

[H.A.S.C. No. 111-176]

**HARNESSING SMALL BUSINESS INNOVA-  
TION FOR NATIONAL SECURITY CYBER  
NEEDS**

---

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  
JULY 28, 2010



---

U.S. GOVERNMENT PRINTING OFFICE

58-232

WASHINGTON : 2010

SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND  
CAPABILITIES

LORETTA SANCHEZ, California, *Chairwoman*

ADAM SMITH, Washington	JEFF MILLER, Florida
MIKE McINTYRE, North Carolina	FRANK A. LoBIONDO, New Jersey
ROBERT ANDREWS, New Jersey	JOHN KLINE, Minnesota
JAMES R. LANGEVIN, Rhode Island	K. MICHAEL CONAWAY, Texas
JIM COOPER, Tennessee	THOMAS J. ROONEY, Florida
JIM MARSHALL, Georgia	MAC THORNBERRY, Texas
BRAD ELLSWORTH, Indiana	CHARLES K. DJOU, Hawaii
BOBBY BRIGHT, Alabama	
SCOTT MURPHY, New York	

KEVIN GATES, *Professional Staff Member*

ALEX KUGAJEVSKY, *Professional Staff Member*

JEFF CULLEN, *Staff Assistant*

# CONTENTS

## CHRONOLOGICAL LIST OF HEARINGS

2010

	Page
HEARING:	
Wednesday, July 28, 2010, Harnessing Small Business Innovation for National Security Cyber Needs .....	1
APPENDIX:	
Wednesday, July 28, 2010 .....	19

### WEDNESDAY, JULY 28, 2010

#### HARNESSING SMALL BUSINESS INNOVATION FOR NATIONAL SECURITY CYBER NEEDS

##### STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

Miller, Hon. Jeff, a Representative from Florida, Ranking Member, Subcommittee on Terrorism, Unconventional Threats and Capabilities .....	2
Sanchez, Hon. Loretta, a Representative from California, Chairwoman, Subcommittee on Terrorism, Unconventional Threats and Capabilities .....	1

##### WITNESSES

Lee, Richard P., Consultant .....	6
Ricketson, John H., Chief Executive Officer, Dejavu Technologies, Inc. ....	3
Thornton, Roger, Founder and Chief Technology Officer, Fortify Software .....	4

##### APPENDIX

###### PREPARED STATEMENTS:

Lee, Richard P. ....	46
Miller, Hon. Jeff .....	25
Ricketson, John H. ....	27
Sanchez, Hon. Loretta .....	23
Thornton, Roger .....	34

###### DOCUMENTS SUBMITTED FOR THE RECORD:

[There were no Documents submitted.]

###### WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING:

[There were no Questions submitted during the hearing.]

###### QUESTIONS SUBMITTED BY MEMBERS POST HEARING:

[There were no Questions submitted post hearing.]



**HARNESSING SMALL BUSINESS INNOVATION FOR  
NATIONAL SECURITY CYBER NEEDS**

---

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON ARMED SERVICES,  
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL  
THREATS AND CAPABILITIES,  
*Washington, DC, Wednesday, July 28, 2010.*

The subcommittee met, pursuant to call, at 2:03 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. The Subcommittee on Terrorism, Unconventional Threats and Capabilities will come to order.

Good afternoon. I would like to thank everybody for coming today, welcome you all for being before us on a very important topic today.

As Congress looks to develop its comprehensive approach to cybersecurity, we will need the perspective of many people, including our private sector and especially, I believe, our small businesses. Because, when you think about it, I think over 90 percent of the businesses in our Nation are considered small- and medium-sized businesses; and everybody, we hope, is using a computer for efficiency and effectiveness these days. And so it is important because you have a large majority of the people who work in our United States under you all.

I am particularly excited about today's hearing because we do have small business representatives in front of us, and that is sometimes unusual for the Armed Services Committee. So we are really thrilled about that. One of the things we do know about our small businesses is that you are very capable of innovating much quicker than large businesses or even government. And if you have innovation, if a lot of the innovation and technology agenda is driven by small business, then that is actually one of those areas that we really do want to protect from people stealing our information or your information, as the case may be.

So, today, the subcommittee is looking to discuss three main objectives for this hearing: One, the small business's view of the cyber challenge facing all of us today; secondly, the technologies that your business, along with others, are pursuing to address those needs; and the third thing is to identify systemic barriers to small businesses as they are entering the marketplace.

The purpose is for the members of this subcommittee to further develop greater cyberspace expertise and awareness but also for us to have an open discussion of how Congress can address certain barriers to small businesses while those small businesses are trying to help us here in the government sector.

And as our country works hard to improve our economy, the first place to take off will be small business. So in order to expand our economy, to grow it as so many of us I think pray every night right now, you really are key to getting that done.

So, today, we hope that the witnesses will provide the subcommittee with a technical look at cybersecurity and what technology and resources are currently available to further protect the systems that small business actually plug into at the Department of Defense [DOD]. That would be another area where we are looking for tools and the hindrances or the things that you might suggest.

So, today, we have three witnesses before us. The first, we have Mr. John Ricketson; and he is the Chief Executive Officer of Dejavu Technologies, Incorporated. So, welcome, and I do believe you are from California, right?

Mr. RICKETSON. Massachusetts.

Ms. SANCHEZ. Massachusetts. What did my people do?

And Mr. Roger Thornton, the Founder and Chief Technology Officer of Fortify Software. I know he is a Californian.

And Mr. Richard Lee, an independent consultant who just came out of the government sector.

So I hope you all will talk a little bit to us about the interface; and, once again, I look forward to your testimony. Without objection, we have put your written testimony into the official record.

I will remind the witnesses that you have 5 minutes to address. You don't have to read your statement. You can talk about the main points or anything you might have thought, oh, gosh, I should have put that in there and I forgot. And, after that, we will ask a series of questions and hopefully you can answer them.

And I will now yield to the ranking member from Florida, Mr. Miller, for his opening statement.

[The prepared statement of Ms. Sanchez can be found in the Appendix on page 23.]

**STATEMENT OF HON. JEFF MILLER, A REPRESENTATIVE FROM FLORIDA, RANKING MEMBER, SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES**

Mr. MILLER. I thank my good friend for yielding.

Thank you, gentlemen, for being here. I hope you have at least been to Florida, if you are not from Florida. You might have traveled there once or twice.

This hearing does come at an appropriate moment, because over the last several weeks General Alexander has in fact been conducting an aggressive road show explaining his vision for the U.S. Cyber Command, and the establishment of the Command follows the 2010 QDR [Quadrennial Defense Review] recommendations that centralized those operations. As the Department implements its vision and as the Command becomes fully operational this com-

ing October, the Department has an opportunity to renew its relationship with the industry and small business in particular.

Given the vital role played by small businesses and the community to develop innovative solutions to the challenges that we all see today, it is critical that both Congress and DOD have a thorough understanding of small businesses' view of the cyber challenges facing our Nation and eliminate those obstacles, as my good friend has already talked about, that many small businesses face when they contract with the Department of Defense.

I do know that our time is limited. We do have a vote coming up in a little while. So I would like to ask that my full statement be entered into the record. And I yield back.

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

Ms. SANCHEZ. Wonderful. I thank the ranking member of the committee.

Now let us start with Mr. Ricketson for 5 minutes or less.

**STATEMENT OF JOHN H. RICKETSON, CHIEF EXECUTIVE  
OFFICER, DEJAVU TECHNOLOGIES, INC.**

Mr. RICKETSON. Well, thank you for inviting me.

My name is John Ricketson. For the last 2 years, I have been managing Dejavu Technologies, which is a software provider of network forensic analysis tools. In my 30-year career in high technology, I have been associated with small companies for my entire career and about 40 transactions, equity-related, of small companies.

Our management team is made up of serial entrepreneurs. We have four prior ventures, all successfully executed. This one is our first primarily focused on government. So we have had a fairly steep learning curve.

I thought what I would do with the brief statement is start with the conclusion, which is we would strongly encourage small business policies to do a bit more towards encouraging innovation; and our view is that cybersecurity in particular is an area where the more ideas, the better. It is an arms race. Better defenses on more creative attacks and the more we can bring new ideas in, the better.

I thought I would explain what we do just from the perspective of the core innovative idea that we have to present which has to do with, in the cybersecurity application, managing what might be, in a military metaphor, might be damage assessments.

There is an infrastructure of many tools that are designed to block and prevent, but the fact is that breaches happen. They are inevitable. So we are helping with the process of discerning what happened, what machines were affected, what can be done about it in the future.

The essence of our product is to search in a Google-like fashion everything that has happened for what may be going on that you don't know at the time it was captured. So it is a fairly simple idea, but it has big implications in terms of scale and features that make an analyst effective at that process.

The principal challenge that we have with our big idea is how to find the sponsors within agencies for whom this would be helpful

with their mission. It is harder to do that than one might think as a small company.

So, in general, the small business policies have many noble goals: furthering economic development and job creation certainly, providing opportunities for groups that would not have those opportunities otherwise. It is more—it is easier to find those in the small-business-oriented programs than it is to find the programs that would help make more efficient the process of introducing new ideas and innovations.

I guess there are a couple of anecdotes I referred to in my report which is I went to the local Small Business Administration [SBA] who have a number of programs, none of which really applied to our particular challenge.

I guess another anecdote is not much of an anecdote. There was a lot of newspaper headlines about stimulus money, but we were unsuccessful at finding any.

But, in general, there is a few hindrances to small businesses presenting their ideas, one of which would be software certification which is an important requirement generally unique to each agency and there is a fairly steep investment for a small company to provide.

Another hindrance in general is security clearances. Again, very important, particularly in the area that we focused. But that requires a sponsor. So there is a bit of a Catch 22. When you introduce a new idea, to try to find the right people who can bring your idea forward and into the realm where it can be fully discussed.

We had experiences with the outreach and small business programs at various agencies, which actually did their job fairly well, which is to provide a mechanism for small companies like us to register ourselves so that we are known. I think that some attention to those programs is well deserved in terms of funding and expansion, because the goal would be for our good ideas to find the right people and agencies who would care.

Another type of organization we encountered was the technical intermediary, generally designed to represent the government to do technical assessment. And that is another area that would be very helpful.

Again, the goal is new idea, find the right application that can really help the mission.

So, in conclusion, I am trying to encourage the idea of a marketplace of ideas and smaller amounts of money distributed more broadly to bring those ideas forward and an information flow that is fair and can give every good new idea a chance.

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

Ms. SANCHEZ. Thank you, Mr. Ricketson.

Now we will hear from Mr. Thornton for 5 minutes or less.

**STATEMENT OF ROGER THORNTON, FOUNDER AND CHIEF  
TECHNOLOGY OFFICER, FORTIFY SOFTWARE**

Mr. THORNTON. Thank you very much, Chairwoman Sanchez, Ranking Member Miller.

I have prepared a short statement to accompany my written testimony today.

I currently serve as the Chief Technology Officer at Fortify Software. I have worked in the information technology [IT] industry in the Silicon Valley for the past 23 years.

My technical expertise is in finding and fixing and preventing software vulnerabilities that are at the very core of our cybersecurity dilemma. My current responsibilities involve the development and design of technologies that eliminate these vulnerabilities in order to make IT systems more resilient to attack, making software “hacker-proof.”

Fortify is a small company. It is a classic Silicon Valley startup. It was founded by myself and my three cofounders in the spring of 2003. Our customers include 8 of the 10 largest banks in the world, all the major branches of the U.S. military, and a majority of the telecommunication firms across the U.S. and Europe.

Through the course of my work, I am familiar with the types of vulnerabilities found in our Nation’s most critical infrastructure; and I can tell you with emphatic certainty we are in a desperate situation. My firm’s technologies have helped conduct audits on thousands of critical IT systems and not once have we found a system without critical vulnerabilities. Typically, we find thousands of such vulnerabilities.

One example set comes from a Fortify team that conducts audits and reviews of military systems. Over the course of 2 years, that team has audited 601 applications across 141 major programs and found over 3.8 million security vulnerabilities, over 400,000 of which were deemed critical. Sadly, this is not an exception but has become the norm, as it represents a problem that is not currently receiving appropriate attention.

There are two compelling reasons for you to consider and actively support the role that small businesses like mine have to play in solving cybersecurity issues.

The first is economic. As Chairwoman Sanchez has noted, small businesses have historically been an incredibly important driver for job growth in our country, and cybersecurity is no exception to that rule.

The second is innovation. Only a small company would have the audacity and impetus to challenge the status quo and offer an entirely new approach when there are entrenched solutions in place. Like many small businesses, my company was founded on a simple observation that challenged conventional wisdom and led to innovation.

Our observations were this. I will share them with you today.

IT systems are compromised of network, computers, and software running on those computers. The prevailing strategy for IT up to now has been to secure the networks by limiting access and attempting to block attacks. That traditional security strategy has failed us. It is outdated. It is fundamentally flawed. Simply put, nearly all software delivered today, including that which the Defense Department is going to use and all the critical infrastructure, will be constructed with major vulnerabilities.

Consider those vulnerabilities as open doors for hackers to gain access to systems. Our adversaries have shifted their approach to leverage those open doors in software at the same time we have re-

sponded with more network security. The results speak for themselves.

If we eradicate software vulnerability, then the attacks won't work. We can build software systems to be resilient to attack. This is very similar to the practice of building buildings that are resilient to fire, but we need to do a better job.

This line of thinking represented a radical departure from the status quo, and in the Silicon Valley that means a new small business determined to solve an old problem in a new way. In spite of the strides we have made at Fortify and other small innovative firms, there are some extraordinary challenges that the status quo pose that I would ask for your support in overcoming.

The first is a disproportionate focus on protecting hardware networks while the majority of the attacks are at the software layer; second, lack of clear policy relating to software security that leads to vague software security requirements and inadequate funding for software security initiatives; and the third is inadequate funding for fixing the vulnerabilities that companies like mine and others are finding every day.

We have a strong conviction and have established high confidence that the right combination of technology, human capital, and process can confront the advanced persistent threat and ultimately protect us from cyber warfare. We look to Congress to establish a strategic policy guidance for cyber, and we applaud Congress for being so active. This inspires mature companies, mature small companies like Fortify, and also gives hope to the next generation of innovators.

In conclusion, please let me compliment this subcommittee for your cybersecurity leadership. In particular, we strongly support the certification and the accreditation language included in the House-passed 2011 NDAA [National Defense Authorization Act]. Combined with the language contained in Section 932 of the Senate companion bill, these provisions are sorely needed to protect the United States in the domain of cybersecurity.

I would like to personally thank Chairwoman Sanchez, Ranking Member Miller, and the members of the subcommittee for holding the hearing. We look forward to working with you and the talented House Armed Services Committee staff to help better strengthen our Nation's cybersecurity defense through effective software security. Thank you.

[The prepared statement of Mr. Thornton can be found in the Appendix on page 34.]

Ms. SANCHEZ. Thank you, Mr. Thornton.

Now we will hear from Mr. Lee for 5 minutes or less.

#### **STATEMENT OF RICHARD P. LEE, CONSULTANT**

Mr. LEE. Well, thank you, Congresswoman Sanchez. I appreciate the opportunity to address the subcommittee.

I believe that we have got—as you commented; I am an independent consultant previously working inside the Federal sector as an acquisition professional and am now in the small business sector attempting to assist others to understand how to bring their products to market.

I believe we have to deal with the intersecting demands of the need to share information, whether it is in the commercial sector or in the Defense Department or government sector, and the need to protect that information, the three pillars of information assurance: the confidentiality, the integrity, and the availability.

Our economy has become very dependent on the Internet. We are not going to be able to abandon that battle space but must be able to work through attacks on our Internet connectivity.

Almost all of the things that we do on a daily basis, from personal banking to managing the logistics trail to get things into the warfighting theaters, for example, depend on Internet connectivity.

I also understand that the subcommittee's focus is on harnessing the passion and innovation and originality and resourcefulness of American know-how. One of the things that I believe that my colleagues have mentioned is that we failed to take a holistic systems engineering approach to the problem and instead look at component piece part fixes that don't seem to ever solve the big problems. The issue of a Maginot line as a wall of defense is not going to work. It never has, and it won't work in the cyber domain, either. And we need to find solutions from a systems engineering perspective to harness that innovation.

I believe there are three fundamental things that are causing difficulty for small businesses to get into the solution space: The first is the acquisition process itself, which I will address a little bit later. The second is the evaluation and the certification process that we go through in order to bring products and solutions into the cyber domain. And, finally, are the financial resources available to the small business sector in just being able to get their products to market.

With respect to the acquisition process, I think that one of the issues we have and continue to have is that there are a number of large integrators who understand the acquisition process and can navigate it. Because of that, it is difficult to get innovation into their tool kit; and, consequently, when we are solving a problem, identifying and resolving a vulnerability, we seem to fall back on the same guys that got us here.

If you recall Albert Einstein's comment, no problem can be solved from the same level of consciousness that created it and, thus, I believe your effort to harness small business innovation in this vital area.

The evaluation and certification process is king in the governmental cyberspace domain. There is a whole army of people who can say no, very few people who can say yes when you want to insert technology into our environment. Most small businesses do not have the resources to navigate the certification process to be able to get their products into the domain to provide either vulnerability fixes or completely new and innovative ways to approach a cyber issue.

And, finally, the ability to get into the cyber domain to identify the resources necessary requires a champion on the inside of government pulling that solution into the cyberspace.

I believe that there are some programs in the executive departments and in the Defense Department specifically that do a good job of identifying and incubating innovative solutions. The Defense

Advanced Research Project Agency [DARPA] has a number of programs, as does Defense Research and Engineering specifically on their ability to do the Defense Acquisition Challenge and their Joint Capability Technology Demonstrations. But, as always, transition into sustainment is the difficult part.

As you noted, Congresswoman Sanchez, my remarks are in the record. So I will conclude there and await your questions. Thank you for the opportunity to address you.

[The prepared statement of Mr. Lee can be found in the Appendix on page 46.]

Ms. SANCHEZ. Thank you very much, Mr. Lee.

I will remind members that—well, I will let you know that each of the members has up to 5 minutes to ask their questions. We will start with those who arrived to the committee prior to the gavel closing, and so I will begin by asking my questions of the panel.

This morning, I met with Zachary Lemnios—he is the Director of Defense Research and Engineering [DDR&E]—in order to discuss this very topic of cybersecurity, and one of the main issues that was brought up was how we get the technical base right. I think that that is one of the crucial questions that we have for DARPA and for DDR&E working on that answer of what are the technical underpinnings to build a secure system. I know they are working with universities and with the private sector to try to answer that question. So I guess I would like to start by asking our witnesses here today what do you think are some of the technical underpinnings to build a secure system?

And anybody can take a stab at it. None of you can take a stab at it. I know it is a “why are we alive” question, but it is one that we are struggling with.

Mr. THORNTON. Chairwoman Sanchez, I would be happy to give some comment on that.

The gentleman you had a conversation with was definitely right on focusing on that. You can think about the resiliency of a system, and let us use this room to say its resiliency to not catch on fire. If we only focused on the fabric, let us say, and we knew the fabric was fireproof, what about the wood tables? What about the articles we bring in? What about the sprinkler systems and what have you?

Cybersecurity today is fragmented into those that worry about access to the networks, those that worry about access to the computers, and my area of expertise, those that worry about the software programs themselves. And our adversary is not. They will look at our systems, they will look at all those components, they will look at the human interaction, find the weakest point and attack.

So one of the things that has escaped us is in our systems engineering, the people that are ultimately responsible for an inventory management system for the military or a financial accounting system, is having those people with the purview of the entire system be the ones responsible for security. They still may need experts to help them, but we need to push the responsibility of security up the system to the senior-most people. That means a change in the thinking of education, what is the educational requirement to be a system designer, a change in roles and responsibilities—

Ms. SANCHEZ. Are you talking from a hardware or software or both standpoint?

Mr. THORNTON. Both, both. So the key is every system has—in information technology world, we call them system architects—people whose responsibility purviews across all the technical components, ensuring that security responsibility is held at that level.

Ms. SANCHEZ. Great.

Anybody else? Mr. Lee.

Mr. LEE. Yes, ma'am.

To pick up on the comments about systems engineering, one of the things that we don't do a good job of is recognizing that when we approach the certification of networks or the software that operates those networks, the computers and the software that runs on them, the evaluation process desires the use of standards which are good in and of themselves because they provide a bound for the evaluation process.

Unfortunately, most of the standards that we rely on were built when the Internet was being evolved and were conceived in an academic environment where trust sort of existed between the colleagues. But as we have gone into a cyber world we can no longer trust the users, and sometimes we can't even trust each other.

So we need to perhaps take a step back and figure out are there some inherent vulnerabilities and standards that we use in architecting our systems that will perpetuate vulnerabilities that we just can't solve. If that is the case, we need to take a look at, from a system's perspective, what we might do to change that environment; and I believe that is where small business innovation fits right into the sweet spot of that solution space.

Ms. SANCHEZ. Thank you, Mr. Lee.

Mr. Ricketson, would you like to comment or—

Mr. RICKETSON. Yes, I would.

I guess my comment is maybe to challenge the underlying assumption of the question. I am skeptical that we could find what you referred to, technical underpinnings. I think the history of the Internet shows that all of the hierarchically driven networks fell by the wayside, and the Internet, with all of its decentralization and messiness, was the best solution.

So I am skeptical of vendors that would promote their underlying technical solution, and I am skeptical of an organized body that would decide to pick winners. I think that we have an Internet that is decentralized, and we need to work on the issues of trust and monitoring and statistical analysis and stay on top of it.

Ms. SANCHEZ. I, too, had that question this morning. I am a little bit more—after having spoken to both the DARPA Director and to Zachary this morning, I think they are going both ways. I think they are doing a double track to ensure that maybe there are, and maybe they are not. So that is a keen observation that you have just made. But I think they are looking at it from both standpoints: Is there a better way or is the Internet, with all its failings, the way we are going to go?

Mr. Miller, my ranking member, please, 5 minutes.

Mr. MILLER. I would like to—and I will keep it brief—talk a little bit about the impediments.

Mr. Ricketson, you talked about it as far as your visit to your local SBA office. SBA, small business initiative research programs, technology transition programs have all been successful for small businesses. I mean, it has been proven so.

You talked about some specific instances with the others. You didn't really go into great detail. But what I would like to know is, have you used them in the past? Did you see the same thing Mr. Ricketson saw when you tried to avail yourself of some of the programs that were there? And what changes would you recommend to allow for greater participation of companies like yours in the software field?

So if I could start with Mr. Lee and then work back to Mr. Ricketson, I would appreciate it.

Mr. LEE. Yes, sir, Mr. Miller.

So to go right to your question, I think one of the advantages that the Defense Department may have is to follow the lead of DARPA that they did with their challenge program where they put a problem out there and bring—or ask people to bring solutions to them in competition for an award. That certainly exposes innovation and innovative technologies for use.

And from a prior government-side person, the two questions one always had to ask a contractor with a great solution was, A, how much is it going to cost and how do I get to you? What is the contract vehicle?

The contracting process is so cumbersome that it is very difficult to get innovation inserted into our existing systems. We can do pilots, and we can do cultivation and incubation, but the transition into the environment is very difficult.

Many of the innovators like Apple and their iPhone go to the commercial marketplace because they can get out there quickly. They have to identify their certification implementation process.

The government is an extraordinarily difficult labyrinth to navigate for the small businessman, and he necessarily has to get married up with a big innovator who has different motivations sometimes than the insertion of technology.

So I think there is a challenge in how you weigh, on one hand, open competition kinds of activities and the other is the insertion of new and innovative technology to solve the problems that we have. The programs exist. It is in the transition into the environment that it seems to be just so difficult to solve.

Mr. THORNTON. Congressman Miller, I would answer your question in thinking about two different ways that the government helps make streamline working with small businesses. One, driving requirements that require innovation, thereby giving the small business an equal footing on the playing field. And I would like to come back to that, because the other is more directly what you were asking, which is the programs that are in place for small businesses like ours to work with the government.

I have been to a lot of seminars and sessions where small businesses complain that it is difficult to access the government and what have you. And I wouldn't sit here and say it is easy, but, in my experience, it is not all that harder than the banking industry or the manufacturing industry in that the government demands

that you understand their environment, that you understand their processes, that you understand how they do work.

So I think part of it is a little bit of level setting the education or what does it take to work with the government. The programs were there for us, but we—our very first revenue as a company came through an SBIR [Small Business Innovation Research] program with the U.S. Air Force, and neither myself nor any of my founders had any connection with the Air Force. We simply worked our way through the system and found that. The National Security Agency has been very helpful, sponsored our company for the right clearances that we need.

So I do think programs that are in place, from what I understand and from talking to other entrepreneurs, there could be more education. My counsel to those other entrepreneurs is, if you want to work with the government and sell to the government, you are going to need to hire people that work in that arena, just like we have hired people that have worked in the banking arena and can help us navigate.

If I could finish on my first point, though. When requirements that the status quo are not good enough are fed from the government to the IT industry, that gives the small innovator a giant advantage. So, from my vantage point, that is, security of just my network, it is not good enough. I need security of my software. But there is opportunities for that in just about every realm of cybersecurity. Demand more or better than what is currently being offered by the status quo.

Mr. RICKETSON. Nothing much more to add than what I had said. I think my modest proposal is to simply bring the criteria “does it help innovation” into the small business programs. Every program that I mentioned there was—it was a worthy program. So I am not knocking any of those. But we just need to do more. Thank you.

Ms. SANCHEZ. Thank you, Mr. Miller. Thank you, gentlemen.

I will now call on my good friend, Mr. Smith, from the State of Washington for his questions.

Mr. SMITH. Thank you, and I appreciate the chairwoman holding this hearing. It is a critical issue for our subcommittee.

I think that for the government to get small business more involved the best ideas are out there I believe in the small business community, in many instances; and, as all of you have mentioned, it oftentimes is impossible for them to do business with the government and we in the government lose out, particularly on this subcommittee that works on IT infrastructure. But this expands out. We do a lot of work with the Special Operations Command. A lot of their needs requires updated better technology, and small businesses are the companies that can provide it. So we appreciate that.

I think most of the questions have been answered. I will just throw this out there, if you gentlemen have anything to say about it in particular. What is the one thing you would say we could change about our acquisition or procurement policy that would most help small businesses get greater access, have the opportunity to be able to sell what they make or their services to government, in this case the DOD?

Mr. LEE. Sir, I would like to take a cut at that.

I think that because we in the acquisition process tend to wind up with the big integration companies that have deep pockets that can navigate the bidding process system and know how to write a proposal that a government evaluator can read, understand, and accept, we tend to get the sameness of the solution competing on price.

One of the things that might help is if there were some tax code incentives or other kinds of things where some of the debt and/or operating loss that a small business necessarily incurs while they are trying to do this innovative thing and get their product to market could be used somehow by the large integrator to help offset some of his financial activity. He may be incentivized to try to bring in some of the new innovative or novel ways to solve some of these cyber problems.

Some of the people that I have worked with have taken a systems engineering perspective and have a new way of looking at the networking architecture to be able to insert distributed defense-in-depth kinds of activities, firewalls, for example, instead of building it at the boundary like the Maginot line. But that technology is extraordinarily difficult to stick into the system because the large integrators are unfamiliar with it and just don't have a way.

Mr. SMITH. Shouldn't there be a way to do this without the large integrators, in some instances? I guess that is—we have small businesses come to us all the time; and, regrettably, one of the first things we have to tell them is here is the eight biggest defense companies; find one and partner with them. But shouldn't there be a way that a small business can simply do it without having to go to a large integrator?

Mr. LEE. Sir, one of the problems from my perspective is that the evaluation and certification process has so many people demanding "certify me" because it is great to have that certification label on your product. And, in some cases, particularly for government networks and environments, you need that evaluated product certification in order to even be considered. If you don't have the champion inside the government pulling on your solution, then you need that integrator to be pushing you into the environment as part of a systems approach that he has recommended or has been hired to implement.

Mr. SMITH. What I would like to do—and it is something we have worked on a lot with different companies—is get the acquisition people out there to be looking for you guys. Instead of seeing one of you guys coming and going, they don't know what they are doing, better call somebody bigger, they say, I am going to take a closer look.

So I think, from our perspective, we need—and this has particular application on the cybersecurity side. Because, as you gentlemen have noted, you are cutting-edge innovators on that, in many instances, but we need acquisition people who can move past that.

I accept your answer. I am running out of time. I don't know if the other two gentlemen wanted to comment at all on how you would change the process.

Mr. RICKETSON. My big idea may not actually be a good idea. I would love to have someone validate it. So my idea—I make a tech-

nical claim. That technical claim may or may not be valid. Even if it is valid, it may or may not forward the mission.

So I will give you an example. We have a search capability that is supposed to scale. That means you can search into huge amounts of data. The word “petabyte” comes up. The petabyte is bigger than I can count, and products break down in situations of stress like that.

So if there is a technical intermediary that represents the government that can take a claim and say, yes, this is true and has the credibility inside the government with the technical sponsors, that is a major step forward and is independent and is a level playing field between a big and small company. It is just about the idea.

Mr. THORNTON. And, Congressman Smith, if I can add—and I will caveat with I am not an expert in Federal acquisition. So this is an idea from a person who—

Mr. SMITH. That may be helpful, actually, that you are not buried in the minutia of Federal acquisition and can simply look at it from a practical standpoint. But go ahead.

Mr. THORNTON [continuing]. That is what I was thinking, is when I—in my experience, I have seen the Federal Government make some really smart acquisitions and other times where I questioned it, whether it was the best technical solution. One thing I noticed was the technical capability to define the requirements were employees of the Federal Government. I can give some examples. But, in general, when the system integrator is writing the requirements for the Federal Government, I think a lot of times those requirements are going to be not demanding the highest, latest innovations.

So maybe a radical shift in theory but building up the capabilities inside of each of the agencies to have some top-of-field technical people that can drive requirements, from personal experience I have seen that work quite well.

Mr. SMITH. That makes a great deal of sense.

I think two directions we need to go in to get there. We have talked about this in a number of contexts, but our somewhat obsessive reliance or I should say excessive reliance on contractors since 9/11 has downgraded the number of people within the acquisition process who are talented and knowledgeable. There just aren’t as many of them there, for one thing.

But the second thing I always want to emphasize is to empower those people. I think part of what drives some people out who do have experience in the acquisition process is, if you are the type of go-getter, really knowledgeable, you are a person who wants to be empowered, you want to know if you make a smart decision you can implement it and see the result of it.

If you are in the acquisition process and you can’t make the decision and say, you know what, this company or—to your idea—this guy has this idea and you know what, it works, it is great, it is what we are going to do, but I cannot do it because there is an 18-month procurement process and it doesn’t fit the RFP [Request for Proposal] that was written sometimes 2 years ago. It doesn’t really fit that RFP. So I would have to go back in, I would have to change the RFP, I would have to go through another 12 months, and then

I come back to you and you go I don't remember who you are because it has been so long. So I think we need to empower people within the acquisition process.

Thank you, Madam Chairwoman.

Ms. SANCHEZ. I like the observations you made, Mr. Smith.

And, of course, the other problem is, at a time when we have such a calling on the government to stop making government bigger and having this push to somehow—it is difficult, because we are dealing with very complex issues. We are dealing with people who get paid a lot of money. Everybody who is worth their salt in your industry is making money, and then we want them to come and work for the Federal Government. So that—

Mr. SMITH. If I could just comment. It is not a matter of making the government bigger. It is a matter of making it better. And we are paying the contractors. We are paying for those RFPs. We are paying for this acquisition process, which in many cases just winds up costing more. So I think you can accomplish both.

Ms. SANCHEZ [continuing]. Well, we always try to do that, and I think that is part of what we did in the slimmed-down acquisition programs that we are putting in place led by Mr. Andrews. But there is always that overlap time where we are trying to get out of one system and really make the other system work, and it is a difficulty. So I would agree with you. It is just difficult how we get to that.

Mr. Ricketson, you said at one point in your testimony that we should encourage small business policy, that we should change small business policy or make small business policy to encourage innovation. If you were a Congressperson sitting up here and you wanted to change small business policy of the government to encourage innovation, how would you go about that? What would you propose would be—

We have already got our small business innovation programs. We have pilot programs. We have got Mr. Lee saying, well, you know, the problem really isn't that you are not encouraging innovation in small business. By having some of these programs is when you get to a point these programs, that falls off—when we tell you, okay, here, we are going to throw you out of the nest and go fly, there is nobody to help you figure out how to fly as you spiral downwards into never-never land.

So what would you say? If you were a Congressperson, when you say change small business policy or mold small business policy to encourage innovation, what would that look like? Because we also have R&D [Research and Development] tax write-offs, for example. What would be—from your angle, what does that mean to you?

Mr. RICKETSON. I am honored to be asked, though I come here from the perspective of our small company trying to move forward, seeing some hindrances, offering constructive suggestions about areas to focus on. Far be it from me to make a lot of specific proposals.

However, a comment you made a minute ago I wanted to respond to that I think is relevant. All of us—there is the challenge of big government versus—bigger government versus what we want government to do. And in the area of fostering innovation, small amounts of money at earlier stages yields much better returns than

large amounts of money that are deployed in mature programs. So I would encourage the government to provide for small businesses that have ideas that seem like they might be interesting, services that eliminate those companies having to come up with the money and take that risk themselves.

So a suggestion a moment ago, which is some technical claims are difficult to validate because they take an infrastructure that is beyond the small company to fully judge. And a technical claim goes beyond technology but also involves risk. Large companies, large integrators, complex procurement programs are, to some extent, a proxy for risk assessment. So if you can at least ask the organizations that are assigned to look after technology and small companies to bring innovation into their criteria and find ways to measure whether they are doing a good job, we are going in the right direction.

Ms. SANCHEZ. The problem for somebody who is working in the government—I am not talking about us, because we are taking risks all the time. We have 2-year jobs, and then we have to go out and campaign again—is that it seems to me within the Federal Government, from what I learned, is that somebody who goes with the known quantity, a Rockwell or a Raytheon or something, is never going to get in trouble if he suggested or gave the contractor somebody like that. Because when those guys mess up—and somewhere along a large project there are a lot of mess-ups. You have to look at some of the subcommittees I have had before to know all the failings that I have seen. Well, it couldn't be done. We are the biggest, we are the best, and it couldn't be done. Or we just—you scoped it wrong or the specs were wrong.

But if a government employee goes and gives it to a small, innovative company and you do fail, then it is like, well, didn't you know that was going to happen? Here is a company that has no track record or doesn't have the resources to cover the losses or look at all the time we have wasted.

So it is really—it is a very difficult thing when I look at these government employees to be able to really take that type of risk.

I would also say that is one of the reasons why we put DARPA in, because that is our risk taking, that is almost throw caution to the wind and go with bold ideas. It is almost a contrarian type of an agency.

So I don't know if we need more DARPAs or what we need in order to give government ability to feel comfortable working with so many of these new issues and what is really a risk to your environment by definition because it is new and a bad attack of cybersecurity can get to all of us at once.

Mr. Miller, do you have any other questions?

Mr. MILLER. Yeah. I would like to follow up on Mr. Smith's line of questioning in regards to insourcing.

I would say that in the First Congressional District it is of great concern not only to me but to some of my constituents because I believe that the standards used in determining which jobs are to be insourced don't really use any true methodology. I think that, in many cases, the numbers seem to be arbitrary.

But what I want to know and, Mr. Thornton, you had—when we were talking a minute ago, you were nodding your head. I couldn't

tell if it was in agreement or dissent. My question is, have any of your companies been affected by DOD's insourcing? And, if it has, could you explain and offer your guidance to the committee on what jobs could be insourced from your field?

So, Mr. Thornton, if you would; and then if the other two want to chime in, you can. If not, that is fine, too.

Mr. THORNTON. Thank you, Congressman Miller.

I cannot say specifically that we have been affected by insourcing on any particular instance, but I can give an example where the government had in its employ some very sharp technical people that were ultimately driving the architecture of a major purchase. And this was at the Veterans Administration [VA], some of the people that work for Mr. Baker there, very technically astute, as good as you are going to find in private industry and what have you. And when you have an environment like that, the government as a customer is being very clear in terms of its expectations of your technical performance.

I could cite some other examples where our company is working with a large integrator and the government employees are more program managers and financial folks and it is really the large integrator that is driving the technical requirements. And from my not expansive number of times I have seen that—I have only seen that a couple of times—it does make sense to me what Congressman Smith was saying. Were the government able to insource technical architecture, empowered individuals that can drive requirements, we will probably end up with more effective, cost-effective, more demanding requirements.

Now, what does that mean to small business? I believe in my heart of hearts more demanding requirements is an unfair advantage for small business. When you ask for something that is not currently being built today, more times than not it is a small business that is going to be able to meet that requirement than a large company.

And so one other way I might contrast that. My company does a lot of work with the Federal Government and a lot of work with the banking industry. As I mentioned with the VA, there were technical people in there that could easily work in the banking industry and drive the same requirements. Just about every bank we come into has technical people that manage the entire requirements process, set the bar for what is good enough, determine if the small business is making legitimate technical claims or not and really owns that. And as we talk here today—this is not an idea I came to bring to you, but as I listen to the discussion that does make a lot of sense to me—I think you would benefit from that.

Mr. LEE. Mr. Miller, I think one of the issues you have in trying to insource is—I am going to bet, looking at us, that my colleagues and I grew up shortly after Sputnik went up and the Mercury space program kicked off and the United States went nuts for science and math and engineering expertise and the kids that I was growing up with were focused on that.

The kids today are not as focused on that. We see our universities, particularly engineering schools, being more inundated by foreign students who take that expertise home. Those are the peo-

ple that you need, the young kids coming out of school that you need to figure out a way to incentivize into the government.

Unfortunately, there is a whole culture that seems to believe that a government job is, A, to serve the Nation but more, and as importantly, to generate a good pension coverage for when you get older. So the issue becomes, how do you incentivize those kids to come into the service, the government service to do the engineering work needed in order to make sure we are pulling the best out of the small business and getting it into our processes?

I don't know if you can think outside the box and say, well, let us have a project, maybe run by DARPA, maybe run by some other organization. I know the services all have good and vibrant laboratories that do innovative things. Perhaps you run a pilot effort for a 2-year initiative to suspend the FAR [Federal Acquisition Regulations] and the DFAR [Defense Federal Acquisition Regulations], write some letter contracts and see what we can do, as my colleagues have said. And if the technical expertise and the delivery is good and the government side can figure out that it is good and can understand how to specify that on a grander scale, you now are in a position that government has learned, industry has learned, and we got out from under the acquisition umbrella that just seems to impede the process, which seems to be where we constantly found ourselves stuck in the labyrinth.

Ms. SANCHEZ. Well, do you have any more questions, Mr. Miller?

Mr. MILLER. No.

Ms. SANCHEZ. Okay. We are going to have votes in a few minutes so we will conclude this, but I just wanted to make some observations.

I can't tell you how many times—and I live in Orange County, California, which is, as you know, an innovative—we carry the innovative agenda, as so many in California, and especially the defense, the aerospace, NASA [National Aeronautics and Space Administration]-driven issues, we have a lot of small companies that work in Orange County that have their people in Orange County, and there have been plenty of times I have seen where these small companies come to the Federal Government—they come to me and they say, we really have some ideas, and someone needs to hear these. You need to help us. Of course, we start banging on doors and stuff.

The reality is, it is very difficult. As you say, unless you have someone who has been in the Pentagon day in, day out, or contracting, it is a very difficult thing for a small business and they really can't afford tons of lobbyists and specialists and everything and to put them out there for a year or two.

As many of you know, the specs are written with, you know—because a technical aspect may not be within one of the government departments that is doing this, they rely a lot on industry coming in and talking to them about what those specs for those RFPs should be. That is a long process. It is usually a year, two, three years before you see the RFP; and it has been written by somebody who already, you know, knows it is coming out. And yet you have the small business who wants to compete. It is very difficult, and they can't afford to compete. That is the truth.

So we do need to find a new way in which we allow this innovation to get in here. Because I certainly see it out in the commercial area day in and day out where I live out there in California, and you don't see it here as much in Washington, DC.

So I would hope that if you do have, given that some of you have hit your head against that wall or been at companies or heard stories, that you might do us a favor of sitting down and writing specifics about what we might change, what we might really try to change in order for these innovative ideas to get a fair shake out here in Washington, DC. That is what this subcommittee is about, at least with respect to the Department of Defense.

I want to thank all of you for being here today. We really appreciated your testimony, and I would appreciate any follow-up that you might have to this issue that I just laid out.

Thank you very much. The subcommittee is now adjourned.

[Whereupon, at 3:05 p.m., the subcommittee was adjourned.]

---

---

**A P P E N D I X**

JULY 28, 2010

---

---



---

---

**PREPARED STATEMENTS SUBMITTED FOR THE RECORD**

JULY 28, 2010

---

---



*The Honorable Loretta Sanchez  
Committee on Armed Services  
Subcommittee on Terrorism and Unconventional Threats and Capabilities  
"Harnessing Small Business Innovation for National Security Cyber Needs"  
July 28, 2010*

**Opening Statement**

Good Afternoon,

I would like to welcome you all and thank you for joining us here today.

As Congress looks to develop a comprehensive approach to cybersecurity we will need the perspectives of our private sector, especially our small businesses.

I am particularly excited about today's hearing as we were able to bring in small business representatives to discuss their views and gain their inputs to better securing our information systems.

Their ability to innovate and create new technologies will be vital in order to successfully protect our information systems.

Today, the Subcommittee is looking to discuss three main objectives for this hearing:

1. The small business' view of the cyber challenges facing us today.
2. The technologies your businesses along with others are pursuing to address these needs
3. And to also identify systemic barriers for small businesses entering this marketplace.

The purpose of this hearing is for Members of this Subcommittee to further develop greater cyberspace expertise and awareness but to also have an open discussion of how Congress can address certain barriers small businesses face while trying to work with the government.

As our country works hard to improve our economy, I believe expanding opportunities for our small businesses is imperative.

Small businesses are a vital component of our economy and the leaders of innovation.

For example, small businesses represent 99.7 percent of all employer firms, and employ half of all private sector employees.

Small businesses have also generated 60 to 80 percent of net new jobs annually over the last decade.

That truly makes American small businesses the engine of innovation for the nation.

As this country responds to and develops ways to face the growing challenges of cyber operations, small businesses will play a critical role in the technologies that are implemented.

That means that Congress needs to have a better understanding of the role small business will play in our national response to cyber threats, including the potential implications for new and proposed legislation and policies.

In addition to understanding challenges small businesses may face in working with the DoD, we also need to have a better understanding of the tools available to us for promoting small business research and development, such as the Small Business Innovative Research program.

I hope the witnesses will provide the subcommittee with a technical look at cybersecurity and what technology and resources are currently available to further protect our DoD systems.

Today, we have three witnesses before us:

- First, we have Mr. John Ricketson. Mr. Ricketson is the Chief Executive Officer of Dejavu Technologies, Inc
- Mr. Roger Thornton, the Founder and Chief Technology Officer of Fortify Software.
- And Mr. Richard Lee, an independent consultant who just came out of the government sector.

Once again I would like to thank all of our witnesses for being here today and I look forward to hearing your testimonies.

Without objection, we will accept your written statements as part of the official record. I'd also like to remind the witnesses that we'd like for you to briefly sum up your statements, and we will be observing the 5 minute rule for questions from the members.

I will now yield to the Ranking Member from Florida, Mr. Miller for his opening statement.  
Thank you

**Mr. Miller Opening Statement for Hearing on the Administration's Counter-Proliferation  
Policies and Programs**

**July 28, 2010**

"This hearing comes at a very appropriate moment. Over the past several weeks, General Keith Alexander has been conducting an aggressive road show explaining his vision for U.S. Cyber Command. The establishment of the command follows the 2010 Quadrennial Defense Review's (QDR) recommendation to centralize command of cyberspace operations. As the Department implements this vision and as the command becomes fully operational in October, the Department has an opportunity to renew its relationship with industry and small businesses in particular. Given the vital role played by the small business community to develop innovative solutions to today's challenges, it is critical that both Congress and the Department of Defense have a thorough understanding of small business' view of the cyber challenges facing the nation and eliminate any obstacles small businesses may face in doing contracting with DoD.

"More and more, we are seeing the expansive nature of cyber operations and the wide ranging impact that cyberspace has on our lives. From a national security perspective, almost all of our military's functions rely on cyber to some extent, and a disruption or intrusion could prove significant, if not catastrophic, to our nation's defense. The Department is constantly under attack. This fact is undeniable and will not change. In light of this unending threat, we must ensure the Department has the tools to stay ahead of the enemy in this cat and mouse game, a game that bears potentially deadly consequences.

"Undoubtedly, many of these tools will come from small business. As U.S. Cyber Command is stood up, it will be critical for the Department to develop a research and development strategy that leverages the existing expertise within the Department, industry, and especially small business, to ensure the Department has as robust a capability as possible in cyber operations. The investments made today help to position General Alexander and Cyber Command for success not only now, but into the future. Therefore, we are also very interested in the witnesses' perspectives on the technologies required to address both near and long-term threats.

"In fact, for the long-term well being of the Department and the function of U.S. Cyber Command, the Department must take steps to create a comprehensive approach to operations in cyberspace, as also recommended by the 2010 QDR. This will require the coordination and synchronization of all lines of activity that feed into cyber operations: selection of personnel; training and education; research and development of new technologies; and procurement of systems and services, to name just a few. Small business may have a role to play in these additional lines of operations, not simply research and development.

"Finally, small business can play a role that is often overlooked – that of facilitating interagency communication. Actions taken in cyberspace touch upon functions well beyond the

Defense Department's scope. But should a cyber attack on a nuclear reactor's control system or on the U.S. banking system be considered a threat to national security? I would argue that such actions should be considered within a national security framework and that the Department must therefore be working alongside the other government agencies to ensure that vulnerabilities to critical infrastructure are mitigated. Clearly, the federal government cannot delegate this responsibility to industry, but industry – including small business – is uniquely suited to spreading best practices and technology beyond the borders of the military, as the community interacts with other customers. In reducing barriers to contracting with the military and in supporting the commercialization of small business technologies, the Department of Defense should consider the secondary benefits that technology transition and commercialization may realize for a whole-of-government approach to cyber.

“Before us today, we have representatives from the small business cyber community to discuss these various matters. While other companies may face other challenges or prioritize them differently, these witnesses should provide the subcommittee with a sample of the issues facing small business, DoD, and the potential solutions that could further empower U.S. Cyber Command.

“Thank you to all of our witnesses today for joining us. I look forward to your testimony on this very important subject.”

**Witness Statement**

Offered on 28 July 2010 to the House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities (TUTC), for the hearing entitled, *Harnessing Small Businesses Innovation for National Security Cyber Needs*.

**Contributor:**

John H. Ricketson  
CEO, Dejavu Technologies, Inc.  
D'Angelo Drive, Marlborough, MA 01752  
508-281-2527  
jricketson@dejavutechnologies.com

**Personal CV**

For the last two years I have managed Dejavu Technologies, a start up software technology company focused on network forensic analysis for cyber security. For over 30 years I have worked in high technology. As a corporate buyer for Dynatech Corporation during the 1980s, and most recently as an independent consultant for 15 years prior to my current position, I have personally managed over 40 equity financial transactions involving small companies in industrial technology markets. I have a BSEE from Princeton University in Electrical Engineering and Computer Science, and an MBA from the Harvard Business School.

**Prior Entrepreneurship**

Dejavu's operating team and angel investor group have been serial entrepreneurs. Dejavu is the fourth sequential start-up technology company associated with this team. I was personally involved in the most recent two ventures. Each prior venture was successful, and sold to large technology product companies. These companies started as commercial customers and became strategic buyers, acquiring the product lines to include in their own portfolio. The prior ventures were as follows: ClearSpring Technologies (acquired by Veritas/Symantec), Synthetic Networks (acquired by Agilent), and Imperfect Networks (acquired by Spirent). Dejavu is our first venture that has been primarily focused on government markets, so we have experienced a steep learning curve.

**Cyber Security Technology**

The **TrafficScape** technology created by Dejavu is a comprehensive network forensic analysis tool. Simply stated, TrafficScape allows an analyst to "Google" network history looking for any clues to discern the nature of newly uncovered cyber threats, and to trace what damage might have been done, and what assets might be most vulnerable.

TrafficScape is a very innovative product in many ways. A key innovation is to capture and store network content utilizing search engine technology, rather than a traditional relational database. As a result, TrafficScape stores pre-analyzed free-form data that may be rapidly searched for any arbitrary item of interest, plus relationships among items. TrafficScape can scale to handle huge quantities of stored forensic data.

Another innovation is the *ePersona* feature, which uses search engine technology to rapidly recall cross-reference relationships. This is a productivity tool for cyber investigators.

TrafficScape uses the underlying search engine to reconstruct views of complex http traffic and Web 2.0 applications. For example, TrafficScape is able to trace botnet machines use of social network sites to communicate with their masters, as was documented with the Ghostnet cyber attacks uncovered last year.

TrafficScape is at a very early stage, the first version having been released early this year. We have only one direct government contract, but other units purchased and on evaluation loan to integrators and cyber security consulting firms.

### **Small Business Agenda**

Dejavu is a small company with a big idea. Thus, Dejavu is an example of small business as a fountainhead for out-of-the-box thinking and innovative ideas for solving the world's most important problems. The challenge for an innovative company like Dejavu is to get the big idea heard by the agencies who should care, because the new technology might further their mission.

Government policy regarding small business has many noble goals, but "innovation" is fairly low on the priority list. The major goal is economic growth and job creation. A secondary goal is to provide opportunity for disadvantaged groups or geographies. Most of the government programs I have seen support those goals. However, support for technical innovation is more difficult to find.

### **Innovation and Cyber Security**

Cyber security is an arms race, with effective defenses spawning newer and more creative threats. There will never be a perfect shield, nor a silver bullet. Dejavu has focused on the forensic problem, because discerning and researching new threats will be a perpetual challenge.

As a nation we must understand that encouraging innovation is key to tackling the cyber security challenge. In fact, this challenge is actually an opportunity for government to experiment with more and better ways to encourage technical innovation.

**Anecdote: a trip to my local SBA office**

We work closely with technical groups within a large systems integrator, and I wanted to further that relationship. When I heard SBA provides support for large systems integrators to "mentor" small innovative companies, I made an appointment with the SBA office in Massachusetts. I immediately discovered the "mentor" program was an 8a set-aside, for which we did not qualify. However, the SBA representative proudly showed me their full list of SBA programs. While all were worthy, none were helpful to us:

- Mentor – 8a set-aside.
- SBA loans through local banks – requires a personal guarantee plus asset collateral, or specific contracts with cash flow needs.
- SBIC equity through local VC firms – no different from other VCs.
- SBIR technology grants – 1-2 year process, applying to each agency.
- Hubzone – targets geographical areas we are not in.
- PTAC (procurement assistance to match our skills to government agencies) – not designed for high technology, but for service contracting firms.
- Consulting advice about business plans – not needed for us.
- Contracting Assistance – not needed for us.

**Anecdote: What Stimulus Money?**

Stimulus money was in the headlines for many months last year. I was amused by the words "shovel ready" to mean projects that could be implemented immediately. Because of our prior technology ventures, we have an extended network of highly qualified engineers, local in Massachusetts, unemployed or doing consulting work. We could put them to work "immediately" building advanced cyber security products, for which we know there are government requirements. I had limited time bandwidth to seek such money, and I was unsuccessful at finding any.

**Hindrances to innovation (and some constructive suggestions)**

**Software Certification.** Certification and accreditation of software is a requirement for many agencies. There are very good reasons, of course. However, this is a significant hurdle for small innovative companies. The going rate for outside consultants to manage this is about \$100,000 plus 6-12 months of time. It would be helpful if there were government money, or a free government-sponsored service, to move promising products through this process.

**Security Clearance.** Many cyber security programs require security clearances for a full discussion of technical requirements and innovations. Security clearance requires a sponsor to take a direct interest. Policies to facilitate this process would be helpful.

**Technical intermediaries.** There are technical consulting organizations, whom government agencies rely upon for objective answers about new technology. MITRE is a good example. Rather than wait for specific government sponsor request, it would be helpful if such organizations were given charter and funding to validate the claims of new and innovative products. Objective validation of technical claims, and comparison of a variety of creative solutions, is a valuable service to both the vendor and the government sponsor.

**Outreach programs.** Some agencies have created a department for handling outreach to new, small companies. In our experience, very good examples are the ARC registration process and intro sessions at both NRO and Ft Meade, and also the DHS S&T industry outreach program. These departments attempt to function as gatekeepers, to potentially link new firms with technical sponsors within the agency. More funding for these activities would be welcome, especially if there were ways to measure such productivity, and if more funding assures that personnel have technical qualifications which allow them to be credible to both outside firms and to the agency experts they serve.

**Tax policy.** Finally, it is obvious to point out that we would like to be rewarded for this hard work, at the end of the day. Therefore, it is very discouraging to hear about raising the long-term capital gains tax for equity that we entrepreneurs hold.

### **Conclusion**

Government policies in support of technical innovation should promote a wide variety of technology ideas to compete openly, rather than attempt to pick technology winners. In this respect, government should be wary of trying to emulate the VC industry, whose mission is to make good returns on their money, rather than to solve the world's most important problems. Competition for new solutions should have a level playing field of information. A little chaos is a good thing. Given a chance, in the form of attention, time, and money, the best ideas will rise to the top.

**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 109<sup>th</sup> 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:** John H. Ricketson

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

Individual

Representative

**If appearing in a representative capacity, name of the company, association or other entity being represented:** Dejavu Technologies, Inc., Marlborough, Mass

**FISCAL YEAR 2010**

federal grant(s)/ contracts	federal agency	dollar value	subject(s) of contract or grant
none	US Navy	<\$1M	Network Analysis & Test

**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			

**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 (2010): 1 ;  
 Fiscal year 2009: 0 ;  
 Fiscal year 2008: 0 .

Federal agencies with which federal contracts are held:

Current fiscal year (2010): US Navy ;  
 Fiscal year 2009: \_\_\_\_\_ ;  
 Fiscal year 2008: \_\_\_\_\_ .

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 (2010): Network Forensic Analysis & Test ;  
 Fiscal year 2009: \_\_\_\_\_ ;  
 Fiscal year 2008: \_\_\_\_\_ .

Aggregate dollar value of federal contracts held:

Current fiscal year (2010): <\$1M ;  
 Fiscal year 2009: \_\_\_\_\_ ;  
 Fiscal year 2008: \_\_\_\_\_ .

**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 (2010): 0 ;  
Fiscal year 2009: 0 ;  
Fiscal year 2008: 0 .

Federal agencies with which federal grants are held:

Current fiscal year (2010): \_\_\_\_\_ ;  
Fiscal year 2009: \_\_\_\_\_ ;  
Fiscal year 2008: \_\_\_\_\_ .

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

Current fiscal year (2010): \_\_\_\_\_ ;  
Fiscal year 2009: \_\_\_\_\_ ;  
Fiscal year 2008: \_\_\_\_\_ .

Aggregate dollar value of federal grants held:

Current fiscal year (2010): \_\_\_\_\_ ;  
Fiscal year 2009: \_\_\_\_\_ ;  
Fiscal year 2008: \_\_\_\_\_ .

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

Hearing on:

*Harnessing Small Businesses Innovation for National Security  
Cyber Needs*

Roger Thornton  
Founder and Chief Technology Officer

Fortify Software  
2215 Bridgepointe Pkwy, Suite 400  
San Mateo, CA 94404

July 28, 2010

**Testimony of Roger Thornton  
Founder and Chief Technology Officer**

**Fortify Software**

**San Mateo, CA  
July 28, 2010**

Good afternoon Chairwoman Sanchez, Ranking Member Miller, and distinguished members of the Committee. I appreciate this opportunity to comment on the crucial role of small business innovation within the realm of cyber security.

My name is Roger Thornton and I currently serve as the Chief Technology Officer at Fortify Software. I have worked in the Information Technology industry in Silicon Valley for the past twenty- three years. During that time I have been involved with the formation and development of over a dozen startup companies and have held engineering and management positions with some of the world's largest technology firms.

My technical expertise is in finding, fixing and preventing the software vulnerabilities that are at the very core of our cyber security dilemma. My current responsibilities involve the development and design of processes and technologies that eliminate software vulnerabilities in order to make IT systems resilient to the literally billions of attacks we see each day on the Internet – making software “hacker-proof” if you will. Traditional IT security strategies – the status quo – attempt to mask these underlying vulnerabilities with bolt-on security features and that approach has led us to the situation we find ourselves in today. The approach my firm has pioneered represents a fundamental shift in thinking as we have moved the security strategy from defending network perimeters and blocking attacks to hardening the core of our IT systems making them impervious to attacks – moving from network security to software security.

Fortify is a small company - a classic “Silicon Valley” startup - founded by myself and three co-founders in the spring of 2003. As with many innovative small businesses we have experienced rapid growth that has not just helped more than 700 customers transform their cyber security strategies, but has also created jobs and increased tax revenues within our communities. Today we employ over 200 people in 14 countries around the globe that help businesses and government agencies locate, eradicate, and prevent the software vulnerabilities that enable our adversaries to penetrate our most critical systems. Our customers include eight of the ten largest banks in the world, all the major branches of the US military, and a majority of the major telecommunications firms in the US and Europe, along with a host of other leading firms in the retail, insurance, healthcare, and manufacturing sectors.

Through the course of my work I am familiar with the amount and types of vulnerabilities found in our nation's most critical infrastructure and I can tell you with emphatic certainty that we are in a desperate situation. My firm's technologies have helped conduct audits on thousands of critical IT systems and not once have we found a system with no critical vulnerabilities - in most cases we find literally thousands of such issues.

One example set of data comes from a Fortify team that conducts audits and reviews of military systems. Over the course of two years that team has audited 601 software applications across 141 major programs and found over 3.8M security vulnerabilities – 441,813 defined as critical. This is not exceptional but has become the norm and represents a problem that is not currently receiving appropriate attention. Now of course, we help organizations eradicate these vulnerabilities as we find them, but for every system we have audited and remediated, there are a thousand others we have not yet engaged. And there are organizations that find thousands of critical vulnerabilities in their systems and due to funding constraints make a conscious decision to do nothing. Fortify is one of a few firms entirely dedicated to solving this problem.

There are two compelling reasons for you to consider and actively support the role that small businesses like Fortify have to play in solving cyber security issues.

The first is economic. Small businesses have historically been an incredibly important driver for job growth in the US economy and cyber security is no exception to that rule. According to the US Small Business Administration the estimated 29.6 million small businesses in the United States:

- Employ just over half of the country's private sector workforce
- Hire 40 percent of high tech workers, such as scientists, engineers and computer workers
- Represent 97.3 percent of all the exporters of goods
- Represent 99.7 percent of all employer firms

*Source: U.S. Small Business Administration Office of Advocacy, September 2009*

At the close of the first year Fortify was in business (2003), the Dow Jones Industrial average was at 10,453.92, this week it opened at 10,424.17 – the nation's largest companies have spent the last ten years treading water. Over the same timeframe, my company has seen a 1,500% growth in revenues and has added nearly 200 high-paying technology jobs to the US economy.

The second imperative for the active participation of small business in the domain of cyber security is their propensity to introduce much-needed, radical innovation into the marketplace.

The status quo for IT security has generated an extraordinary amount of profit in creating the unsustainably insecure environment we find ourselves in today. According to Gartner Group over the past five years the IT security spending in the US was nearly \$70B / year – this at a time when all branches of the US military and nearly every major company in America were victims of cybercrimes large and small. Only a small company would have the audacity and the impetus to challenge the status quo and offer an entirely new approach to a problem with entrenched solutions.

Like many small businesses, our company was founded on a simple observation that challenged conventional thinking. That observation led to a fundamental innovation – a radical departure from the status quo and in our case a complete change in the way we look at and solve the problem of cyber security, and that resulted in our success and growth.

Our observation was this:

1. IT systems are comprised of networks, hardware and software. Networks connect computers that have software programs running them.
2. The prevailing strategy for IT security is to "secure networks" by limiting access and attempting to block attacks as they happen.

3. That traditional cyber security approach has become outdated and is fundamentally flawed. It is a game we are destined to lose. Why? Simply put, nearly all the software we rely upon to run our critical infrastructure is built with major vulnerabilities – consider them effectively “open doors” for hackers. Our adversaries have shifted their approaches to leverage these “open doors” in software and we have responded with increased spend in the security of our networks. The results speak for themselves.
4. If we eradicate the software vulnerabilities the attacks won’t work – we can build our software systems to be resilient to attack. This is not much different from today’s practice of building office buildings that are resilient to fire.

This line of thinking represented a radical departure from the status quo and a complete change in the way we look at and solve the problem of cyber security – and in the Silicon Valley that means a new small business determined to solve an old problem in a new way. In spite of the strides we have made at Fortify and other small firms developing innovative cyber security solutions, the status quo still poses extraordinary challenges that could use your support to overcome.

These include:

1. **Disproportionate** focus on protecting Hardware and Networks while the majority of the attacks are at the Software Layer
2. **Lack of Policy** relating to software security that leads naturally to vague software security requirements and inadequate funding for software security initiatives
3. **Inadequate Funding** to fix the “holes” once they are found in legacy software programs
4. **Outsourcing of Mission Critical Software Development to Contractors** and third parties

As an industry, we have inadvertently developed our way into an unsustainable cyber security dilemma and only the most disruptive innovations will help us find our way out. The solutions to address this problem are almost certain to come from small, innovative companies. These small businesses have produced enormous economic prosperity for our nation and in this realm they will hold an extraordinary importance in our national security.

Allow me to frame the problem for you as we have observed it over the last seven years in greater detail.

Last summer a journalist asked the newly appointed Federal Chief Technology Officer, Aneesh Chopra, a typical question “What keeps you up at night?” The CTO responded with “it is not the recent denial of service attacks over the Fourth of July – but sloppy software implementations that have left holes open for hacking.” Hackers, all over the world, rely on these holes or vulnerabilities being left open so that they can easily penetrate systems operating in the US whether they are in the defense, financial, or critical infrastructure protection industries. We would submit, however, that it is less an issue of “sloppy software implementations” but more often a lack of awareness on how to build and maintain secure software. The ability to find and fix existing vulnerabilities in legacy systems as well as prevent additional vulnerabilities from being introduced into new developments has become part of the critical path to thwart the Advanced Persistent Threat that professional hackers hosted by nation-states have come to represent.

In the last year, we have witnessed an important evolution of thought represented by the draft cyber legislation from several committees that has elevated the focus on software to provide parity for software security. We were pleased to see the Armed Services Committee address the specific issue of software security in the Draft NDAA for FY2011 in Section 932. The language in Section 932 will advance America’s long term security goals by transforming how the software industry and users approach security to deal with the growing threat of Cyber Warfare. Historically there has been a disproportionate focus on funding for hardware and network security. In the last ten years considerable sums of money have been spent specifically to bolster network defenses.

However when a critical breach occurs the refrain is not “my network was stolen”, instead the lament is typically “thousands of data records were stolen.” Ultimately the majority of these attacks have exploited vulnerabilities in the software layer that allowed them to access data. Industry analysts now estimate that up to 75% of attacks are attributable to the software layer. Our goal is to raise awareness on the necessity to harden the software layer as the last line of defense to protect critical systems and their data.

Select critical infrastructure industries have mandated adherence to software security principles. As an example the financial industry enacted the Payment Card Industry- Data Security Standards (PCI-DSS) requiring companies to analyze their software for known vulnerabilities, and to fix those vulnerabilities. The penalty for failing a PCI audit is strict – loss of the ability to process credit card transactions – and has contributed to stronger software systems and a reduction in overall exploitable vulnerabilities. Adoption of software security requirements outside of the financial industry is lagging; nevertheless, awareness of the problem is growing dramatically due to the spate of recent hacks that have been made public and the realization that the software layer is so vulnerable.

I’m sure you are aware of the publicity surrounding the Google hack in 2009, in which one of Google’s primary applications, Gmail, was hacked into ostensibly to spy on communications between Chinese human rights activists. Google was not the only company hacked. According to recent reports, over 30 other US-based companies were compromised, with the primary intent to gain access to software code repositories. There are two reasons to access source code repositories – either to steal intellectual property, or to modify the source code without the owner’s knowledge, perhaps inserting a backdoor for future use. But the main reason I draw attention to this issue is because it wasn’t a “network” breach – most networks are open for business everyday – rather the root cause was a software vulnerability that allowed the hackers to gain control and credentials on the target organization’s systems.

While the damage done to date by massive cyber espionage (of exploitable software code) is impossible to calculate from an economic and national security standpoint, we are facing even more pressing disasters if immediate actions are not taken to counter a host of cyber warfare scenarios, especially those targeting mission critical information systems.

The United States Government is struggling considerably with the issue of secure software due to some unique constraints that have evolved out of aggressive outsourcing of software development to contractors and third parties. There are only a few agencies in the U.S. Government that still employ their own in house software development organization – the Department of Veteran’s Affairs, Social Security Administration, Federal Aviation Administration and the Internal Revenue Service are examples of agencies who maintain in house software development. The majority of the Federal Government, including the Department of Defense and Intelligence Community, outsource much of their software development to Contractors. In many other critical infrastructure industries it is the exact opposite where 80% of their software development is performed internally and only 20% is outsourced.

We have witnessed that the industries that have more control over their software development are much more inclined to incorporate software security into their development efforts. This one key difference represents a significant delta in how securely software is developed and whether or not the final software deliverable is only implied to be secure or is actually devoid of known vulnerabilities. While it is unrealistic to expect the Government to swap the ratio, recognition of this fact should be taken into account in any new legislation seeking to improve software security.

Another key point to illustrate the unique struggle of the Federal Government is the reliance upon custom software development in support of mission critical systems as opposed using Commercial off the Shelf (COTS) technologies. Weapons systems, guidance systems, satellite systems, and UAV’s are all examples of custom coded software systems that have been publicly reported to be under constant attack by hackers. For example, it has been reported that the F35 program was penetrated and purportedly several terabytes of data were stolen. It is highly probable that vulnerabilities in the software layer were exploited to gain access to that significant amount of data.

A stronger defensive posture to improve the security of third party custom developed software is paramount to improving the overall defense of these mission critical systems. The Federal Government should not accept software from third parties that have known vulnerabilities within the code.

A lack of clearly defined software security policy has led to a lack of clearly defined software security requirements which translate into a lack of funding for software security being incorporated into major programs. Furthermore, when vulnerabilities are found in software, it is not easy to determine who is responsible for fixing the problem and paying for the fix – the Government Agency or the developer of the software. Due to this lack of clarity it has become common practice to try and find a waiver around the problem rather than remediate and fix the vulnerabilities.

In terms of successfully requiring software assurance, the private sector – and the financial community in particular – surpasses the public sector. Financial organizations must develop, maintain and regularly test secure systems and applications under the Payment Card Industry Data Security Standard. Those that fail risk losing their ability to do business or face audits and fines.

Despite overwhelming and long-known evidence that software security is essential to safeguard sensitive data, no federal mandates exist for software security similar to other IT security practices. Most organizations don't sufficiently implement software security under the current certification and accreditation (C&A) model the federal government currently requires for agencies and partners. No federal budgets to date have included specific language requiring software security or how to implement it.

The federal government has taken some small steps to require software assurance in the software development life cycle for products it creates and buys. The Federal Information Security Management Act of 2002 (FISMA), which sets out federal IT security C&A requirements, only generally mentions software security assurance as part of an overarching IT security strategy. Instead, the law focuses on ensuring agencies implement a broad array of Commercial Off-the-Shelf (COTS) technologies such as firewalls and antivirus – all built, and designed to protect, according to the “bolting on” security model. That model was appropriate in the days when FISMA was enacted, but a more advanced “baking in” model is now available, which removes the vulnerabilities in the application itself, thereby effectively weaving a “Kevlar vest” into the software.

FISMA's attendant guidance, NIST Special Publications 800-37 and 800-53, provides more specific information but still concentrates more on adding security technologies to defeat threats instead of ensuring federal systems don't contain vulnerabilities in the first place. The Department of Defense has even more demanding requirements through the DoD Information Assurance Certification and Accreditation Process (DIACAP), which defines levels of system priorities and defect rationalization all the way to the application vulnerability layer. While the process itself is broad in scope, encompassing the entire DoD “defense in depth” strategy, it stops just short of mandating automated source code scanning and fixing vulnerabilities in the core software assets running the entire Department!

Unfortunately, all these steps have been largely unsuccessful for many reasons. They have lacked funding for implementation and penalties for noncompliance. No requirements exist for automated code scans, remediation and active protection of running applications. Many government and industry experts have complained since FISMA was passed that it is a paper tiger that rewards completing compliance checklists more than actually improving IT security.

Because FISMA does not require software security directly, accompanying guidance or procurement language does not include sufficiently specific detail. That has translated into awarding individual “stove-piped” software security-related contracts that only include the appropriate level of detail for software security implementation, instead of having such language included in all IT security-related contracts.

In spite of the lack of clear policy direction there are several DOD organizations and Government Agencies that have adopted a pro-active stance vis-à-vis incorporating software security practices. The U.S. Air Force has established the Application Software Assurance Center of Excellence (ASACoE) in Montgomery, Alabama after a foreign adversary successfully attacked the Air Force's Military Assignments application and stole tens of thousands of personnel records.

The Air Force has amassed a compelling body of reusable vulnerability knowledge from assessing the software of 600 applications resident at 141 Program Management Offices. They have discovered 3.8 Million total software security issues and approximately 440,000 critical issues that require remediation. The software vulnerabilities discovered by the Air Force likely represents the current attack surface of software for a typical DOD installation. The valuable insight gained by the ASACoE should be used to strengthen software applications throughout the entire Department of Defense and could also assist the Department of Homeland Security among others.

The U.S. Army has taken the issue of software security a step further by conducting both assessments of their software and requiring remediation of the critical vulnerabilities that they discover during the process. The Army Data Center in Fairfield, California is a software hosting facility where they plan to assess the security of the software before they allow the software access to their networks. Software that is deemed too vulnerable will not be provided an authority to operate on the networks that they control thereby creating an important gate that the software must pass. This is a common practice throughout the Financial Community where it is imperative to keep vulnerable software away from their networks so that it does not compromise other connected systems.

The Department of Veteran's Affairs employs over two thousand software developers to build their systems. The VA has invested in an enterprise capability to build software security into their software development cycle from inception instead of bolting on security as an afterthought. The Healthcare industry has also become increasingly cognizant of the need for strong security due to HIPAA and privacy requirements that have driven their adoption of software security principles.

Funding obstacles have bedeviled each one of these organizations and prevented them from fully implementing a mature software security program in the timeframes that they desire. Lack of an overall Federal Policy relating to software security has led Program Managers to look to their own Agencies for policy direction or be left to try and implement it one by one on their own programs. This piecemeal approach has been ineffective at thwarting the advanced persistent threat attacks as the level of intensity and volume of cyber attacks continues to escalate.

After hearing this refrain from countless organizations we strongly support the direction that the Armed Services Committee has taken in the draft NDAA Section 932 on Software Security. We believe that the draft language adequately addresses the four key challenges that we have observed. Namely, it recognizes Software as a distinct challenge separate but equal to the challenges in securing Hardware and Networks. This is an admission of the key role that software plays today in all major custom built applications whether they are administrative personnel systems or highly advanced targeting and weapons systems.

Second, the language addresses establishing strong policy guidance for assuring software systems particularly for covered acquisition systems initially. We feel strongly that in time this positive guidance will naturally flow down into all systems that are worthy of these security protections.

Third, the language will help establish achievable and measurable requirements for incorporating software security requirements into new, but more importantly existing legacy systems, to limit their exposure to exploitation by attackers. The language makes it very clear, for the first time, that when software vulnerabilities are found they must be fixed. That is not the case today and it has obviously caused considerable chaos and left the United States extremely vulnerable to attack.

Lastly, it is essential that a funding mechanism be established to ensure that the principles of software security are implemented in a timely fashion so that we can create the best possible defense.

As a small, innovative technology start-up we spend a considerable amount of our time creating awareness of what the true problems are in the fight against cyber threat and which problems are currently addressable by today's technology offerings. We have a strong conviction and have established high confidence that the right combination of technology, human capital, and processes can combine to confront the Advanced Persistent Threat and ultimately prevent Cyber Warfare. We look to Congress to establish the top level strategic policy guidance for Cyber and we applaud Congress for being so active as this inspires not only the mature small companies, like Fortify, but it also gives hope to the next generation of innovators to invest.

On behalf of all of us at Fortify, I would like to heartily compliment this committee, as well as both the House and Senate Armed Services Committee, for the leadership that you have shown on addressing the issue of cyber security. We have been very impressed with the professionalism and tenacity of your staff's ability to break down a complex and technical issue so that they could fully comprehend the implications of software security, and you are truly performing groundbreaking work

I would like to personally thank Chairwoman Sanchez, Ranking Member Miller, and the members of the Subcommittee for holding this hearing on the impact of small business innovations on cyber security issues. Software security is a key facet of any attempt to protect critical systems and to secure the data stored within those systems. We look forward to working with you and the House Armed Services Committee to continue to make sure software security becomes a fundamental component of all federal cyber security efforts.

**Roger Thornton****Founder & Chief Technology Officer**

Roger Thornton founded Fortify Software in October 2002, convinced that information security required a fundamental shift in thinking - from a focus on the perimeter to a focus on the core - the software code itself. Incubated with acclaimed venture firm, Kleiner Perkins Caufield & Byers and recognized by Business 2.0 magazine as the "Smartest Start-Up for 2005", A Silicon Valley native, his career began at Cypress Semiconductor, the technology stalwart labeled "a quintessential entrepreneurial company" by The Wall Street Journal. At Cypress he was ultimately responsible for the development of the firm's renowned manufacturing planning systems. Roger earned his BS and MS degrees in Engineering with honors at San Jose State University. Roger consistently consults with several venture capital firms, corporate executives and government leaders on security, cyber security policy and emerging trends.

**Fortify Software**

Software code has become the focus and ultimate target of cyber security exploitation. While the individuals and nations, who continue to excel at gaining access to systems software and data, have refined their ability to exploit the software that runs mission critical systems the policies to protect Government systems have not evolved to counter this advanced persistent threat. Fortify Software, the leader in Software Security Assurance, automates the ability to find vulnerabilities throughout millions of lines of code, and assists with the remediation of those vulnerabilities ultimately fortifying the software from attack. Fortify has been working closely with the AF, Army, OSD, IC, HASC and SASC to strengthen the guidance for Software Assurance in the DOD Certification and Accreditation process.

**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 109<sup>th</sup> 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: Roger Thornton**

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

Individual

Representative

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

**FISCAL YEAR 2010**

federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
Contracts	U.S Air Force	1.5 Million	Application Security Software/Services
Contracts	U.S Army	\$880,000	Application Security Software/Services
Contracts	U.S. Navy	\$217,000	Application Security Software/Services
Contracts	U.S. Veterans Administration	3.8 Million	Application Security Software/Services
Contracts	MDA	\$272,000	Application Security Software/Services
Contracts	NOAA	\$22,000	Application Security Software/Services
Contracts	DOD	\$46,000	Application Security Software/Services
Contracts	OSD	\$187,000	Application Security Software/Services

**FISCAL YEAR 2009**

federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
Contracts	U.S. Government	\$147,000	Application Security Software/Services
Contracts	DHS	\$165,000	Application Security Software/Services
Contracts	DLA	\$295,000	Application Security Software/Services
Contracts	U.S. Army	2.3 Million	Application Security Software/Services
Contracts	U.S. Air Force	3 Million	Application Security Software/Services

Contracts	MDA	\$185,000	Application Security Software/Services
Contracts	DTRA	\$439,000	Application Security Software/Services
Contract	Executive Office of President	\$120,000	Application Security Software/Services
Contracts	Federal Reserve	\$53,000	Application Security Software/Services
Contracts	U.S. Treasury	\$132,000	Application Security Software/Services
Contracts	NOAA	\$33,000	Application Security Software/Services
Contracts	DOD	\$45,000	Application Security Software/Services

**FISCAL YEAR 2008**

Federal grant(s)/ contracts	federal agency	dollar value	subject(s) of contract or grant
Contracts	U.S. Air Force	\$343,000	Application Security Software/Services
Contracts	U.S. Army	\$330,000	Application Security Software/Services
Contracts	DHS	\$36,000	Application Security Software/Services
Contracts	DOD	\$100,000	Application Security Software/Services
Contracts	OSD	\$86,000	Application Security Software/Services
Contracts	DOD	\$87,000	Application Security Software/Services
Contracts	NOAA/NASA/IRS	\$45,000	Application Security Software/Services

**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 (2010): 26  
 Fiscal year 2009: 37  
 Fiscal year 2008: 17

Federal agencies with which federal contracts are held:

Current fiscal year (2010): **U.S. Army, DOD, EPA, U.S. Air Force, US. Navy, Veterans Administration; TRICARE, OSD, DOD**  
 Fiscal year 2009: **NIH, DLA, DOD, Department of Energy, U.S. Air Force, IRS, FRB, U.S. Army, Executive Office of The President, EPA, FTC, NASA, MDA, DTRA, DLA, U.S. Government**  
 Fiscal year 2008: **U.S. Army, U.S. Air Force, IRS, NASA, DOD, DHS, NOAA, State Department, U.S. Treasury Thrift, OSD, DLA, FRB**

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 (2010): Application Security Software and Services;  
Fiscal year 2009: Application Security Software and Services;;  
Fiscal year 2008: Application Security Software and Services;.

Aggregate dollar value of federal contracts held:

Current fiscal year (2010):7.1 Million Dollars;  
Fiscal year 2009: 6.9 Million Dollars;  
Fiscal year 2008: 1.1 Million Dollars

**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 (2010) 0  
Fiscal year 2009: 0  
Fiscal year 2008: 0

Federal agencies with which federal grants are held:

Current fiscal year (2010): 0  
Fiscal year 2009: 0  
Fiscal year 2008: 0

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

Current fiscal year (2010): 0  
Fiscal year 2009: 0  
Fiscal year 2008: 0

Aggregate dollar value of federal grants held:

Current fiscal year (2010): 0  
Fiscal year 2009: 0  
Fiscal year 2008: 0

**RICHARD P. LEE**  
9471 Harrowhill Lane  
Burke, VA 22015-1538

July 26, 2010

Subject: Testimony before the Terrorism, Unconventional Threats and Capabilities subcommittee of the HASC on *Harnessing Small Businesses Innovation for National Security Cyber Needs*

Thank you for inviting me to address the Subcommittee on this topic of increasing importance to the Nation. I approach the challenges of maintaining and sustaining the cybersecurity of our Nation's information resources from a lifetime of exposure to the intersecting demands for rapid, reliable information sharing and protecting the confidentiality, integrity and availability of that information – the three pillars of Information Assurance.

I understand of the focus of the Sub-Committee's hearing is on the challenges and impediments to enabling the Nation's ability to dominate and operate in the emerging cyber space arena, and to taking advantage of American technical know-how. Because the Nation's economy and operational capabilities depend on Internet connections – our ability to manage and respond to crises, our ability to access and share data and information, and our ability to communicate and collaborate – we must not abandon the "battlefield" but must find ways to operate through attack.

A significant challenge facing the Nation, particularly when executing governmental functions, is how to harness the passion, originality and resourcefulness of US innovators. Users, collectively the operational mission elements, are expected to articulate their requirements in technical terms. A problem is that operational elements and technical solutions providers often "talk past" each other – the former trying to describe what is needed in mission language; the latter hearing the need in terms of the products or implementations with which they are familiar. Too often, rather than take a step back to apply holistic systems engineering principles, engineering effort is expended to fix a discovered vulnerability, meet an emergent external threat, or enable tighter control over the user community – countering the "insider threat".

In my opinion, there are three primary areas that impede innovation and the introduction or adoption of novel approaches to cyberspace threats:

- A. The acquisition process
- B. The Evaluation and Certification Process
- C. Financial resources

July 26, 2010

Page 2

The acquisition process pulls cyber solution space toward the “big pocket” integrators who can afford the “Bid & Proposal” process funding needed to compete for implementation contracts. In a normal hardware based large system acquisition, the technical proposal is often limited in size, is focused on responding to technical specifications that bound the competitive space, and often “wins” on best value (*i.e.*, cost to implement and sustain.)

Difficult to estimate are potential costs to transition from existing systems implementations to the new. Impossible to estimate is the “lost opportunity” and future costs from only “patching” the architecture with upgrades and incremental fixes. Recall Albert Einstein’s statement: “No problem can be solved from the same level of consciousness that created it.” ([http://www.tc.umn.edu/~bure0050/quotes\\_einstein.html](http://www.tc.umn.edu/~bure0050/quotes_einstein.html))

Total Cost of Ownership (TCO) is also difficult to estimate, including the potential impacts on physical plant (space, weight, power, heat dissipation or air conditioning required), manpower, training, and logistics issues. Larger companies experienced in providing solutions to government customers are often better able to navigate the proposal process, describing offerings in language familiar to proposal evaluation teams. An effect may be an inadvertent and unrecognized institutional bias toward a well crafted proposal without appreciation for underlying “sameness” of the technology to current implementations.

The evaluation and certification process is king in the government cyberspace arena. For valid reasons, cyber technology solutions must be known to work, the vulnerabilities to attack, breach, exploitation or failure understood, and *a priori* plans made to mitigate, manage or respond to potential situations in which system functions are in jeopardy. A problem is that there are few practitioners available to evaluate cyber space technical offerings. As a result, technology offerings are required to conform to existing standards and implementations that have been studied, and their vulnerabilities understood. Starting from that point, the evaluators can quickly assess the “correct” implementation of the standards invoked in a solution, can assess how the known vulnerabilities inherent in the standards are mitigated or addressed by the solution, and can accomplish however much “penetration testing” may be called for given the planned environmental use for the solution, *e.g.*, will financial information, secret military information, or other information be processed on the system?

Since the evolution of many of the cyber space standards and protocols were originally developed in an academic environment where trust was assumed between colleagues, mitigating some of the now known vulnerabilities has required layering on manpower intensive procedures, monitoring and internal “fire-breaks” to prevent exploitation of the “insider threat” – the disgruntled or malignant human operator, poorly designed or malfunctioning hardware or software, or poorly trained or inattentive user.

The dilemma facing the evaluation and certification communities are that new often proprietary approaches, innovative implementation of defined standards, or novel

July 26, 2010

Page 3

concepts require first understanding the “new” (getting into the innovators’ heads), evaluating the concepts, architectures, or proposed implementations for potential vulnerabilities, and then assessing the specific implementations against the just evaluated approach. Without a stated government customer who can define the planned operating environment where the new solution will be used, evaluation of proposed mitigation techniques (*e.g.*, administrative processes, physical access controls, *etc.*) cannot proceed. With limited resources to recruit, train, and maintain trusted evaluation staff, the workload is daunting. A result is a bias to embrace current architectures, approaches, and standards and protocols with known vulnerabilities.

Some people have proposed a “fee for evaluation service” approach in which the innovators can fund the evaluation of their innovative or novel approaches to cyber problems. A problem persists, however, in identifying the planned environment in which the solution will be employed. The resolution of that problem lies in “the Champion” for the solution – the person with sufficient influence and authority to “pull” a novel solution into evaluation. A difficulty for most small business innovators is finding the government official or organization that can perform the role of “Champion,” and then gaining an audience to expose the solution. The acquisition process further dissuades this approach to avoid an appearance of competition manipulation.

There are some programs and initiatives pursued by Executive Departments to provide fora for the exposure of innovation to the people with the problems to solve. Two examples include DARPA programs and the Defense Research and Engineering Directorate Joint Capabilities Technology Demonstration Program.

Recommendations:

1. Fund research and development innovation incubation initiatives that formalize linking innovators and “Champions” to accelerate identifying operating environments and promising technologies.
2. Fund expanded evaluation activities to more quickly respond to novel or innovative approaches to cyber solutions.
3. Direct Executive Departments to report on systems engineering activities to examine holistic approaches to cyber challenges. (*E.g.*, how might an emerging computing and communications multi-core hybrid fabric mesh enable defense in depth security services?)

**Richard Patrick Lee**

9471 Harrowhill Lane  
Burke, VA 22015-1538

Day: (571) 239-6718  
Eve: (703) 323-8957  
Richard.Lee@richardplee.com

**OBJECTIVE** Enable mission success by applying information centric concepts and technologies to achieve information interoperability, implementing information sharing policies and organizational enterprise vision.

**SUMMARY** Over twenty-eight years' progressive leadership and management experience in complex strategic and tactical business processes, communications systems operations, and information systems integration.

**ACCOMPLISHMENTS**

**Concepts definition** Advocate for "Data with Context" application to Defense Department operating concepts, information systems, and business processes, leading to department information interoperability demonstrations.

**Personnel leadership** Oversight of diverse teams of government, industry, academia and Military personnel to deliver advanced technology solutions for Warfighter operational problems; over 80% transition to sustainment.

**Coalition building** Adept consensus builder. Establishes trust and guides team interactions. Sought out for cross-community problem solving.

**WORK HISTORY**

2009 – Present Self Employed Information Systems Consultant, 9471 Harrowhill Lane, Burke, VA 22015  
Project management consulting in data, information and systems interoperability. Assist clients to align project resources to mission, including decomposition of mission challenges and operational concepts for solutions generation through comprehensive information systems engineering.

2005 – 2009 Deputy Director, Information Centric Projects, Joint Capability Technology Demonstration (JCTD) Program (formerly Asst Deputy Under Secretary of Defense (Information Integration & Operations), Pentagon IPA from SRI International, 333 Ravenswood, Menlo Park, CA 94025  
Oversight of \$200 million in fourteen information technology demonstration projects applying data interoperability concepts to demonstrate solutions for shortfalls in cyberspace capabilities in communications, command & control, and information assurance.  
Ensured Netcentric JCTD projects conformed to enterprise Defense Department visions, goals, principles and policies. Performed strategic capital investment planning, including performance-based budgeting, President's budget exhibit development, and transition of proved technology to program of record sustainment.

- 2001 – 2005 Asst Deputy Under Secretary of Defense (Information Superiority)  
 USD (AT&L)/DDR&E/ODUSD (AS&C), Pentagon  
 IPA: SRI International, 333 Ravenswood, Menlo Park, CA 94025-3493  
 Proposed, evaluated and guided execution of Advanced Concepts Technology Demonstrations (ACTDs) in Command & Control, Computers, Communications and Intelligence (C4I) mission areas. Formulated project implementation and acquisition transition strategies.  
 Oversight of \$100 million in C4I ACTDs, in communications, information interoperability, network security, and command & control.  
 Successfully transitioned ACTD products into commercial production, sustained network functionality, or Service capability and technology bases. Coordinated the termination of projects that did not meet expectations, were immature in implementation, or for which there was no sustaining path.
- 1999 – 2001 Director (Operations), Information Assurance Division, Galaxy Scientific Corporation, Arlington, VA (since purchased by SRA International)  
 Program manager for 100-person contracted support to the CIO, US Patent and Trademark Office (USPTO), in Software Acquisition, Software QA, Requirements Analysis and Management, Configuration Management, Data Quality Management, and Independent Test and Evaluation.  
 Led independent verification and validation team in planning and executing USPTO enterprise-wide simultaneous test of business critical automated information systems to demonstrate Year 2000 (Y2K) readiness.
- 1996 – 1998 Program Manager for Satellite Communications Systems Integration, Defense Information Systems Agency, Arlington, VA  
 Active Duty, Captain, US Navy  
 Initiated Information Dissemination Management Program which became content discovery and staging services within Netcentric Core Enterprise Services (NCES). Led DARPA-DISA Bosnia C2 Augmentation (BC2A) transition to sustainment – first Predator video distribution capability.
- 1972 - 1996 Active Duty, US Navy: Previous work assignments included director of daily operations of worldwide Navy telecommunications networks; executive director for personnel, training, maintenance and safety programs for 325-person unit conducting Navy fleet operations; scheduling and logistics coordination for 42 individual Navy fleet units conducting geographically dispersed operations; United Nations peacekeeper.
- EDUCATION M.S. in Communications Engineering, Naval Postgraduate School, Monterey, CA  
 B.S. in Marine Engineering, U.S. Naval Academy, Annapolis, MD
- SECURITY CLEARANCE: Top Secret effective August 2008

**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 110<sup>th</sup> 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:** Richard P. Lee

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

Individual

Representative

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

**FISCAL YEAR 2010**

<b>federal grant(s) / contracts</b>	<b>federal agency</b>	<b>dollar value</b>	<b>subject(s) of contract or grant</b>
Consulting Agreement	Institute for Defense Analysis	\$50,000.00	Command & Control Data Pilot for US Army
Consulting Agreement	US Navy	\$40,000.00	Demonstrate Organic Network Interoperability
Subcontract	US Navy	\$30,000.00	OSD JCTD Support

**FISCAL YEAR 2009**

<b>federal grant(s) / contracts</b>	<b>federal agency</b>	<b>dollar value</b>	<b>subject(s) of contract or grant</b>
Consulting Agreement	OSD/DDR&E	\$85,000.00	OSD JCTD Support
Intergovernmental Personnel Act	OSD/AT&L	\$114,312.00	Assigned to staff of DUSD (AS&C)

**FISCAL YEAR 2008**

Federal grant(s) / contracts	federal agency	dollar value	subject(s) of contract or grant
Intergovernmental Personnel Act	OSD/AT&L	\$167,375.00	Assigned to staff of DUSD (AS&C)

**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 (2010): 3 ;  
 Fiscal year 2009: 2 ;  
 Fiscal year 2008: 1 .

Federal agencies with which federal contracts are held:

Current fiscal year (2010): IDA, US Navy ;  
 Fiscal year 2009: OSD ;  
 Fiscal year 2008: OSD .

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 (2010): Interoperability, Cybersecurity ;  
 Fiscal year 2009: Interoperability, Cybersecurity ;  
 Fiscal year 2008: Interoperability, Cybersecurity .

Aggregate dollar value of federal contracts held:

Current fiscal year (2010): \$120,000.00 ;  
 Fiscal year 2009: \$199,312.00 ;  
 Fiscal year 2008: \$167,375.00 .

**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 (2010): NA ;  
Fiscal year 2009: NA ;  
Fiscal year 2008: NA .

Federal agencies with which federal grants are held:

Current fiscal year (2010): NA ;  
Fiscal year 2009: NA ;  
Fiscal year 2008: NA .

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

Current fiscal year (2010): NA ;  
Fiscal year 2009: NA ;  
Fiscal year 2008: NA .

Aggregate dollar value of federal grants held:

Current fiscal year (2010): NA ;  
Fiscal year 2009: NA ;  
Fiscal year 2008: NA .