks we witness today should not be surprising. The more we depend on a system, the more attractive a target it becomes to somebody intent on causing disruption; and the more value that is controlled by a system, the more attractive a target it becomes to somebody seeking illicit gain. But more disturbing than the growth in attacks is that our defenses can't keep up. The core of this problem is the asymmetric nature of cyber-security:

- **Defenders are reactive; attackers are proactive.** Defenders must defend all places at all times, against all possible attacks (including those not known about by the defender); attackers need only find one vulnerability, and they have the luxury of inventing and testing new attacks in private as well as selecting the place and time of attack at their convenience.

- **New defenses are expensive to develop and deploy; new attacks are cheap.** Defenders have significant investments in their approaches and business models, while attackers have minimal sunk costs and thus can be quite agile.

- **The effectiveness of defenses cannot be measured; attacks can.** Since we cannot currently quantify how a given security technology or approach reduces risk from attack, there are few strong competitive pressures to develop defenses. So vendors frequently compete and are evaluated on the basis of ancillary factors (e.g., speed, integration, brand development, etc.). Attackers see their return-on-investment and have strong incentives to improve their offerings.

The result has been a cyber-security mentality and industry built around defending against known attacks. Our defenses improve *only* after they have been successfully penetrated. And this is a recipe to ensure some attackers succeed—not a recipe for achieving system trustworthiness and not an acceptable state of affairs for military systems. We must move beyond reacting to yesterday's attacks (or what attacks we predict for tomorrow) and instead start building systems whose trustworthiness derives from first principles.

Yet today we lack the understanding to adopt that proactive approach; we lack a "science base" for trustworthiness. We understand that the landscape includes attacks, defense

mechanisms, and security properties. But we are only now starting to characterize the lay of the land in terms of how these features relate—answers to questions like: What security properties can be preserved by a given defense mechanism? What attacks are resisted by a given mechanism? How can we overcome the inevitable imperfections in anything we might build, yet still resist attacks by, for example, forcing attackers to work too hard for their expected pay-off. Having a science base should not be equated with implementing absolute security or even concluding that security requires perfection in design and implementation. Rather, a science base should provide—independent of specific systems— a principled account for techniques that work, including assumptions they require and ways one set of assumptions can be transformed or discharged by another. It would articulate and organize a set of abstractions, principles, and trade-offs for building trustworthy systems, given the realities of the threats, of our security needs, and of a broad new collection of defense mechanisms and doctrines. And it would provide scientific laws, like the laws of physics and mathematics, for trustworthiness.

An analogy with medicine can be instructive here. Some maladies are best dealt with in a reactive manner. We know what to do when somebody breaks a finger, and each year we create a new influenza vaccine. But only after significant investments in basic medical sciences are we starting to understand the mechanisms by which cancers grow, and developing a cure seems to require that kind of deep understanding. Moreover, nobody believes that disease will some day be a "solved problem." We make enormous strides in medical research yet new threats emerge and old defenses (e.g., antibiotics) are seen to lose their effectiveness.

Like medicine and disease, system trustworthiness is never going to be a "solved problem". There will be no "magic bullet" trustworthiness solution, just as there is not going to be a miracle cure for all that ails you. We must plan to make continuing investments, because the problem will continue evolving:

- **The sophistication of attackers is ever growing, so if a system has vulnerabilities then they will find it**. Any assumption made when building a system does, in fact, constitute a vulnerability, so every system will have vulnerabilities of one sort of another. And with enough study, attackers will find these vulnerabilities and find ways to exploit them.

- **The technology base used by our systems is rapidly changing.** Systems are replaced on a 3-5 year time span, not because computers or software wear out but because newer software and hardware offers improved functionality or better performance (which is then leveraged into new functionality). New systems will work differently, will involve different assumptions, and therefore will require new defenses.

- **The settings in which our computing systems are deployed and the functionality they provide is not static.** With new settings come new opportunities for attack and disruption, whether it is creating a blackout by

attacking the "smart grid" or predicting the target destination for a Predator UAV by monitoring the (unencrypted) video stream it broadcasts while en route.

We can expect to transcend the constant evolution only through the understanding that a science base provides. A science base is also our only hope for developing a suite of sound quantitative trustworthiness measures, which in turn could enable intelligent risk-management decisions, comparisons of different defenses, and incentivize investments in new solutions.

A science base for trustworthiness would not distinguish between classified and unclassified systems, nor would it distinguish between government and private-sector systems. The threats and trade-offs might be different; the principles are going to be the same. But even an understanding of how to build trustworthy systems for the private sector would by itself be useful in military and government settings, simply because so-called COTS (commercial off the shelf) technologies that are developed by the private sector for the private sector are widely used within the military too.

Many equate cyber-security research with investigations solely into technical matters. This oversimplifies. Achieving system trustworthiness is not purely a technology problem. It also involves policy (economic and regulatory). Technological solutions that ignore policy questions risk irrelevance, as do policy initiatives that ignore the limits and capabilities of technology. So besides investing in developing a science base for trustworthiness, we must also invest in research that bridges the technical and the non-technical. We need to understand when we might get more traction for trustworthiness from a policy solution than from a technology one. For example, identifiers—your mother's maiden name, your credit card number, your bank account number, and your social security number—are not a good basis for authentication because they will be known to many. So regulation that prohibits the use of identifiers as authenticators might more effectively defend against identity theft than new technology could.

As another example, there is much talk now about making the Internet more secure by adding the means to trace packets back to their senders and the software that generated the packets. With this *doctrine of accountability*, unacceptable actions aren't prevented but simply attributed, which in turn brings repercussions for the perpetrator—trial, conviction, and penalties in the civilian setting or some sort of sanctions or military retaliation in the international setting. Of course, suitable evidence must be available, and the accuracy of claims being made about accountability is crucial.

But there is a tension between accountability and anonymity, so a doctrine of accountability if not instantiated with great care could impinge on our societal values, our culture, and our laws. Such changes may be feasible in the military setting; but they are unlikely to be embraced in Internet, and the military will have to depend on the Internet for some time come. Thus, we need to understand what effects proposed technological changes could have; forgoing social values like anonymity and privacy (in some sense, analogous to freedom of speech and assembly) in order to make the Internet more-

trustworthy might significantly limit the Internet's utility to some, and thus not be seen as progress.

Moreover, a doctrine of accountability in networked systems isn't something that can be enforced locally. When network traffic crosses international borders, accountability for originating a packet can be preserved only if all countries carrying that traffic cooperate. Some countries will see mandates for cooperation as mandates to cede autonomy, and they will resist. Various cultures resolve tension between anonymity and accountability in different ways, perhaps even selecting different trade-offs for their own traffic than for outsiders' traffic. In short, there is no universal agreement on mandates for accountability. Yet without either having such agreement or limiting places with which we are willing to communicate, our attempts to implement a doctrine of accountability cannot succeed.

Finally, beyond system and legal support for accountability, we will need analysis methods that can be used to identify a perpetrator after an offense has occurred. Classical techniques for criminal investigations in the physical world—the fingerprint on the wine glass, the fiber sample from the rug, DNA matching—aren't much use on data packets. Bits are bits, and they don't travel with detritus that can help identify their source, intent, or trajectories. Thus, the relatively new field of computer forensics faces some tough challenges, especially when there's scant system support for accountability, as is the case today. The DARPA "Cyber Genome Project" announced in January is intended to support research that addresses this problem, and thus this DoD initiative is a step in the right direction at the right time.

**Question:** *What research agenda should the DoD be pursuing related to IT and cybersecurity?*

The Department of Homeland Security recently posted a list of studies[2] that each give research agendas for cyber security and trustworthiness. That list of studies includes 19 entries, including two National Research Council (NRC) volumes and one Defense Science Board study. And the list is limited only to recent work. It, for example, omits a 1991 NRC Computer Science and Telecommunications Board study "*Computers at Risk: Safe Computing in the Information Age,*"[3] which, rather presciently begins:

> "The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."

It also omits mentioning the 1999 NRC study "*Realizing the Potential of C4I: Fundamental Challenges,*"[4] which focused on three key areas—interoperability, information system security, and DoD process and culture—in the command, control,

[2] See http://www.cyber.st.dhs.gov/documents.html.
[3] http://www.nap.edu/catalog.php?record_id=1581#toc
[4] http://www.nap.edu/catalog.php?record_id=6457

communications, computers, and intelligence programs in the military. The start of the security recommendations section of the report states that

> "The same military diligence and wisdom that the U.S. military uses to defend physical space can and must be applied to defend the cyberspace in which C4I systems operate."

What is perhaps more impressive than the number of government-supported studies that elucidate cyber-security research agendas is that these cyber-security research agendas all are in agreement about research needs. The requirements of the military are not all that different, here, than the cyber-security needs for other sectors. The policy options available in a military setting might be different, but the basic outlines of the technological options are probably not. In short, there is little to be gained in constructing yet one more research agenda and there is a considerable cost: constructing another research agenda would take valuable time, causing a further delay before our nation's researchers can turn their attention to making progress on solutions.

I would, however, like to take this opportunity to provide a lens through which the space of research might be viewed, giving what I see as key principles for defining the scope and direction of DoD trustworthiness research investments, going forward.

- **We must not let short-term needs derail the research investments that are the only way to obtain long-term and long-lasting solutions.** Too much federal funding—especially DoD funding—in the recent past has been focused on developing near-term solutions to immediate problems. Funding short-term solutions is consistent with the reactive approach to cyber security. We can no longer afford to be reactive. Instead of putting our thumb in the dike, we need to look into the future and think proactively.

- **Researchers must consider the real attackers we face today and those we expect to encounter tomorrow—not just hypothetical attackers.** This requires access to real data about how the systems and networks that are to be protected are being used. There is a tension here, as the military is reluctant to release operational data about its systems and networks, even in a sanitized form.

- **We must embrace research that bridges policy (regulation and economics) with technology.** As discussed above, to do research in technology without knowledge of policy or vice versa risks irrelevance. With the monetization of hacking, understanding the economics of the underground cyber criminals is critical to defending against them and /or disrupting their criminal activities.

- **We must continue to invest broadly in research concerned with building software systems: operating systems, networks, programming languages, formal methods, database systems, etc.** Ultimately, the things that undermine a system's trustworthiness will be traced to errors in design, implementation, requirements, or assumptions.

**Federal Funding for Research.** A list of research problems is just a start. Somebody needs to do the research listed on any research agenda. Faculty at our nation's universities are the engines of innovation. Not only do faculty drive basic research in the U.S., but university researchers also have a strong track record of transitioning that work to practice, This means that the funding climate for cyber-security research at universities is critically important for making progress on any cyber-security research agenda. Faculty are attracted by hard problems (and cyber-security provides plenty of those), but faculty are only attracted to research areas where resources are available to work on solutions.

DoD supports cyber security research through DARPA, through the MURI program, and through the services (AFOSR, ARO, and ONR). Over the last 30 years, this has been a critical source of funding for those of us in the research community who are concerned with topics most relevant to trustworthiness.

NSF recently has become a significant source of research funding, but this was partly offset by DARPA's decision under former Director Tether not to fund unclassified work in trustworthiness at universities. Other agencies, such as DHS and IARPA picked up some of the slack when DARPA stopped providing funding. However, DHS's cyber security funding tends to be more short-term and at a much lower level. IARPA has funded some trustworthiness research, but again it leans towards short-term projects.

Long-term stable funding in trustworthy computing is crucial for progress. The President's Information Technology Advisory Committee's independent report *Cyber Security: A Crisis of Prioritization*[5] points out that a lack of continuity in cyber security funding discourages younger faculty and graduate students from entering fields where future funding is uncertain. This prevents researchers from undertaking the kind of long-term exploration that is so needed to rise above our reactive approach. It also leads to a shortage of cyber security expertise, as researchers exit the field for better-funded areas of inquiry.

The overall level of funding for cyber security research is generally seen as dangerously low. The PITAC report makes this point quite explicitly. IT security expenditures are estimated to reach $79 billion annually by 2010[6]. According to the NITRD *Networking and Information Technology Research and Development Program*[7], $342.5M was being requested for FY2010 "Cyber Security & Information Assurance." This means Federal budget requests for unclassified research in system trustworthiness total roughly .4% of the expenditures that might be leveraged by the research. Moreover, anecdotal information about specific funding programs at various key Federal agencies suggests

---

[5] *Cyber Security: A Crisis of Prioritization*. President's Information Technology Advisory Committee, Feb. 2005. http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

[6] *Information Security Products & Services – Global Strategic Business Report*, Global Industry Analysts, Inc, July 2007.

[7] *The Networking and Information Technology Research and Development Program*. Report by the Subcommittee on Networking and Information Technology Research and Development, May 2009. page 21, http://www.nitrd.gov/Pubs/2010supplement/FY10Supp-FINAL-Preprint-Web.pdf

that only a portion of the $342.5M is spent on academic research in cyber-security. It then comes as no surprise to find the recent National Research Council CSTB report *Toward a Safer and More Secure Cyberspace*[8] stating that funding levels for cyber-security research are low, preventing researchers from pursuing their promising research ideas. And this echoes the findings in the PITAC report[9] which stated that (i) cyber-security solutions would emerge only from a vigorous and well funded program of research and (ii) that levels of funding were dangerously low to solve problems or to sustain a community of researchers.

Finally, note that having an ecology of Federal agencies that fund cyber-security research—and indeed, computing research broadly—is quite valuable. And there once was such a diverse ecology of funding sources for the various styles and topics that trustworthiness research spans. But that ecosystem has been eroding, as funding agencies have redefined their priorities. Inter-agency coordination that has been voluntary and tight budgets have prompted some of the Federal funding-agencies to reduce their IT and cyber-security research investments and/or to focus those expenditures on short-term work, which they see as better suited for their missions. Some of these decisions are difficult to defend, given the central role that system trustworthiness plays in the missions these agencies are supposed to support. DoD, which involves a number of distinct units that fund IT and cyber-security research, is thus missing an opportunity when it allows these to function as isolated and independent agencies.

**Question:** *What are we doing as a nation to ensure we have a future pipeline of IT professionals (including supporting K-12 educational activities)?*

Cyber-security professionals are today not adequate in number and not being adequately trained to meet the needs of either the military or civilian sectors.

- **Part of the problem is resources**. University Computer Science (CS) departments lack the faculty to offer the relevant courses. Few faculty members have the necessary expertise to offer courses in this area. And even if a CS department has managed to hire a few cyber-security specialists, they will likely also be involved in teaching the large complement of other classes that need to be covered by a department giving undergraduate and graduate CS degrees.

- **Part of the problem is content**. The field is relatively young and fast moving. There is not yet widespread agreement about what technical content must be covered, which makes this an exciting time to be teaching cyber-security at the university level. But it also means that textbooks and other teaching materials have short lives unless they are frequently revised, which is a disincentive to some

[8] *Toward a Safer and More Secure Cyberspace*. S Goodman and H. Lin (eds), National Academies Press, Washington, DC, 2007. Appendix B.6. http://books.nap.edu/catalog.php?record_id=11925

[9] *Cyber Security: A Crisis of Prioritization*. President's Information Technology Advisory Committee, Feb. 2005. http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

> authors. So there are fewer good textbooks than would be found in a more mature subject. Yet, creating agreement on content by legislating a curriculum would be a serious mistake at this point, because it would retard the dissemination of new ideas to students and it would discourage faculty from writing texts that reflect improvements in our understanding of the field.

Some institutions have been able to distinguish themselves by offering particularly strong programs in trustworthiness and in cyber-security. Little is gained by giving that list here. However, I would be remiss if I failed to mention two DoD programs that have been leaders in cyber-security education, not only within DoD but at the national level: West Point and the Naval Postgraduate School. DoD investments in these programs have been highly leveraged both (i) in producing military personnel who are well educated and (ii) in helping other universities design their courses and curricula in cyber-security.

Outside of DoD educational institutions, the problem of undergraduate education in cyber-security is complicated by the broad clientele that Computer Science departments serve. Some have argued that all undergraduates should be trained in cyber-security; and this might be a reasonable strategy for our nation's service academies. But not all undergraduate Computer Science majors in public or private universities are headed for system-building careers, and students destined for other careers need to master other content. Also, not all system developers were computer science majors as undergraduates. Thus, it just doesn't make sense to impose a cyber-security requirement on all students in University Computer Science departments.

**University Curriculum**. I believe that the more sensible approach is for our nation's universities to offer specializations in system trustworthiness. Students will choose this specialization, in part to make them attractive to employers and in part because the subject matter is so engaging. A well trained cyber-security professional needs to have exposure to a broad variety of topics. One would expect to see courses that cover technical topics, such as computer security principles, distributed systems and networking, systems reliability, software engineering, cryptography, and user interfaces and human factors. But I also strongly advocate exposure to non-technical topics, including cyber-law (intellectual property law, communications law, privacy law), ethics, economics of computing and networking, business strategy, and human relations (i.e., management of people). This broad education would enable a cyber-security professional to use all conceivable technical and policy tools for achieving trustworthiness. It would also ensure that solutions could be evaluated in a broader societal context, so that risk-management and trade-offs between different social values (such as privacy versus accountability) can be contemplated.

There is likely more than 1 year's worth of content past today's CS BS degree, but there is probably less than 3 years of course material. This would argue for creating some sort of graduate, professional degree program. It would be designed so that its students would learn both the technical and the non-technical topics needed to define and develop trustworthy computing systems, manage them, and oversee their deployment, use, and evolution.

**A Cybersecurity Credential.** Most professions expect their practitioners to have a credential before they are allowed to practice. But I believe that credentials by themselves are not the solution. At best, they are a symptom of a solution. For example, you might hope that a credentialed individual would engage in best practices. But hope is all you can do. Possession of a credential does not by itself compel the use of best practices, and it is easy to imagine credentialed system builders cutting corners by choice (such as out of laziness) or by mandate (such as from management trying to cut costs). Also, the value of a credential depends on the institutions that define what content must be mastered to obtain the label. To whom should society be willing to vest that responsibility? How do we ensure that the content and standards enshrined by the credential have been selected based entirely on society's best interests rather than financial gain or commercial advantage?

In a fast moving field, content will change rapidly. The credentialing process must keep up, as must credential holders. Otherwise, credentials impede the spread of innovation because people who employ practices learned for a credential are soon engaging in outdated methods. So a credentialing scheme must take this into account.

We are not the first group of professionals to face these problems. Credentialing schemes that the legal and medical professions use, for example, seem to serve society well. Therefore, it would be wise to understand the particulars of those credentialing processes before endeavoring to create one for producers of trustworthy systems. I see three elements as being crucial to the success of these extant schemes:

- Obtaining a credential requires far more than passing an examination. To earn a credential, a candidate undertakes years of post-bachelors education, in which the curriculum has been set by the most respected thinkers and practitioners in the field.
- Credential holders are required to stay current with the latest developments in the field by continuing their education through courses sanctioned by the institution that issues credentials.
- The threat of legal action to individuals (including malpractice litigation) incentivizes professionals to engage in best practices.

In sum, using exams to create labels for our workforce might sound like a way to get more trustworthy systems, but it's not. To have the desired effect, a credential must bestow obligations and responsibilities on practitioners. Moreover, curriculum and educational programs—not an exam—are central to the enterprise.

**The Overall IT Workforce.** Beyond concerns about the supply of cyber-security professionals, there is considerable concern within the IT community about the adequacy of the overall IT workforce—particularly in light of recent Bureau of Labor Statistics' projections of the increasing demand for computing and mathematical science graduates

in the U.S. and recent enrollment and degree production statistics. The most recent BLS ten-year projections (from 2008-2018) predict computing and mathematical occupations will grow by 22 percent, the fastest of any "professional" occupations in the survey. That's about 150,000 new job openings requiring a computer science or mathematical background over the next decade—an amount that significantly outstrips current degree production.[10] In fact, during the period from 2002–2007, the number of undergraduate degrees in computer science actually dropped by 34 percent.

The statistics at the K-12 level, further up the pipeline, are not particularly encouraging either. While the number of high school students taking Advanced Placement science and math exams has roughly doubled over the past decade, the number of students taking the AP computer science exam has declined in recent years.[11] Participation rates among women and underrepresented minorities in computing at the K-12 level are also troubling. In 2008, only 17 percent of AP computer science test-takers were women, although women represented 55 percent of all AP test-takers. While AP CS participation rates among underrepresented groups has increased the past 10 years, it remains low at 11 percent for the AP CS test, compared to 19 percent for all AP test-takers.

Addressing these issues will require action from federal, state and local policy makers, as well as from the high-tech industry and scientific and education societies like CRA and its affiliates. It is encouraging to see that DARPA, recognizing these pipeline issues are "an issue of national importance," has released a solicitation aimed at garnering innovative new ideas to encourage students to major in computer science and pursue careers as engineers and scientists.[12] Similar efforts at the National Science Foundation aimed at increase participation rates among underrepresented populations, particularly its Broadening Participation in Computing program, have shown positive results. While the root causes of these problems are probably beyond federal agencies' ability to address, efforts like DARPA's CS-STEM program and NSF's BPC can help mobilize communities that have impact. The most recent student data seem to indicate that enrollment in CS programs is once again on the increase, although still way off its peak.[13]

[10] http://www.acm.org/public-policy/08-18%20chart.jpg
[11] http://www.acm.org/public-policy/AP.jpg
[12] https://www.fbo.gov/utils/view?id=69c81b4b7f892d4e0e0d8a7bec0eba29
[13] http://www.cra.org//resources/crn-archive-view-detail/upward_trend_in_undergraduate_cs_enrollment/

**Biographical Sketch**

Fred B. Schneider is Samuel B. Eckert Professor of Computer Science at Cornell University. He joined the Cornell faculty in Fall 1978, having completing a Ph.D. at Stony Brook University, preceded by a B.S. in Engineering from Cornell in 1975. Schneider currently also serves as the Chief Scientist for the NSF-funded TRUST Science and Technology Center, which brings together researchers at U.C. Berkeley, Carnegie-Mellon University, Cornell University, Stanford University, and Vanderbilt University.

Schneider's research has focused on various aspects of trustworthy systems—systems that perform as expected, despite failures and attacks. His early work concerned formal methods to aid in the design and implementation of concurrent and distributed systems that satisfy their specifications; he is author of two texts on that subject: *On Concurrent Programming* and *A Logical Approach to Discrete Mathematics* (co-authored with D. Gries). He is also known for his research in theory and algorithms for building fault-tolerant distributed systems. And his paper on the "state machine approach" for managing replication brought an SOSP "Hall of Fame" award for seminal research.

More recently, his interests have turned to system security. His work characterizing what policies can be enforced with various classes of defenses is widely cited, and it is seen as advancing the nascent science base for security. He is also engaged in research concerning legal and economic measures for improving system trustworthiness.

Schneider was elected Fellow of the American Association for the Advancement of Science in 1992, the Association of Computing Machinery in 1995, and the Institute of Electrical and Electronics Engineers in 2008. He was named Professor-at-Large at the University of Tromso (Norway) in 1996, and was awarded a Doctor of Science *honoris causa* by the University of NewCastle-upon-Tyne in 2003 for his work in computer dependability and security.

Schneider has served since Sept 2006 as a member of the Information Security and Privacy Advisory Board (ISPAB), which advises NIST, the Secretary of Commerce, and the Director of OMB on information security and privacy issues pertaining to Federal Government Information Systems. He was appointed to the Defense Science Board in January 2010. He chaired the National Academies Computer Science and Telecommunications Board study on information systems trustworthiness that produced the 1999 volume *Trust in Cyberspace*. He also served as a member of CSTB from 2002-2008 and served from 2004-2007 on the CSTB study committee for improving cyber-security research. Schneider was a member of the NSF Computer and Information Science and Engineering advisory committee 2002-2006. And in Fall 2001, he chaired the United Kingdom's pentennial external review of research funding for academic Computer Science.

In 2007, Schneider was elected to the board of directors of the Computing Research Association (CRA) and appointed to the steering committee of CRA's Computing Community Consortium. He currently chairs CRA's Government Affairs Committee.

Schneider is a frequent consultant to industry, believing this to be an efficient means of implementing technology transfer as well as learning about the real problems. He is co-chair of Microsoft's Trustworthy Computing Academic Advisory Board, which comprises outside technology and policy experts who meet periodically to advise Microsoft about products and strategy. He also provides technical expertise in computer security as well as more broadly to a variety of firms, including: BAE Systems, Fortify Software, and Microsoft.

# VITA

**FRED B. SCHNEIDER**

Cornell University
Department of Computer Science
4115C Upson Hall
Ithaca, New York 14853
(607) 255-9221 (business)
(607) 257-7762 (home)

January 6, 2010

Date of Birth: December 7, 1953
Citizenship: United States

## EDUCATION

1975 B.S., Cornell University, Computer Science and Electrical Engineering.
1977 M.S., SUNY at Stony Brook, Computer Science.
1978 Ph.D., SUNY at Stony Brook, Computer Science.
Thesis: Structure of Concurrent Programs Exhibiting Reproducible Behavior
Advisor: Professor A. J. Bernstein

## EXPERIENCE

1978 Assistant Professor, Cornell University, Department of Computer Science.
1984 Associate Professor, Cornell University, Department of Computer Science.
1993 Professor, Cornell University, Department of Computer Science.
Director, AFRL/Cornell Information Assurance Institute, January 2000–July 2008.
Chief Scientist, Griffiss Institute, January 2003–January 2004.
Chief Scientist, NST TRUST Science and Technology Center, May 2005–present.
2009 Appointed *Samuel B. Eckert Professor of Computer Science*, Cornell University.

## PROFESSIONAL ACTIVITIES

**Editor:**

*Distributed Computing*, Springer-Verlag, October 1984–present,
(Editor-in-chief, January 1989–August 2000).
*Information Processing Letters*, North-Holland Publishing Company,
March 1987–March 2004.
*IEEE Transactions on Software Engineering*, April 1992–April 1999.
*IEEE Security and Privacy*, March 1994–present (Associate editor-in-chief).
*High Integrity Systems*, March 1993–December 1996.
*Annals of Software Engineering*, January 1994–December 2002.
Texts and Monographs in Computer Science, Springer-Verlag,
January 1988–present, (Co-managing editor since October 1992).
*ACM Computing Surveys*, March 1995–May 2003.
*IEEE Transactions on Dependable and Secure Computing*, March 2004–January 2009.

**Industrial and Professional Advisory:**

CSNet Technical Advisory Panel, July 1980–December 1983;

National Research Council Graduate Fellowship Evaluation Panel, February 1981;
IFIP Working Group 2.3 (Programming Methodology), Observer,
September 1982–July 1984; Member, July 1984–present;
College Board Committee for Advanced Placement Computer Science,
July 1983–July 1988;
Committee on Recommendations for U.S. Army Basic Research,
July 1984–June 1988;
Chairman, Information Systems Trustworthiness,
Computer Science and Telecommunications Board,
National Research Council, National Academy of Sciences;
JavaSoft Security Advisory Committee, JavaSoft Inc., June 1997–Nov 2000;
JXTA Technical Advisory Council, SUN Microsystems, Nov 2000–Nov 2001;
CIGITAL Technical Advisory Board, Nov 2000–present;
deCode Genetics Security Advisory Board, Feb 2000–March 2002;
Eweb University.Com Board of Advisors, March 2000–March 2002;
FAST ASA Technical Advisory Board, March 2000–present;
Intel Microprocessor Research Lab Advisory Board, Oct 2001–August 2004;
UK Dependability Interdisciplinary Research Collaboration (DIRC),
Steering Committee, March 2001–January 2007;
Chairman, UK International Review of Computer Science, March 2001;
ACM Advisory Committee on Security and Privacy (ACSP), Oct 2001–Nov 2003;
National Research Council Computer Science and Telecommunications Board,
March 2002–June 2008;
NSF/CISE Advisory Committee, May 2002–March 2006;
Co-Chair, Microsoft, Trustworthy Computing Academic Advisory Board,
August 2002–present;
IBM Autonomic Computing Advisory Board, August 2002–May 2004;
Packet General Networks Technical Advisory Board, March 2003–September 2007;
Fortify Software Technical Advisory Board, Feb 2004–present;
Committee on Improving Cybersecurity Research,
Computer Science and Telecommunications Board,
National Research Council, National Academy of Sciences, June 2004–September 2007;
Advisory Board, Department of Computer Science, University of Virginia,
July 2005–present;
PCAST Technical Advisory Group on Networking and Information Technology,
July 2006–present;
Information Security and Privacy Advisory Board, Department of Commerce,
Sept 2006-Sept 2010;
Board of Directores, Computing Research Association, July 2007–June 2010;
Council, Computing Community Consortium, July 2007–January 2010;
Defense Science Board, March 2008–present.

**Awards:**

IBM Faculty Development Award (1983).
Fellow, American Association for Advancement of Science (1992).
Fellow, Association for Computing Machinery (1995).
Professor-at-Large, University of Tromsoe, Tromsoe, Norway (1996–).

Daniel M. Lazar Excellence in Teaching Award (2000).
Doctor of Science (*honoris causa*), University of Newcastle, U.K. (May 2003).
ACM SIGOPS Hall of Fame Award (2007).
Fellow, Institute of Electrical and Electronics Engineers (November 2008).

### Patents

1. Fault tolerant computer system with shadow virtual processor. United States Patent 5,488,716, January 30, 1996. Co-inventors: E. Balkovich, B. Lampson, and D. Thiel.
2. Transparent fault tolerant computer system. United States Patent 5,802,265, Sept. 1, 1998. Co-inventors: T. C. Bressoud, J. E. Ahern, K. P. Birman, R. C. B. Cooper, B. Glade, and J. D. Service.
3. Transparent fault tolerant computer system. United States Patent 5,968,185, Oct. 19, 1999. Co-inventors: T. C. Bressoud, J. E. Ahern, K. P. Birman, R. C. B. Cooper, B. Glade, and J. D. Service.
4. A method for improving search engine efficiency. Norwegean Patent 327318, June 8, 2009. Co-inventors: Johannes Gehrke and Robbert van Renesse.

## PUBLICATIONS

### Books

1. *A Logical Approach to Discrete Math.* Springer-Verlag, NY, 1993, 500 pages. With David Gries.
2. *Instructor's Manual for "A Logical Approach to Discrete Math".* D. Gries and F. B. Schneider, Ithaca, NY, 1993. 311 pages. With David Gries.
3. *On Concurrent Programming.* Springer-Verlag, NY, 1997, 473 pages.
4. *Trust in Cyberspace.* (Editor) National Academy Press, December 1998, 331 pages.

### Journals

1. Conditions for the equivalence of synchronous and asynchronous operation. *IEEE Transactions on Software Engineering* SE-4, 6 (November 1978), 507–516. With A. J. Bernstein, E. A. Akkoyunlu and A. Silbershatz.
2. Master keys for group sharing. *Information Processing Letters* 12, 1 (February 1981), 23–25. With D. Denning.
3. More on master keys for group sharing. *Information Processing Letters* 13, 3 (December 1981), 125–126. With D. Denning and H. Meijer.
4. Synchronization in distributed programs. *TOPLAS* 4, 2 (April 1982), 125–148.
5. Fail-stop processors: An approach to designing fault-tolerant computing systems. *TOCS* 1, 3 (August 1983), 222–238. With R. D. Schlichting.
6. User recovery and reversal in interactive systems. *TOPLAS* 6, 1 (January 1984), 1–19. With J. Archer and R. W. Conway.
7. The 'Hoare Logic' of CSP and all that. *TOPLAS* 6, 2 (April 1984), 281–296. With L. Lamport.

8. Fault-tolerant broadcasts. *Science of Computer Programming* 4, 1 (April 1984), 1–15. And D. Gries and R. D. Schlichting.
9. Key exchange using 'Keyless Cryptography'. *Information Processing Letters* 16, 2 (February 1983), 79–82. With B. Alpern.
10. Concepts and notations for concurrent programming. *ACM Computing Surveys* 15, 1 (March 1983), 3–44. With G. Andrews. Reprinted in:
    i. *bit Magazine* (in Japanese),
    ii. *Programming Languages: A Grand Tour*, Third Edition, E. Horowitz (ed.), Computer Science Press,
    iii. *Concurrent Programming*, Narian Gehani and Andrew D. McGettrick (eds.), Addison-Wesley Publishing Company, 1988.
    iv. *Distributed Computer Systems*, H. S. M. Zedan (ed.), Butterworths, London, 1990.
11. Using message-passing for distributed programming: Proof rules and disciplines. *TOPLAS* 6, 3 (July 1984), 402–431. With R. D. Schlichting.
12. Byzantine generals in action: Implementing fail-stop processors. *TOCS* 2, 2 (May 1984), 145–154.
13. Derivation of a distributed algorithm for finding paths in directed networks. *Science of Computer Programming* 6, 1 (January 1986), 1–9. With R. McCurley.
14. Thrifty execution of task pipelines. *Acta Informatica* 22, 1 (1985), 35–45. With R. W. Conway and D. Skeen.
15. Defining liveness. *Information Processing Letters* 21, 4 (October 1985), 181–185. With B. Alpern.
16. Safety without stuttering. *Information Processing Letters* 23, 4 (November 1986), 177–180. With B. Alpern and A. J. Demers.
17. Recognizing safety and liveness. *Distributed Computing* 2, 3 (1987), 117–126. With B. Alpern.
18. Verifying temporal properties without temporal logic. *TOPLAS* 11, 1 (January 1989), 147–167. With B. Alpern.
19. Implementing fault-tolerant services using the state machine approach: A tutorial. *ACM Computing Surveys* 22, 4 (December 1990), 299–319.
20. Trace-based network proof systems: Expressiveness and completeness. *TOPLAS* 14, 3 (July 1992), 396–416. With J. Widom and D. Gries.
21. Preserving liveness: Comments on "Safety and Liveness from a Methodological Point of View". *Information Processing Letters* 40, 3 (November 1991), 141–142. With M. Abadi, B. Alpern, K. R. Apt, N. Francez, S. Katz, and L. Lamport.
22. A formalization of priority inversion. *Real Time Systems* 5 (1993), 285–303. With O. Babaoglu and K. Marzullo.
23. Proving nondeterministically specified safety properties using progress measures. *Information and Computation* 107, 3 (November 1993), 151–170. With N. Klarlund.
24. A new approach to teaching discrete mathematics. *Primus V* 2 (June 1995), 113–138. With D. Gries.
25. Teaching math more effectively, through the design of calculational proofs. *The Mathematical Monthly* (October 1995), 691–697. With D. Gries.
26. Equational propositional logic. *Information Processing Letters* 53, 3 (February 1995), 145–152. With D. Gries.
27. Verifying programs that use causally-ordered message-passing. *Science of Computer*

*Programming* 24, 2 (1995), 105–128. With S. Stoller.

28. Hypervisor-based fault-tolerance. *ACM Transactions on Computer Systems* 14, 1 (February 1996), 80–107. With T. Bressoud.
29. Adding the everywhere operator to propositional logic. *Journal of Logic and Computation* 8, 1 (February 1998), 119–129. With D. Gries.
30. Building trustworthy systems: Lessons from the PTN and Internet. *IEEE Internet Computing*, 3, 5 (November-December 1999), 64–72. With S. Bellovin and A. Inouye.
31. Enforceable security policies. *ACM Transactions on Information and System Security* 3, 1 (February 2000), 30–50.
32. A TACOMA retrospective. *Software–Practice and Experience 32* (2002), 605–619. With D. Johansen, K. J. Lauvset, R. van Renesse, N. P. Sudmann, and K. Jacobsen.
33. COCA: A secure distributed on-line certification authority. *ACM Transactions on Computer Systems* 20, 4 (November 2002), 329–368. With Lidong Zhou and Robbert van Renesse.
34. Tolerating malicious gossip. *Distributed Computing 16*, 1 (February 2003) 49–68. With Yaron Minsky.
35. Least privilege and more. *IEEE Security and Privacy 1*, 3 (Sept/Oct 2003), 55-59.
36. CODEX: A robust and secure secret distribution system. *IEEE Transactions on Dependable and Secure Computing* 1, 1 (January-March 2003), 34–47. With Michael Marsh.
37. Automated analysis of fault-tolerance in distributed systems. *Formal Methods in System Design* 28, 2 (March 2005), 183–196. With Scott D. Stoller.
38. APSS: Proactive secret sharing in asynchronous systems. *ACM Transactions on Information and System Security* 8, 3 (August 2005), 259–286. With Lidong Zhou and Robbert van Renesse.
39. Implementing trustworthy services using replicated state machines. *IEEE Security and Privacy 3*, 5 (Sept/Oct 2005), 34–43. With Lidong Zhou.
40. Computability classes for enforcement mechanisms. *TOPLAS* 28, 1 (January 2006), 175–205. With Kevin Hamlen and Greg Morrisett.
41. The monoculture risk put into context. *IEEE Security and Privacy 7*, 1 (January/February 2009), 14–17. With Ken Birman.
42. Quantifying Information Flow with Beliefs. *Journal of Computer Security* 17(5), pages 655–701, 2009. With Michael R. Clarkson and Andrew C. Myers.

### Conference Proceedings

1. On language restrictions to ensure deterministic behavior in concurrent systems. *Proc. of Third Jerusalem Conference on Information Technology* (Jerusalem, Israel, August 1978), North-Holland, New York, 537–541. With A. J. Bernstein.
2. Ensuring consistency in a distributed database system by use of distributed semaphores. *Proc. International Symposium on Distributed Databases* (Paris, France, March 1980), North-Holland, New York, 183–189.
3. The master key problem. *Proc. 1980 Symposium on Security and Privacy* (Oakland, California, April 1980), IEEE Computer Society, Oakland, California, 103–107. With D. Denning.
4. Towards fault tolerant process control software. *Proc. of 1981 International Symposium on Fault-Tolerant Computing* (Portland, Maine, June 1981), IEEE Computer

Society, Oakland, California, 48–55. And R. D. Schlichting.

5. Understanding and using asynchronous message-passing primitives. *Proc. of ACM Symposium on Principles of Distributed Computing* (Ottawa, Canada, August 1982), ACM, New York, 141–147. With R. D. Schlichting.
6. Fail-Stop processors. (Invited Paper.) *Digest of Papers Spring Compcon '83* (San Francisco, California, March 1983), IEEE Computer Society, Oakland, California, 66–71.
7. Declarations: A uniform approach to aliasing and typing. *Proc. of 12th Annual ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages* (New Orleans, Louisiana, January 1985), ACM, New York, 205–216. With L. Lamport.
8. Inexact agreement: Accuracy, precision, and graceful degradation. *Proc. Fourth Annual SIGACT-SIGOPS Symposium on Principles of Distributed Computing* (Minaki, Ontario, Canada, August 1985), ACM, New York, 237–249. With S. R. Mahaney.
9. Symmetry and Similarity in Distributed Systems. *Proc. Fourth Annual SIGACT-SIGOPS Symposium on Principles of Distributed Computing* (Minaki, Ontario, Canada, August 1985), ACM, New York, 13–22. With R. E. Johnson.
10. Abstractions for fault-tolerance in distributed systems. (Invited Paper.) *Proc. IFIP 10th World Computer Congress, IFIP '86* (Dublin, Ireland, September 1986), 727–733.
11. A paradigm for reliable clock synchronization. (Invited paper.) *Proc. Advanced Seminar on Real-Time Local Area Networks* (Bandol, France, April 1986), INRIA, 85–104.
12. Completeness and incompleteness of trace-based network proof systems. *Proc. of 14th Annual ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages* (Munich, F. R. Germany, January 1987), 27–38. With J. Widom and D. Gries.
13. Proving Boolean combinations of deterministic properties. *Proc. of 2nd Annual Symposium on Logic in Computer Science* (Ithaca, New York, June 1987), 131–137. With B. Alpern.
14. Primary-Backup Protocols: Lower Bounds and Optimal Protocols. *Proc. 3rd IFIP Working Conference on Dependable Computing for Critical Applications* (Sicily, Italy, September 1992), 187–196. With Navin Budhiraja, Keith Marzullo and Sam Toueg.
15. Optimal primary-backup protocols. *Proc. 6th International Workshop, WDAG '92* (Haifa, Israel, November 1992), Lecture Notes in Computer Science, Volume 647, Springer-Verlag, New York, 1992, 362–378. With Navin Budhiraja, Keith Marzullo and Sam Toueg.
16. Reasoning about Programs by exploiting the environment. *Proc. 21st International Colloquium, ICALP '94* (Jerusalem, Israel, July 1994), Lecture Notes in Computer Science, Volume 820, Springer-Verlag, New York, 328–339. With L. Fix.
17. Hybrid verification by exploiting the environment. *Formal Techniques in Real Time and Fault Tolerant Systems* (Luebeck, Germany, September 1994), Lecture Notes in Computer Science, Volume 863, Springer-Verlag, New York, 1–18. With Limor Fix.
18. Teaching logic as a tool. *Proc. 26th SIGCSE Technical Symposium on Computer Science Education* (Nashville, Tennessee, March 1995), SIGCSE Bulletin 27, 1, 384–385. With D. Gries.
19. Operating system support for mobile agents. *Proc. Fifth Workshop on Hot Topics in Operating Systems (HOTOS-V)* (Orcas Island, Washington, May 1995), 42–45. With Dag Johansen and Robbert van Renesse. Reprinted in:

    - *Readings in Agents*, Michael N. Huhns and Munindar P. Singh (eds.), Morgan Kaufman Publishers, San Francisco, California, 1997. 263–266.

- *Mobility: Processes, Computers, and Agents*, Dejan S. Milojicic, Frederick Douglis, and Richard G. Wheeler (eds.), Addison Wesley and the ACM Press, April 1999, 557–563.

20. Faster possibility detection by combining two approaches. *Proc. 9th International Workshop, WDAG '95* (Le Mont-Saint-Michel, France, September 1995), Lecture Notes in Computer Science, Volume 972, Springer-Verlag, New York, 1995, 318–332. With Scott Stoller.
21. Hypervisor-based Fault Tolerance. *Proc. Fifteenth ACM Symposium on Operating Systems Principles* (Copper Mountain Resort, Colorado, December 1995), Operating Systems Review 29, 5, 1–11. With T. Bressoud.
22. Cryptographic support for fault-tolerant distributed computing. *Proc. of the Seventh ACM SIGOPS European Workshop "System Support for Worldwide Applications"* (Connemara, Ireland, September 1996), ACM, New York, 109–114. With Yaron Minsky, Robbert van Renesse, and Scott D. Stoller.
23. Supporting broad internet access to TACOMA. *Proc. of the Seventh ACM SIGOPS European Workshop "System Support for Worldwide Applications"* (Connemara, Ireland, September 1996), ACM, New York, 55–58. With Dag Johansen and Robbert van Renesse.
24. Automated analysis of fault-tolerance in distributed systems. *Proc. of the First ACM SIGPLAN Workshop on Automated Analysis of Software*, (Paris, France, January 1997), ACM, New York, 33–44. Rance Cleaveland and Daniel Jackson, (eds.). With Scott Stoller.
25. Towards fault-tolerant and secure agentry. *Proc. 11th International Workshop WDAG '97* (Saarbrucken, Germany, September 1997), Lecture Notes in Computer Science, Volume 1320, Springer-Verlag, Heidelberg, 1997, 1–14.
26. Automated stream-based analysis of fault-tolerance. *Formal Techniques in Real-time and Fault-Tolerant Systems (FTRTFT '98)* (Lyngby, Denmark, September 1998), Lecture Notes in Computer Science, Volume 1486, Springer-Verlag, Berlin, 1998, 113–122. With Scott Stoller.
27. NAP: Practical Fault-tolerance for Itinerant Computations. *Proc. 19th IEEE International Conference on Distributed Computing Systems* (Austin, Texas, June 1999), IEEE, 180–189. With D. Johansen, K. Marzullo, K. Jacobsen, and D. Zagorodnov.
28. SASI enforcement of security policies: A retrospective. *Proceedings of the New Security Paradigms Workshop* (Caledon Hills, Ontario, Canada, September 1999), Association for Computing Machinery, 87–95. With Ulfar Erlingsson. Reprinted in:

    - *DARPA Information and Survivability Conference and Exposition (DISCEX'00)* (Hilton Head, South Carolina, January 2000) IEEE Computer Society, Los Alamitos, California, 287–295.

29. IRM enforcement of Java stack inspection. *Proceedings 2000 IEEE Symposium on Security and Privacy* (Oakland, California, May 2000), IEEE Computer Society, Los Alamitos, California, 246–255. With Ulfar Erlingsson.
30. Open source in security: Visiting the bizarre. *Proceedings 2000 IEEE Symposium on Security and Privacy* (Oakland, California, May 2000), IEEE Computer Society, Los Alamitos, California, 126–127.
31. A language-based approach to security. *Informatics: 10 Years Back, 10 Years Ahead* (Saarbrucken, Germany, August 2000), Lecture Notes in Computer Science, Volume

2000 (Reinhard Wilhelm, ed.), Springer-Verlag, Heidelberg, 2000, 86-101. And Greg Morrisett, Robert Harper.

32. Language-based Security: What's needed and Why. *Static Analysis, Proceedings 8th International Symposium SAS 2001* (Paris, France, July 2001), Lecture Notes in Computer Science Volume 2126, Springer-Verlag, Heidelberg, 2001, page 374.
33. Lifting reference monitors from the kernel. *Formal Aspects of Security, FASec 2002* (London, United Kingdom, December 2002), Ali E. Abdullah, Peter Ryan, and Steve Schneider (eds.). Lecture Notes in Computer Science, Volume 2629, Springer-Verlag, New York, 2003, 1–2.
34. Chain replication for supporting high throughput and availability. *Sixth Symposium on Operating Systems Design and Implementation* (OSDI '04), (San Francisco, California, December 2004), USENIX Association, 2004, 91–104. With Robbert van Renesse.
35. Peer-to-peer authentication with a distributed single sign-on service. *Peer-to-Peer Systems III, Third International Workshop IPTPS 2204* (La Jolla, CA, February 2004), Lecture Notes in Computer Science, Volume 3279 (G. Voelker and S. Shenker, eds.), Springer-Verlag, Heidelberg, 2004, 250–258. With William Josephson and Emin Gun Sirer.
36. Distributed Blinding for Distributed ElGamel Re-encryption. *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems* (Columbus, OH USA, June, 2005), IEEE Computer Society, 2005, 815–824. With L. Zhou, M.A. Marsh, and A. Redz.
37. Belief in information flow. *Proceedings 18th IEEE Computer Security Foundations Workshop* (Aix-en-Provence, France, June 20-22, 2005), 31–45. With Michael R. Clarkson and Andrew C. Myers.
38. Certified in-lined reference monitoring on .NET. *Proceedings of the 2006 Programming Languages and Analysis for Security Workshop* (Ottawa, Ontario, Canada, June 10, 2006), ACM, 2006, 7–16. With Kevin W. Hamlen and Greg Morrisett.
39. Independence from obfuscation: A semantic framework for diversity. *Proceedings 19th IEEE Computer Security Foundations Workshop* (Venice, Italy, July 2006), IEEE Press, 2006, 230–241. With Riccardo Pucella.
40. The building blocks of consensus. *Proceedings 9th International Conference on Distributed Computing and Networking* ICDCN 08, (Kolkata, India, Jan. 2008), Lecture Notes in Computer Science, Volume 4904 (S. Rao et al, eds.), Springer-Verlag, Heidelberg, 2008, 54–72. With Yee Jiun Song, Robert van Renesse, and Danny Dolev.
41. Device driver safety through a reference validation mechanism. *Proceedings of the 8th USENIX Symposium on Operating Systems Design and Implementation OSDI '08* (San Diego, CA, December 2008), 241–254. With Dan Williams, Patrick Reynolds, Kevin Walsh, and Emin Gun Sirer.
42. Hyperproperties. *Proceedings 21st IEEE Computer Security Foundations Symposium* CSF 2008, (Pittsburgh, PA, June 2008), 51–65. With Michael R. Clarkson.

## Other Publications

1. Scheduling in Concurrent Pascal. *Operating Systems Review* 12, 2 (April 1978), 15–21. With A. J. Bernstein.
2. Synchronization and concurrent programming. *Handbook of Electrical and Computer Engineering*, John Wiley and Sons, 1983.

3. Abstract data types. *Handbook of Electrical and Computer Engineering*, John Wiley and Sons, 1983.
4. Broadcasts: A paradigm for distributed programs. *Proc. Workshop on Fundamental Issues in Distributed Computing* (Fallbrook, California, December 1980), ACM, New York.
5. Book review: The Practical Guide to Structured Systems Design. *IEEE Spectrum* 18, 3 (March 1981), 92.
6. The fail-stop processor approach. Invited chapter in *Reliability in Distributed Software and Database Systems* (B. Bhargava, ed.), Von Nostrand Reinhold Company, New York, 1987, 370–394.
7. *Distributed Systems—Methods and Tools for Specification.* Lecture Notes in Computer Science, Volume 190, Springer-Verlag, New York, 1985. With M. W. Alford, J. P. Ansart, G. Hommel, L. Lamport, and B. Liskov.
8. A reply to "A Review of the Advanced Course Description in Computer Science of the Educational Testing Service". *Contemporary Education Review* 2, 3. With P. Miller, T. Gill, S. Owicki, B. Presley, and J. Wadkins.
9. Reaching agreement: A fundamental task even in distributed computer systems. *Engineering: Cornell Quarterly* 20, 2 (Fall 1985), 18–22. And O. Babaoglu, K. P. Birman, and S. Toueg.
10. Programming methodology: Making a science out of an art. *Engineering: Cornell Quarterly* 20, 2 (Fall 1985), 23–27. With D. Gries.
11. Concepts for concurrent programming. (Invited Paper.) *Current Trends in Concurrency*, (J. W. de Bakker, W. P. de Roever, and G. Rozenberg, eds.), Lecture Notes in Computer Science, Volume 224, Springer-Verlag, New York, 1986, 669–716. And G. Andrews.
12. The state machine approach: A tutorial. (Invited paper.) *Proc. Workshop on Fault-tolerant Distributed Computing*, (B. Simons and A. Z. Spector, eds.) Lecture Notes in Computer Science, Volume 448, Springer-Verlag, New York, 1990, 18–41.
13. Another position paper on "fairness". *Software Engineering Notes* 13, 3 (July 1988), 1–2. With L. Lamport.
14. Critical (of) issues in real-time systems: A position paper. (Invited paper.) *Real-time systems Newsletter* 4, 2 (Summer 1988), 3–5. Also reprinted in *Distributed Processing Technical Committee Newsletter* 10, 2 (November 1988), 75–77.
15. Cornell's real-time reliable (RR) systems project. *Proc. Foundations of Real-time Computing*, Office of Naval Research Research Initiative Kickoff Workshop, 28–32.
16. Computer Systems. *Computer Science: Achievements and Opportunities*, SIAM Reports on Issues in the Mathematical Sciences, SIAM, Philadelphia, Pennsylvania, 1989, 29–40. With F. Baskett, D. Clark, A. N. Habermann, B. Liskov, and B. Smith.
17. Formal verification of concurrent software. *Proc. of Thirteenth Annual International Computer Software and Applications Conference* (Orlando, Florida, September 1989), 59.
18. Simpler proofs for concurrent reading and writing. *Beauty is Our Business*, Springer-Verlag Texts and Monographs in Computer Science, May 1990, 373–389.
19. Towards derivation of real-time process-control programs. *Proc. of Third Annual Workshop, Foundations of Real-time Computing Initiative* (Washington, DC, October 1990), Office of Naval Research, 373–384. With K. Marzullo.
20. Derivation of sequential, real-time process-control programs. *Foundations of Real-*

*Time Computing: Formal Specifications and Methods*, (A. M. van Tilborg and G. Koob, eds.), Kluwer Academic Publishers, 1991, 39–54. With K. Marzullo and N. Budhiraja.

21. Fault-tolerance support in distributed systems workshop. *ESN Information Bulletin* 91-03 (July 1991), Office of Naval Research European Office, 58–59.
22. The challenge is usability. *2021 AD: Visions of the Future*, National Engineering Consortium, 1991, 50.
23. Putting time into proof outlines. *Proc. of the REX Workshop "Real-Time: Theory in Practice"*, (J. W. de Bakker, C. Huizing, W. P. de Roever, G. Rozenberg, eds.), Lecture Notes in Computer Science, Volume 600, Springer-Verlag, Berlin, 1991, 618–639. And Bard Bloom and Keith Marzullo.
24. Reasoning about real-time actions. *Proc. of Fourth Annual Workshop, Foundations of Real-time Computing Initiative*, (Washington, DC, October 1991), Office of Naval Research, 85–91. And Bard Bloom and Keith Marzullo.
25. Lower bounds for primary-backup implementations of BOFO services. *Proc. of Second Annual Workshop, Ultradependable Multicomputers and Electronic Systems* (Washington, DC, November 1991), Office of Naval Research, 81–86. With Navin Budhiraja, Keith Marzullo, and Sam Toueg.
26. Assertional methods for fault-tolerant, real-time concurrent programs. *Proc. Software Technology Conference 1992* (Los Angeles, California, April 1992) Defense Advanced Research Projects Agency, Software and Intelligent Systems Technology Office and Computing Systems Technology Office, 516–517.
27. Introduction. *Distributed Computing* 6, 1 (June 1992), 1–3.
28. Adding fault-tolerance, virtually. *Proc. of First Annual Workshop on Embedded Systems* (Austin, Texas, January 1993), Office of Naval Research, 41.
29. What good are models and what models are good? Chapter 2, *Distributed Systems*, 2nd Edition (S. Mullender, ed.), Addison Wesley, 1993, 17–25.
30. Replication management using the state machine approach. Chapter 7, *Distributed Systems*, 2nd Edition (S. Mullender, ed.), Addison Wesley, 1993, 169–195.
31. The primary-backup approach. Chapter 8, *Distributed Systems*, 2nd Edition (S. Mullender, ed.), Addison Wesley, 1993, 199–215. With Navin Budhiraja, Keith Marzullo, and Sam Toueg.
32. A role for formal methodists. *Fourth International Workshop on Dependable Computing for Critical Applications* (San Diego, California, January 1994), 29–30. Reprinted in *Dependable Computing and Fault-Tolerant Systems* Volume 9, (F. Cristian, G. LeLann T. Lunt, eds.) Springer-Verlag, 1995, 43–45.
33. Research on fault-tolerant and real-time computing. Software and Systems Program Summary. (Bolling Air Force Base, Washington, DC, September 1994), Air Force Office of Scientific Research, 75–77.
34. Refinement for Fault-Tolerance: An Aircraft Hand-off Protocol. *Foundations of Ultradependable Parallel and Distributed Computing, Paradigms for Dependable Applications*, Kluwer Academic Publishers, 1994, 39–54. With K. Marzullo and J. Dehn.
35. On teaching proof. *Arts & Sciences NewsLetter* 16, 2 (Spring 1995), 3. With D. Gries.
36. Avoiding AAS Mistakes. (Invited paper.) *Proc. of the Air Traffic Management Workshop*, (L. Tobais, M. Tashker, A. Boyle, eds.), NASA Conference Publication 10151, NASA Ames Research Center, February 1995, 133–149.
37. Avoiding the undefined by underspecification. *Computer Science Today Recent Trends and Developments* (Jan van Leeuwen, ed.), Lecture Notes in Computer Science, Volume

1000, Springer-Verlag, 1995, 366–373. With David Gries.
38. On Traditions in Marktoberdorf. *Deductive Program Design* (M. Broy, ed.), ASI Volume F152. Springer-Verlag, Heidelberg, 1–4.
39. Notes on Proof Outline Logic. *Deductive Program Design* (M. Broy, ed.), ASI Volume F152. Springer-Verlag, Heidelberg, 351–394.
40. Report on Dagstuhl Seminar on Time Services, Schloss Dagstuhl, March 11–March 15 1996. *Real-Time Systems* 12, 3 (May 1997), 329–345. With Danny Dolev, Rudiger Reischuk, and H. Raymond Strong.
41. Editorial: New Partnership with ACM. *Distributed Computing* 10, 2 (1997), 63.
42. Improving Networked Information System Trustworthiness: A Research Agenda. *Proceedings 21st National Information Systems Security Conference* (October 1998, Arlington, Virginia), National Computer Security Center, 766.
43. What Tacoma Taught Us. *Mobility: Processes, Computers, and Agents*, Dejan S. Milojicic, Frederick Douglis, and Richard G. Wheeler (eds.), Addison Wesley and the ACM Press, April 1999, 564–566. With Dag Johansen and Robbert van Renesse.
44. Interview with Fred B. Schneider. *Distributed Systems Online.* http://www.computer.org/channels/ds.
45. Formalizations of substitutions of equals for equals. *Millennial Perspectives in Computer Science, Proceedings of the 1999 Oxford-Microsoft Symposium in honour of Professor Sir Antony Hoare*, (Davies, Roscoe, and Woodcock eds.) Palgrave Publishers, Hampshire, England, November 2000, 119–132. With David Gries.
46. A language-based approach to security. *Informatics: 10 Years Back, 10 Years Ahead.* Lecture Notes in Computer Science, Vol. 2000 (Reinhard Wilhelm, editor), Springer Verlag, Heidelberg, 2000, pp. 86-101. And Greg Morrisett, Robert Harper.
47. WAIF: Web of Asynchronous Information Filters. *Future Directions in Distributed Computing* Lecture Notes in Computer Science, Volume 2585 (Schiper, Shvartsman, Weatherspoon, and Zhao, eds.) Springer-Verlag, 2003, 81–86. With Dag Johansen and Robbert van Renesse.
48. Least privilege and more. *Computer Systems: Papers for Roger Needham*, Andrew Herbert and Karen Sparck Jones, eds. Springer-Verlay, New York, 2003, 253–258.
49. Language-Based Security for Malicious Mobile Code. *Department of Defense Sponsored Information Security Research: New Methods for Protecting Against Cyber Threats.* Wiley Publishing Company, Indianapolis, Indiana, 2007, 477–494. With Dexter Kozen, Greg Morrisett, and Andrew C. Myers.
50. Credentials-Based Authorization: Evaluation and Implementation. Abstract of Plenary Lecture. *Proceedings 34th International Colloquium, ICALP 2007* (Wroclaw, Poland, July 2007), Lars Arge, Christian Cachin, Tomasz Jurdzinski, and Andrzej Tarlecki (eds.). Lecture Notes in Computer Science, Volume 4596, Springer-Verlag, Heidelberg, 2007, 12–14.
51. Mapping the Security Landscape: A Role for Language Techniques. Abstract of Invited Lecture. *Proceedings 18th International Conference ,CONCUR 2007* (Lisbon, Portugal, September 2007), Luis Caires and Vasco T. Vasconcelos (eds.). Lecture Notes in Computer Science, Volume 4703, Springer-Verlag, Heidelberg, 2007, 1.
52. Interview: Silver Bullet Talks with Fred Schneider. *IEEE Security and Privacy Magazine 7*, 6 (November/December 2009), 5–7.

**Editorials**

1. On Concurrent Programming. Invited "Inside Risks" column. *Communications of the ACM* 41, 4 (April 1998), 128.
2. Toward Trustworthy Networked Information Systems. Invited "Inside Risks" column. *Communications of the ACM* 41, 11 (November 1998), 144.
3. Evolving Telephone Networks. Invited "Inside Risks" column. *Communications of the ACM* 42, 1 (January 1999), 160. With S. Bellovin.
4. Editorial: Time for Change. *Distributed Computing* Vol. 13, No. 4 (November 2000), 187.
5. Secure Systems Conundrum. Invited "Inside Risks" column. *Communications of the ACM* 45, 10 (October 2002), 160.
6. The Next Digital Divide. Editorial. *IEEE Security and Privacy* 2, 1 (January/February 2004), 5.
7. Time Out for Station Identification. Editorial. *IEEE Security and Privacy* 2, 1 (September/October 2004), 5.
8. It Depends on What You Pay. Editorial. *IEEE Security and Privacy* 3, 3 (May/June 2005), 3.
9. Here Be Dragons. Editorial. *IEEE Security and Privacy* 3, 3 (May/June 2006), 3.
10. Trusted Computing in Context. Editorial. *IEEE Security and Privacy* 5, 2 (March/April 2007), 4-5.
11. Technology Scapegoats and Policy Saviors. Editorial. *IEEE Security and Privacy* 5, 5 (September/October 2007), 3–4.
12. Network Neutrality versus Internet Trustworthiness. Editorial. *IEEE Security and Privacy* 6, 4 (July/August 2008), 3–4.
13. Accountability for Perfection. Editorial. *IEEE Security and Privacy* 7, 2 (March/April 2009), 3–4.
14. Program Committee Overload in Systems. *Communications of the ACM 52*, 05 (May 2009), 34–37. With Ken Birman.
15. Accountability for Perfection. Editorial. *IEEE Security and Privacy* 7, 2 (March/April 2009), 3–4.

**Policy Documents**

1. *Toward a Safer and More Secure Cyberspace.* S Goodman and H. Lin (eds), National Academies Press, Washington, DC, 2007, 328 pages.
2. Security is not a commodity: The road forward for cybersecurity research. Computing Research Initiatives for the 21st Century, Computing Community Consortium. February 2009. With Stefan Savage.
3. Notes for White House 60-day Cyber-Policy Review. E. Lazowska and F.B. Schneider (eds), NSF submission for Cyberspace Policy Review conducted Spring 2009 for the White House.
4. Testimony. United States House of Representatives Committee on Science and Technology, Research and Science Education Subcommittee. Hearing June 10, 2009 on Cyber Security R & D.
5. Testimony. United States House of Representatives Committee on Science and Technology, Technology and Innovation Subcommittee. Hearing October 22, 2009 on Cybersecurity Activities at NIST's Information Technology Laboratory.

**DISCLOSURE FORM FOR WITNESSES**
**CONCERNING FEDERAL CONTRACT AND GRANT INFORMATION**

**INSTRUCTION TO WITNESSES:** Rule 11, clause 2(g)(4), of the Rules of the U.S. House of Representatives for the 111th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants) received during the current and two previous fiscal years either by the witness or by an entity represented by the witness. This form is intended to assist witnesses appearing before the House Armed Services Committee in complying with the House rule.

**Witness name:** **Fred B. Schneider**

**Capacity in which appearing:** (check one)

_X__Individual

___Representative

**If appearing in a representative capacity, name of the company, association or other entity being represented:** Computing Research Association

**FISCAL YEAR 2009**

| federal grant(s) / contracts | federal agency | dollar value | subject(s) of contract or grant |
|---|---|---|---|
| FA9550-06-1-0019 | AFOSR | $301,316 | From Fault-tolerance to Attack Tolerance |
| 0424422 | NSF | $701,225 | Team for Research in Ubiquitous Secure Technology (TRUST) |
| N00014-09-1-0652 | ONR | $320,832 | A Higher-Level Abstraction for Building Secure Distributed Applications |
| | | | |
| | | | |
| | | | |
| | | | |

**FISCAL YEAR 2008**

| federal grant(s) / contracts | federal agency | dollar value | subject(s) of contract or grant |
|---|---|---|---|
| FA9550-06-1-0019 | AFOSR | $67,105 | From Fault-tolerance to Attack Tolerance |
| 0424422 | NSF | $553,869 | Team for Research in Ubiquitous Secure Technology (TRUST) |
| FA8750-07-2-0037 | AFRL | $240,413 | Nexus Operating System for Trustworthy Computing |
| | | | |
| | | | |
| | | | |
| | | | |

**FISCAL YEAR 2007**

| Federal grant(s) / contracts | federal agency | dollar value | subject(s) of contract or grant |
|---|---|---|---|
| FA9550-06-1-0019 | AFOSR | $255,552 | From Fault-tolerance to Attack Tolerance |
| 0424422 | NSF | $643,000 | Team for Research in Ubiquitous Secure Technology (TRUST) |
| FA8750-07-2-0037 | AFRL | $729,711 | Nexus Operating System for Trustworthy Computing |
| FA9550-07-1-0569 | | $75,000 | Homogeneous Enclave Software vs Controlled Heterogeneous Enclave Software |
| FA9550-07-1-0304 | AFRL | $1,000,000 | AFRL/Cornell Information Assurance Institute (IAI) |
| | | | |
| | | | |

**Federal Contract Information:** If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) with the federal government, please provide the following information:

Number of contracts (including subcontracts) with the federal government:

Current fiscal year (2009): 3;
Fiscal year 2008: 3;
Fiscal year 2007: 5.

Federal agencies with which federal contracts are held:

Current fiscal year (2009): 3;
Fiscal year 2008: 2;
Fiscal year 2007: 2.

List of subjects of federal contract(s) (for example, ship construction, aircraft parts manufacturing, software design, force structure consultant, architecture & engineering services, etc.):

Current fiscal year (2009): cyber-security;
Fiscal year 2008: cyber-security;
Fiscal year 2007: cyber-security.

Aggregate dollar value of federal contracts held:

Current fiscal year (2009): $1,323,373;
Fiscal year 2008: $861,387;
Fiscal year 2007: $2,703,263.

**Federal Grant Information:** If you or the entity you represent before the Committee on Armed Services has grants (including subgrants) with the federal government, please provide the following information:

Number of grants (including subgrants) with the federal government:

Current fiscal year (2009):_____;
Fiscal year 2008:_____;
Fiscal year 2007:_____.

Federal agencies with which federal grants are held:

Current fiscal year (2009):_____;
Fiscal year 2008:_____;
Fiscal year 2007:_____.

List of subjects of federal grants(s) (for example, materials research, sociological study, software design, etc.):

Current fiscal year (2009):_____;
Fiscal year 2008:_____;
Fiscal year 2007:_____.

Aggregate dollar value of federal grants held:

Current fiscal year (2009):_____;
Fiscal year 2008:_____;
Fiscal year 2007:_____.

**WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING**

THURSDAY, FEBRUARY 25, 2010

## RESPONSE TO QUESTION SUBMITTED BY MR. MARSHALL

Mr. BOND.

| | Federal Avg. Annual Wage (2008) | Private Sector Avg. Annual Wage (2008) | Wage Differential |
|---|---|---|---|
| Computer Systems Design and Related Services | **$53,355** | **$88,698** | **66%** |
| Engineering Services | **$76,732** | **$79,363** | **3%** |
| Research and Development in Physical, Engineering, and Life Sciences | **$89,732** | $**97,709** | **9%** |

Source: Bureau of Labor Statistics, QCEW Database.

**EDUCATION**

For-profit firms are the largest employer of individuals with science and engineering degrees.

- For-profit firms employ 47% of individuals whose highest degree is in science and engineering, compared to 13% employed by the government. (The rest are employed by colleges/universities, nonprofits, or are self-employed)
- For-profit firms employ 28% of individuals with science and engineering doctorates, compared to 9% employed by the government. (The largest employers here are 4 year colleges and universities which account for 42%.)

Source: National Science Board. 2010. *Science and Engineering Indicators 2010.* Arlington, VA: National Science Foundation. P. 3–24. [See page 13.]