HEARING TO RECEIVE TESTIMONY ON CYBERSECURITY RESEARCH AND DEVELOPMENT IN REVIEW OF THE DEFENSE AUTHORIZATION REQUEST FOR FISCAL YEAR 2013 AND THE FUTURE YEARS DEFENSE PROGRAM

TUESDAY, MARCH 20, 2012

U.S. SENATE,
SUBCOMMITTEE ON EMERGING
THREATS AND CAPABILITIES,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:35 a.m. in room SR–232A, Russell Senate Office Building, Senator Kay R. Hagan (chairman of the subcommittee) presiding.

Committee members present: Senators Hagan and Portman.

Majority staff members present: Richard W. Fieldhouse, professional staff member; Thomas K. McConnell, professional staff member; and Robie I. Samanta Roy, professional staff member.

Minority staff members present: John W. Heath, Jr., minority investigative counsel; Daniel A. Lerner, professional staff member; and Michael J. Sistak, research assistant.

Staff assistants present: Kathleen A. Kulenkampff, Hannah I. Lloyd, and Bradley S. Watson.

Committee members' assistant present: Brent Bombach, assistant to Senator Portman.

OPENING STATEMENT OF SENATOR KAY R. HAGAN, CHAIRMAN

Senator HAGAN. We're going to go ahead and open this meeting up. I know that Senator Portman is definitely coming, but has gotten tied up, so I think we'll go ahead and start because I think you also know that we have some votes occurring this afternoon, and what I'd like to do is go ahead and get started.

This afternoon the Emerging Threats and Capabilities meets to review testimony on cyber security research and development, in review of the defense authorization request for fiscal year 2013 and the future years defense program. The topic of cybersecurity has been the subject of growing concern and has figured prominently, not only in the newest strategic defense guidance released in January of this year, but also in previous national security and defense planning documents.

The 2010 national security strategy states that: "Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a Nation." The recent strategic defense guidance lists as one of the primary missions of the U.S. Armed Forces the need to operate effectively in cybersecurity and space, which will require investments by DOD in advanced capabilities to defend its networks, operational capability, and resilience in cybersecurity.

The challenge the Department of Defense faces is to find resources to address this growing threat in an era where there are increasing budgetary pressures on investments in the future. To its credit, cyber is one of the few areas in which the Defense Department actually increased its investments in the fiscal year 2013 budget request.

The objective of this hearing is to gain a better understanding of DOD's cybersecurity research and development activities and how these activities support DOD's cybersecurity objectives. We would like to better understand the research challenges facing the cybersecurity R and D community, the diversity of approaches to solving these challenges and gaps if they exist. And we would like to understand the interactions between DOD with other Federal agencies, such as DOE's national laboratories, industry, and academia.

We welcome the ranking member, Senator Portman.

The focus today will be on gaining a better understanding of mechanisms to rapidly develop, test, and field innovative approaches to address the expanding threat spectrum and whether appropriate coordination is present across all the various cyber research communities. In addition, we would like to address the status of DOD's cyber testing infrastructure as well as the health and status of its cyber workforce and DOD's ability to attract and retain the best and the brightest in the field.

This hearing is planned to have both open and closed sessions. We're pleased to have four expert witnesses to help us understand these complex issues. Mr. Zack Lemnios is the assistant Secretary of Defense for Research and Engineering, and in this position he is the Department's chief technology officer and oversees and coordinates that Department's broad cyber research portfolio across the Services and DARPA. In addition, Mr. Lemnios oversees the Department's efforts in science, technology, engineering, and mathematics education efforts, of which cyber is an important element. The subcommittee looks forward to hearing about the DOD's overarching strategies, plans, and programs in cybersecurity R and D.

Dr. Ken Gabriel is the acting Director of the Defense Advanced Projects Agency, DARPA. Created in the wake of the surprise launch of the world's first satellite by the Soviets in 1957, DARPA was created to prevent technological surprise to our Nation. DARPA is investing heavily in cyber-related research, with roughly $500 million requested over the future years defense program, and has developed some innovative approaches to addressing emerging cybersecurity threats.

I should point out that our original hearing notice listed Dr. Regina Dugan as the witness for DARPA. However, she is leaving DARPA for the private sector, and I would like to acknowledge Dr.

Dugan's contributions to DARPA and sincerely thank her for her service to our country.

Dr. Michael Wertheimer is the Director of Research and Development at the National Security Agency. The Director of NSA is also the commander of the United States Cyber Command, so NSA is an indispensable partner in cybersecurity efforts. The subcommittee looks forward to hearing about the research activities at the NSA and how they support DOD's cybersecurity objectives.

Dr. James Peery is the Director of the Information Systems Analysis Center at Sandia National Laboratories, a Department of Energy national laboratory at Albuquerque, New Mexico, and a source of expertise on cybersecurity. We look forward to hearing how Sandia's activities are benefiting the DOD.

I really want to thank all of our witnesses for your service in the cause of our National security, and we look forward to your testimony. In order for us to have adequate time to discuss a broad range of topics, I do ask that our witnesses keep your opening remarks to no more than five minutes each. But we will include your full written statements in the hearing record.

For the information of the members and our witnesses, I do want to indicate how we plan to proceed in light of the series of roll call votes scheduled at 4:00 o'clock today. We'll conduct the open portion of the hearing until we have to vote, and then we'll reconvene in Room SVC–217 of the Capitol for the closed portion of the hearing after we finish voting. And I think there's a series of three votes.

Before we hear from our first panel, I'd like to turn to my colleague and ranking member, Senator Portman, for his opening remarks. Senator Portman.

STATEMENT OF SENATOR ROB PORTMAN

Senator PORTMAN. Thank you, Madam Chairman. I appreciate your holding the hearing and look forward to the testimony from these well-informed and sophisticated witnesses, who can help us in a very important task.

But before I do that, I must mention that this Friday the Bobcats of Ohio University are playing the Tar Heels, and I would like in public hearing——

Senator HAGAN. Then we play NC State. [Laughter.]

Senator PORTMAN. We'll see, injuries aside. But anyway, since we beat number four seed Michigan, UNC shouldn't be a problem for the Bobcats. So we'll make a bet later, maybe chocolate Buckeyes and North Carolina barbecue sauce.

This is a great opportunity for us to hear from you. Again, I look forward to doing it. This is sort of the topic of the day. When you look at our budgets, you can see it. In a very tough budget environment, we see significant increases at DOD for cyber defenses, a $200 million increase from last year; Department of Homeland Security, $310 million increase from 2012. So, coupling these figures with the billions of dollars likely to be invested by the public or by the private side, private sector, universities and others, it's evidence that we have a serious concern here and it's now being acknowledged, and that we view ourselves as being vulnerable to cyber attacks.

These increases in spending do come at a time when we are looking at decreases in I guess what you call our physical defenses. One of the purposes of this hearing I believe is to be sure that we are balancing those two. We can't ignore the threats posed to the technological infrastructure by terrorist groups and other adversaries, rogue hackers, but we also can't win the battle, of course, in cyber alone. We've got to have both, and as we're downsizing our military are we becoming too reliant on cyber defense, is one question I would like to have us discuss today.

I think the answer, of course, is that our cyber capabilities should be complementing our kinetic forces and resources and make sure that we're working together.

With the kind of increase in funding we're talking about here, of course, there's also the potential for some wasteful spending and duplication. So knowing better what the private sector is doing, universities are doing, is important, too, and you have some great information there, I'm sure.

I've heard from some of you about your concern about the workforce and particularly with more and more young people not getting into subjects like computer science, which are critical to cyber capabilities. We've got to talk about how we be sure that we have a workforce that's capable of defending America in these new ways. The STEM disciplines is something we all talk about. How do we actually make that a reality and what are your recommendations there?

Then, as Chairman Hagan has pointed out, we've got to be sure we're properly coordinating across the Federal Government, because again we've got these new resources. Like all science and technology programs we invest in, we've got to be sure we're eliminating that duplication and having a synergistic relationship between various agencies and departments. Again, you'll be very helpful to us understanding how we do that.

This is just one more challenge we have as a country, isn't it? We've got to be sure that we're spending our limited tax dollars in a difficult budget environment in the most prudent way possible.

So this is a great witness panel—defense, intelligence, energy agencies—and we look forward to a frank assessment in both sessions today and a good sense of where you think our defenses are today and where we're going tomorrow.

So thank you, Madam Chair. I look forward to the testimony.

Senator HAGAN. Thank you, Senator Portman.

Secretary Lemnios, if you would like to begin.

STATEMENT OF HON. ZACHARY J. LEMNIOS, ASSISTANT SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING, DEPARTMENT OF DEFENSE

Mr. LEMNIOS. Yes. Good afternoon, Chairwoman Hagan, Ranking Member Portman. I have a short statement that I'd like to read and just leave my written testimony for the record.

Last year the Department issued its strategic guidance and strategy and operating in cyberspace. That defined cyberspace as an operational domain. It was a landmark point, and it defined the critical element of cyber operations as a concept to enable business operations, military operations, and the command and control backbone for the Department, critically important.

In fiscal year 2013, the President's budget request for the Department includes a $3.4 billion investment in cyber activities, of which $486 million is dedicated to science and technology investments. This investment is significant and critically necessary to give the Department a complex set of cybersecurity responsibilities and challenges. The responsibilities extend beyond our enterprise systems to 15,000 networks, the 7 million computing devices across hundreds of installations in dozens of countries around the globe which are used for business operations.

That capability has to extend to include the mission- critical command and control networks, our cyber physical systems, and our cyber radio frequency systems, our communications systems that make up the Department's tactical systems. The emergence of networked tactical systems and cyber physical systems have created new opportunities for increased cybersecurity attack and disruption.

When I think of cyber operations, I think of computer network defense of our enterprise IT systems and I think of computer network defense, attack, and exploitation of our tactical systems. In regard to mobile radio, a desktop terminal and an unmanned surveillance aircraft are all clients on our networks that need to be protected.

This is an operational domain built upon measures and countermeasures, where tactical depth, operational innovation, and technology transition are the key ingredients for leadership.

In mid-2009 we assembled the technology leaders from across government, industry, and academia to provide their insight into the fundamental challenges faced by the Department and the tactical approaches that are emerging in academia, precisely to the point, Senator, that you made regarding academia. We followed through on that insight and focused our cyber investments in four key areas. We focused on mission assurance, resilient architectures, agile operations, and foundations of trust.

Over this past year I've added an additional area, a cyber measurement campaign. All of these are described in my written testimony.

We realize the importance of ensuring the taxpayers' dollars are invested wisely and efficiently. We have the appropriate forms in place to ensure cybersecurity research is well coordinated among the Department's organizations, among other Federal activities, and across all of government. Investments are also scrutinized by the Department's senior leadership through the recently established Cyber Investment Measurement Board.

The key to success of all of our cybersecurity efforts is the talent, the workforce that we have in our laboratories, in academia, in industry, in our small business community, and the workforce of tomorrow. There are a number of programs under way in advance of cyber research and development workforce, and they are described again in our written testimonies.

Madam Chairwoman, thank you for the opportunity to present these brief remarks and I look forward to questions from the committee.

[The prepared statement of Mr. Lemnios follows:]

Senator HAGAN. Thank you, Secretary Lemnios.

Dr. Gabriel, if you'll go next. Thank you.

STATEMENT OF KAIGHAM J. GABRIEL, PH.D., ACTING DIRECTOR, DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, DEPARTMENT OF DEFENSE

Dr. GABRIEL. DARPA's role in the creation of the Internet means we were party to the immense opportunities the Internet created and we share in the intense responsibility of protecting it. While national policymakers will ultimately determine how cyber capabilities will be employed, DARPA's responsibility is to explore the outer boundaries of such capabilities so that the U.S. is best prepared for future challenges.

Chairwoman Hagan, Ranking Member Portman, members of the subcommittee: My name is Ken Gabriel. I am the acting Director of the Defense Advanced Research Projects Agency. DARPA's bottom-line message today is that DOD is capability- limited in cyber, both defensively and offensively. We need to change that.

It goes without question that a complete picture of the cyber threat should inform policies and laws related to DOD's cybersecurity efforts. Such decisions depend on a complete understanding of the threats and opportunities, an understanding that can be supported by our discussions today, but one that will remain incomplete. The complete picture requires a discussion at the special access level.

In this unclassified discussion, much of what we can share you already know. Attackers can penetrate our networks. Users are the weakest link in cybersecurity. The defense supply chain is at risk. Physical systems are at risk, and the U.S. continues to spend billions on cybersecurity with limited increase in protection.

Our approach to cybersecurity is dominated by a strategy that layers security onto a uniform architecture. This approach is taken for good reason, to protect against known threats and to create tactical breathing room. But it is not convergent with a growing and evolving threat. That's the defensive picture.

With respect to cyber offense, modern warfare will demand, as you said, Senator Portman, the effective use of both cyber and kinetic means. The tasks required for military purposes are sufficiently different that we cannot simply scale intelligence-based cyber capabilities and adequately serve the needs of the DOD.

Features that are vital for intelligence-based capabilities, such as nonattribution and persistence, are typically not as critical for DOD operational cyber capabilities. For example, a cyber exploit that always causes the target system to crash is not much of an intelligence exploit. But it may be exactly the effect that a DOD mission calls for.

DARPA activities are part of the larger effort within the whole of government at the NSA, the newly formed CYBERCOM, the services, and as appropriate DHS. DARPA's engagement in defensive and offensive cyber is not new. The agency's expanded efforts build on an existing foundation and continuing contributions to cyber. DARPA-developed technologies are widely prevalent in military, intelligence, and commercial use today, but there is still much to do.

From our vantage point, the greatest vulnerability in cyber offense for the DOD is the lack of capabilities with proportionality, speed, and diversity of effects.

Thank you.

[The prepared statement of Dr. Gabriel follows:]

Senator HAGAN. Thank you.

Dr. Wertheimer.

STATEMENT OF MICHAEL A. WERTHEIMER, PH.D., DIRECTOR, RESEARCH AND DEVELOPMENT, NATIONAL SECURITY AGENCY

Dr. WERTHEIMER. Madam Chairman, Ranking Member Portman: Thank you very much for inviting NSA Research today. NSA Research is unique in the intelligence community. Of all 16 components in the Office of the Director of National Intelligence, we are the only component with in-house research, a national government workforce that's dedicated to providing research. We do very little program management. We're supporting both the information assurance and the signals intelligence mission of the NSA.

We do that with a very, very highly skilled technical workforce, better than a third of which have Ph.D.s, another third masters, and just under a quarter have bachelor's degrees.

Our legacy is mostly in cryptography and in the design and breaking of encryption. Over the past ten years, in the living laboratory that really is the SIGINT system we have seen our mission grow in defensive cyber and offensive cyber. NSA Research is responsible for virtually all the major tool sets that we deploy both offensively and defensively. We're very proud of that legacy.

But I would be remiss in not sharing with you things that concern me most at night when I go to sleep. First, the production of computer scientists in our Nation is on the decline. I can share facts and figures with you. We are not recruiting and retaining them. There are things we can and must do to retain them that we are not.

I am concerned also that the investments from the Congress and from the people in research is almost all period of performance of one year or less that I see. It's to build tools, it's to be a rapid deployment of capability. I rarely get the opportunity to think three years down the line even in research. The money that comes to us has very directed purpose. I will tell you in closed session many of the wonderful things we're doing with that money, but I feel that the Nation is a little frightened to think much beyond one or two years on this problem, and that keeps me up at night as well.

Most of the examples I'd like to share with you in closed session, so I'll conclude my remarks at that point.

[The prepared statement of Dr. Wertheimer follows:]

Senator HAGAN. Thank you.

Dr. Peery.

STATEMENT OF JAMES S. PEERY, Ph.D., DIRECTOR, INFORMATION SYSTEMS ANALYSIS CENTER, SANDIA NATIONAL LABORATORIES

Dr. PEERY. Chairman Hagan and Ranking Member Portman: Thank you for giving me the opportunity to testify today. I'm James Peery, Director of Information Systems Analysis Center at Sandia National Laboratories. As you may know, Sandia is a multiprogram national security laboratory owned by the U.S. Government and operated by Sandia Corporation for the National Nuclear Security Administration, or NNSA.

Sandia is one of three NNSA laboratories with responsibility for stockpile stewardship and annual assessment of the Nation's nuclear weapons. But within the U.S. nuclear weapons complex, Sandia is uniquely responsible for assuring that U.S. nuclear weapons cannot be used without the President's intent. It's because of this responsibility that Sandia has had an extensive cyber research and development program for over 50 years, with a rich history of providing vulnerability and adversarial threat assessments for U.S. nuclear command and control systems.

Although nuclear weapons remain Sandia's core mission, it because of these capabilities has been able to support other agency missions in national security, including nonproliferation, counterproliferation, counterterrorism, Defense, Energy, and Homeland Security. In all of these areas, I think you recognize that cyber is a key element.

My written statement focuses on the questions you raised, including the challenges and technical developments in cybersecurity, along with how the Department of Energy laboratories contribute to the Department of Defense mission in cybersecurity. There are three points I'd like to emphasize:

Today the DOE laboratories are a resource to the DOD in raising the bar to our adversaries in cybersecurity. I am very confident that a large part of the DOD is aware of where the cyber talent lies or resides within the DOE laboratories and has effectively used DOE procedures to acquire that talent.

The second point is—and I think you're aware of this—there is no silver bullet to solve the existing cyber problem. That's true for DOD, DOE, and the private sector. It's virtually impossible to make an absolutely secure information technology system. However, with sustained and coordinated investments and deployment of government-owned science and technology, we can dramatically change the cost equation to our adversaries.

Third, compliance-based security is not effective. We need a set of metrics to objectively measure system security. New technologies and policies should be evaluated and adopted based on how they objectively improve system security and how much they cost. This is not a static process. The adversary will adapt.

Specific to the committee's requested questions: On the area of encryption versus network security, I would just like to point out that they shouldn't be viewed as competing alternatives. Better network security and careful use of high-quality encryption significantly raises the adversary's costs, but unfortunately today the driver in IT systems is cost reduction. Diversity is another way to increase the cost, but today again cost reduction is the predominant driver in IT.

The question of transition from signature-based detection of attacks to behavioral-based detection. I just point out—we can talk more in closed session about this, but new classes of anomaly detection methods have been developed and are based on aggregating events across time and multiple sources to identify network and host-based behavior that might be malicious. These approaches and behavioral-based methods have been successful in finding previously undiscovered malware. One drawback of this technology, though, is that it has a very high false positive rate.

I think I'll conclude my comments now on the issue of workforce within Sandia, which I can speak on and is near and dear to my heart. I believe, as was said earlier, confronting today's cyber challenges requires a highly skilled and motivated research community. It's well documented that the demand for cyber expertise greatly exceeds the supply.

At Sandia, through several enticement programs we've been able to attract and hire some of the top U.S. students, both at the undergraduate and graduate level. But I would like to draw your attention that retention is a growing concern. Although the importance of the National security mission and job stability remain highly attractive features to our employees, new hires today receive benefits similar to those found in U.S. industry, so we should start expecting that in this area that we might see retention rates approaching that of U.S. industry, which is approximately five years.

The reason this is a concern is that historically the laboratories have been asked to solve some of the impossible problems, and that requires a cadre of senior experienced staff members. Just like in nuclear weapons, the government level of resources in cyber—to get the skills to the level the government needs usually takes between 3 to 5 years. If the retention rate is around 5 years, then we have a growing problem of trying to keep those people around to solve the impossible problems.

Presently, many of Sandia's cyber staff are being solicited by private companies offering greater than 50 percent increases in salary and better benefits. We've been very fortunate that historically we've only been losing on the order of about less than one percent annually in the area of cyber, but this year we expect to reach approximately 10 percent loss in our staff to outside employment.

Just in summary, I'd say that the DOE labs complex has a deep reservoir of technical talent and science and technology capabilities that have helped address some of the government's most challenging national security problems, including the cyber area, and I look forward to the closed session to be able to tell you about some of those accomplishments.

Thank you.

[The prepared statement of Dr. Peery follows:]

Senator HAGAN. Thank you. Thank you all for your opening testimony. Now we will go to the questions, and I will ask that we will have 6 minutes each, and then if nobody else comes in you can certainly go longer.

The Department of Defense is facing challenges seeking new graduates with advanced degrees, and I think each one of you mentioned that in your opening testimony, specifically in scientific and technical fields to help develop complex military systems. The field of cybersecurity is a key example where there is a rising demand, as you just mentioned specifically in the private sector, too. Yet I think we all know it appears that the supply side is not keeping pace.

Secretary Lemnios, as the key person in DOD responsible for our science, technology, engineering, and mathematics education and outreach activities, how are you ensuring that the DOD is able to recruit and retain the best and brightest in cybersecurity research? And how are you monitoring the quality of DOD's cybersecurity research workforce? Then the final part of this question is: How much is a highly experienced, trained cybersecurity research paid within the Department?

Mr. LEMNIOS. Senator Hagan, I think through testimony and through our written material, I think we've all recognized that the workforce, the talent, is central to this entire discussion. As such, we have been shaping our STEM programs to include cyber as one of the disciplines that we're focused on. Our Smart program, our scholarship program which provides a year of scholarship for each year of service in one of our laboratories, is one example of many. In my testimony, my written testimony, I gave several of these.

This summer we will have roughly 600 students from that program entering the Department's laboratory infrastructure, and of those a significant number of them—I'll get back to you with the exact number—are in the cyber or related technology areas. I view that as one of a number of ways to attract young talent to pursue their work and to understand where their work will actually make a difference for the Department.

The challenge beyond that, though, is to track those students long term in competition with industry, in competition with other pay grades and other environments. I think you do that by, first of all, engaging those students in first-rate work—and you've heard from Dr. Wertheimer about the NSA piece of it. The same could be said with regard to the environment at Sandia.

I think you also engage those students in an environment where they can actually learn, where they are contributing and they have a mentor side by side that helps them increase their skillcraft and increase their game, and certainly putting students and those groups on a project that has national significance, and we're doing that through the Smart program and other programs.

Senator HAGAN. How about salaries?

Mr. LEMNIOS. I'm sorry?

Senator HAGAN. How about actual salaries?

Mr. LEMNIOS. I don't have the salary numbers. I'd defer to others that might have that, and we can certainly take that question for the record.

[The information referred to follows:]

[SUBCOMMITTEE INSERT]

Senator HAGAN. DARPA has taken some interesting approaches to hiring personnel from nontraditional areas, such as the hacking community, where these individuals might not have a doctorate in a traditional academic field. I don't know if they have a master's or a college degree. But what lessons has DARPA learned by tapping into this talent pool that may have applicability across the broader DOD spectrum? And then, what does DARPA has as far as the necessary mechanisms to rapidly hire talented cybersecurity researchers? And then how much are they paid?

Dr. GABRIEL. Three questions.

Senator HAGAN. The hacking community.

Dr. GABRIEL. The white hat hacker community I think has been instrumental in us beginning to understand the nature, the challenges and opportunities in cybersecurity, both defensively and offensively. And in particular I point to the Cyber Fast Track program, which I think we described to you briefly.

It was with the insight that we gained from recruiting from that community program managers that we understood that the connectivity to that community was very poor, not only for DARPA but the Federal Government overall. The time frame of contracts, the other things that typically go into reaching out to the research community from our perspective, was not well matched to the pace of business that they did.

Through the Cyber Fast Track program, which we launched last August, we have had 135 proposals, submissions, over that eight-month period, 87 percent of them, from innovative, nontraditional performers who have never done work for the government before. That was through a contracting mechanism that matched the speed and the period of performance.

Just to give you an example, 36 contractors were awarded. The average period of performance is five months. So if we don't have contracting procedures that are much shorter than that period of time, it makes no sense to take nine months contracting if they're only going to do 5 months of work. So the average time from submission to award has been 8 days, and we view that as a very vital part of getting the freshness, the innovation, and the perspective coming from that community.

Our program managers, you asked what are the mechanisms we have to hire them. As you know, ma'am, we have a culture where we essentially refresh essentially every three to five years. Program managers come to DARPA 3 to 5 years. They come to do their work and they leave, and that's true from program managers to office directors to the deputy director to the director, as you pointed out earlier.

That is the pace at which we believe you need to bring in the talent, to bring in the perspective and the sense of urgency.

We are paid just like any other civil service scales and other hiring authorities in the Department.

Senator HAGAN. Since I said we would limit it to 6 minutes, I'll hold the next two questions for the other two until it comes back to me. Senator Portman.

Senator PORTMAN. Thank you.

Thanks for that response. I guess I'd like to back up a little bit and talk about the budget. As I indicated in my opening and you have identified, there are areas where we're increasing spending. DOD's budget is one. Homeland Security is another. Despite this, Secretary Carter has said recently, Mr. Secretary, as you know, that we're not spending as much as we need to. He's also said we'd spend a lot more if we could figure out where to spend it.

So I guess I have two questions for you, and others feel free to chime in. One is, in terms of the budget levels, and as a former OMB director I know your answer is always going to be we could spend more. But honestly, are we spending enough? And then the second question, you can think about it, would really be to Dr. Gabriel's intriguing testimony, which is: We're spending more and yet there are more attacks; is that because there are just such an increase in attacks that the more spending and the more we throw against it, although we're having some impact, it's still resulting in a net increase in attacks? Or is it because we're not spending the money wisely?

So if you could start with the first question, Secretary Lemnios, and then if others could chime in with regard to both of those questions.

Mr. LEMNIOS. Senator, the question of the Department's funding level is something that we took head-on early last year. I was interested in actually two questions. First is what should the Department's funding level be for science and technology, 6–1 through 6–3, but also what should the content of that spend be?

It goes to your point: Are we funding-limited or idea- limited in some of these issues? We tried to parse that. We did it the following way. I spent between August 15 and essentially the end of October last year going through every project in the Department. I went through 270 program elements. I visited each of our laboratories. I visited DARPA, the services. I got a look at the project spend in dollars and content, what were the ideas that were being funded.

We rolled that up to compare it against the strategic guidance that was being developed at the time to try to understand where were the gaps in ideas, where were those areas that if we had a little bit more money they were ideas that were ready to be harvested vice if we have more money we'll just kind of peanut butter it to the right. I wasn't interested in the peanut butter cut. I was looking at strategic investments.

As a result, the President's budget request that's on the Hill now includes in it increases in targeted areas where we identified ideas and we identified concepts that would be ready for funding, that would be responsive to the strategic guidance of the Department.

Within that, one example, we looked at a new concept at the convergence of cyber and electronic warfare. We can talk about it in detail in closed session, but it was an area that it was clear to us was going to come about and we had good ideas that we could harvest in that particular area and get well ahead of a threat.

We also plussed up work in manufacturing and some other areas, and we identified those concepts. And we took funding out of some topics that we identified were either mature enough or weren't leading to a program of record that would be of critical importance for the Department. So we actually made those trades, and the trades were not in budget ceiling; the trades were informed by what are the ideas that we thought we could address. As you can imagine, that was a spirited discussion. But at the end of the day we put in the budget request those ideas that we thought would make that trade for us.

As far as network attacks, the question is at what point do we make investments in cyber network defense to the point we can curb network attacks? The way we're looking at that—and I think Dr. Gabriel has done some groundbreaking work in that area—is to identify where do we start changing the calculus for the work factor that an attacker presents as a function of how much work we have to put in to defending that attack. So we're trying to measure that, that calculus, and put concepts in place that in fact are non-convergent. They don't track with the work level of an attacker, but they actually fundamentally change the game. And we have some concepts again we can talk about in closed session that address that.

But the fundamental issue is identifying those areas that were funding-limited and those areas that were idea- limited, and I think we balanced that in the budget submittal that's on the Hill.

Senator PORTMAN. You covered most of those ideas? You feel these requests are adequate to cover most of them?

Mr. LEMNIOS. I think there were some others that we'd like to go back and take a look at, and we'll be reviewing those over time. But I think we put in place a balanced portfolio that covers some real long shots and some things that we can in fact make clarity on over the next year or so.

Senator PORTMAN. Dr. Gabriel, could you follow up on that, again in reference to your comment that we are, as I wrote here, capability limited on defense and offense, and that you see more funding and yet more attacks?

Dr. GABRIEL. Thank you, sir. I would specifically like to address the comment you made. I don't believe it's that we're doing wrong things. It's just the nature of playing defense in cyber that it's hard, and the analogy that we've used in the buying tactical breathing room, it's much like treading water. If you find yourself in the middle of the ocean, treading water is a good thing. You need to tread water to stay above, keep your head above water. But if that's the only strategy you have for getting out of the predicament, you will eventually get tired and become overwhelmed.

That's what we mean by taking advantage of the tactical breathing room, some of the work that we're doing today to protect us, the patching and the consistency of defensive measures. But if that's all we do, it is not convergent with the evolving and growing threat.

So we have articulated and begun to make and shifted investments over the last two years to make sure we're looking, not only at things that buy us tactical breathing room, but to actually look at aggressive programs that seek to become convergent with the threat, to change the game, so its' not the way it is difficult to play defense, and make it difficult, to change those asymmetries, to change the cost calculus for what it means to have an attack on a cyber system.

Likewise, I would say we'd be happy to get into some of the specifics of how we believe we can do that, given some of the investments we're making.

Senator PORTMAN. My time has expired, but I would just say that——

Senator HAGAN. You can take some more time.

Senator PORTMAN. Okay, I'll just take a couple minutes if that's okay and turn it to you.

Dr. Wertheimer mentioned earlier the fact that he's concerned that some of the spending is too short term. I don't mean to paraphrase you, but are you referring in part to the tactical breathing room approach? In other words, are you concerned that we're not looking long enough term? Or is it more that we are focused more on just retaining our current position rather than, as Dr. Gabriel indicated, looking at how to deal with some of these asymmetrical threats and being more creative?

What's your take on it?

Dr. WERTHEIMER. Senator, at the risk of pushing March Madness too far, we have to deploy a division 1 team because the adversaries are division 1 in most cases that the Department sees. Google, any of the headlines you've read, their first inclination was to attribute this to a nation- state adversary, one which in some sense they felt or implied that they couldn't be held accountable for defending against that.

It is my belief that we are rushing to this threat numbers, lots of attacks, and we're trying to deploy tools and techniques to slow that, and we aren't keeping our—in my view, we're not keeping enough of a strategic eye on that nation-state threat, that division 1 that's going to come at us and adapt to most of the kinds of tools and techniques that you're going to need to stop your routine—and routine doesn't mean it isn't important and it isn't scary—botnets and other large efforts.

Senator PORTMAN. And is it your sense that the numbers that are being requested would be adequate for us to think more strategically, so in other words, it's not so much a question of budgets as it is a function of approach?

Dr. WERTHEIMER. I agree exactly with that statement.

Senator PORTMAN. With regard to NSA, you also talked about what I mentioned in my opening about the production of computer scientists being on the decline. You said you had some information about that. We don't need it all today, but if you could provide that to the committee that would be very helpful, because, as we have discussed in previous hearings, there are various approaches and some involve more direct government action. Secretary Lemnios talked about some interesting ways in which you're encouraging more young people to get into the STEM disciplines and providing them an opportunity along the way.

There was discussion about whether it's advanced degrees that are needed or whether it may be something more fundamental, just to attract people into the field and then maybe help them to subsidize their advanced degrees.

Just what are your thoughts as to how to deal with what you identified as a major problem, which is a talent shortage?

Dr. WERTHEIMER. I agree that the seeding of more talent must occur. We have charts and I will share them with the committee gladly. Today, if you look at the number of Ph.D.s in 2010, that was 1,500 Ph.D.s. 720 were U.S. citizens or U.S. persons. 64 in total came to work for any form of government.

We are not competitive salary-wise. We tend to hire Ph.D. computer scientists at grade 12, step 7, which is about $90,000. The middle 50 percent of offers run 75 to 124,000 in the private sector. They come in at a 12, step 7, and they hit a pay freeze. The average increase in salary for a computer scientist in industry is 4 percent a year. We hit them with a pay freeze.

They come in as a 12, step 7, and they hit the pay caps that we have imposed upon us by the Department of Defense and particularly the Under Secretary of Defense for Intelligence issued a memo on the conversion to DECIPS, the pay banding that never happened, and it limits us to how many 13s, 14s, and 15s we may have as an agency.

The average time in grade if it was just fair-shared is 12 years to your first promotion, 12 years to your second promotion. You can't walk in and tell them you're going to wait 6 years if you're good, 12 years if you're average.

Just to give you another number—as a mathematician, I can't control myself—NSA—if you look at attrition across the National Security Agency, 44 percent of the people who attrite are resigning as opposed to retiring. In computer science it's 70 percent.

Senator PORTMAN. So you've identified—and I'll turn it back to the chair after I ask this last question. You've identified an obvious problem. Looking at Dr. Peery's testimony here, to bring him into it, he's talked about the DOE labs and all the cyber talent that's there. You talked about the retention issue. You said five years on average is not enough time to be able to plan and to be able to develop the kind of, I assume, both offensive and defensive capabilities that are needed.

What are some of your solutions? What would you do to try to both attract and retain? One would obviously be salary from what you said. If there are only 64 going into government, that may in part be because that range of 75 to 100 grand versus 60 grand is a disincentive coming out of school with a bunch of loans.

So I assume you would agree with that. And you talked about pay bands and you talked about—and we've done this in other agencies and departments and do it to a certain extent in your agencies, I know we do at DOD. But what are some other ideas that you would have for this subcommittee as to how to attract and retain?

Dr. WERTHEIMER. The first thing I would like to recommend is across the government in particular a STEM waiver for pay, for pay limitation. That is, I'd like to be able to promote to 13, 14, 15 based on merit if they're in a STEM field, especially if they're in an advanced STEM field. I think that would be a simple and exciting solution, to know that the government makes an exception for STEM and that there isn't a career ceiling.

We are expanding—we put out a three-year postdoc program at NSA precisely to attract new folks. Three years. We had 140 applications before we even advertised. This is something, they only are allowing me to get three. I'm only allowed to have three because it's a prototype, something we haven't done before.

I would like a great deal more of a sense of the Congress and others that we can experiment in the STEM fields in nontraditional ways. Give us some more latitude to bring them in for three years at a time, again promotions, pay. They love the work. The data we showed them, the challenges they have, they absolutely adored it.

Every one of them says to me on an exit interview: It's less about the money; it's the sense that I cannot advance in my organization; I simply cannot advance.

Senator PORTMAN. I'll turn it back to the chair, but maybe we could continue this conversation at least in a submission to the committee that would be helpful. It does sound like it's a matter of pay, but also because it is exciting work and some people are willing to take lower pay to do it and for their sense of service and certainly the National security area, but they also want the ability to be recognized and promoted through merit.

Thank you, Madam Chair.

Senator HAGAN. Thank you.

I think when we're talking about this, too, and we're talking about national security, we're talking about the new threat of cybersecurity as the next terrorist activity, that it really concerns me that we're limited in pay scales, promotion scales, because when I look at what the alternative is, the private sector that is also desperately trying to attract the same talent, I think it is an issue of national security that we do need to address.

Dr. Wertheimer, you answered some of the questions that I was going to raise for you. But when you specifically mentioned the point about personnel policies that are not conducive to hiring and retaining the best and brightest cybersecurity researchers, I was wondering if you could elaborate, or Secretary Lemnios, on what we need to do to change that? Secretary?

Mr. LEMNIOS. Sure. Let me try to recenter some things and add a little bit of sunshine to something that is a very difficult problem, and that is how do we attract talent for new areas. While NSA has a remarkably talented research laboratory second to none—and Mike and I have spent a lot of time there and I love spending a day there or longer—the bet that we're making in the Department is that it has to be a balance between what we have in terms of internal resources, those concepts that we see from industry, from academia, and from our government laboratories. So when I look to drive early stage innovation, some of that will come through our laboratories, some of that will come through captive laboratories, but we're really trying to make a bet with how we can increase the pace of innovation and drive technical concepts through the small business community, through the rapid innovation fund, through other channels, through contract research and development agreements that couple our laboratories with early stage developers. The DARPA experiment of nontraditionals is absolutely superb.

Much of that we can do with our existing authorities. As one example, we talked, we spoke last week about the rapid innovation fund. We received 3500 proposals from the small business community in that area in a fairly short-notice set of broad agency announcements. Some of those in fact were targeted to address cybersecurity concerns, wireless security concerns.

We're going through that source selection now. But it seems to me that that's an environment that taps a community that wasn't engaged in this discussion earlier, and it's one that I think we'll see lots of good ideas from with enormous leverage.

So when I think about our investments in STEM, absolutely we need to strengthen the Department's position in our laboratories and in the core workforce of the government. But I'm also looking at how do we strengthen the skillcraft and the game of industry and of academia as we move into these new fields. I think we've started along that path.

Senator HAGAN. But, Secretary, how can we change the policies as far as the freeze on pay and the freeze on advancement? I mean, I think if you've been told—is it 12 years, 6 years, 12 years? I think we'll be losing those people to be contract employees.

Mr. LEMNIOS. I don't have a comment on that. I just don't have a suggestion at this point.

Senator HAGAN. Dr. Peery, if you could just comment on hiring and retaining? And you mentioned it in your opening statement, but how much is at highly experienced, trained person at Sandia paid?

Dr. PEERY. I probably don't have exactly the numbers that you need, but we could get that to you. What I will say is that we're able from an initial offering to compete with U.S. industry for starting salaries, and I can give you those numbers.

[The information referred to follows:]

[SUBCOMMITTEE INSERT]

Dr. PEERY. Where we run into problems is, because we are under a GOCO model, the government has a say in what kind of raises we can provide to the workforce, and because of that we've seen significant salary compression in this area over the last five, maybe ten years. And because of that, that's what's starting to drive people out.

We're not quite in the same restrictions with regard to promotions that mike spoke about, but we do have somewhat of a promotion policy. I'd hate to see us accelerate that just for the sake of retaining people. It's really supposed to be performance-based. But we don't have any artificial limits on that.

Like I said, we are able to attract people to the laboratory because of the very challenging work that we can offer them in cyber, the fact that we have certain resources that we can train them up and get them some really special skills. Then if we can work on that work environment, I think we could have a better retention policy. We're not within the Department of Defense. We're within the Department of Energy. I think you can go—you probably heard of the latest National Academies study on the work environment within the NNSA laboratories, led by Dr. Shenk. That's pretty much a good description of exactly what our workforce is seeing today.

Senator HAGAN. It appears to me that the DOE is paying considerably more than DOD in hiring.

Dr. PEERY. I think our initial salaries are considerably more. Our initial salary for a computer scientist Ph.D. is $115,000. For a master's it's $95,000. Some of the enticements we have been able to offer is we can give very top undergraduate U.S. citizens, out of an undergraduate program and after a year of service send them to a school of their choice to get their master's degree. In that program we provide them 75 percent of their salary while they work on their master's degree and then they owe us two years of service back.

Senator HAGAN. So not only is DOD competing with the private sector; they're also competing with our own DOE laboratories. So I see a conflict here, obviously.

Dr. Gabriel?

Dr. GABRIEL. I'd like to just make an observation, perhaps from a different perspective. The shelf life of cyber capabilities is short. I think we've all heard that, and we understand that. We might even posit that the shelf life of cyber skills is relatively short. So this might create opportunities for us where there would be a core subset of folks that we would want to retain, but in fact perhaps that we should just plan on building a model where there will be a significant refresh of folks coming from the cyber community.

This is a community where the traditional metrics of a master's degree or a Ph.D. may not be as important. Half of our so-called cyber punks, the group of about a half a dozen or eight program managers at DARPA, don't have Ph.D.'s. Their skills, their capabilities, their insights, are coming from their practice in the community. And frankly, it will have a shelf life. They'll go through the 3 to 5 years and then they'll move on and others will come in with a newer, different perspective.

I think that's an interesting thing about cyber. That's the perspective, that it has such a fast refresh and a short shelf life that we may have opportunities for a different model of how we retain that capability.

Senator HAGAN. That's a valid point, but I also think the mentoring aspect in some of these other areas certainly plays a role. You do need some time for that.

Let me move to another area, and that is the cyber ranges. These are physical and virtual networks that can be used across the spectrum for research and development to the test and evaluation of new technologies, to providing the real-world environment for training. I understand that DOD does not perhaps have a complete inventory of all of the cyber ranges dispersed through military commands and services.

I'd like to ask all of you, what cyber ranges does your agency use? Are they adequate and could they be improved? Secretary Lemnios?

Mr. LEMNIOS. Senator, the concepts that are being developed in cyber are emerging, as are the testing and the way we evaluate those concepts. The Department currently operates 60 ranges total. We can give you lat-long locations for these. We know where they are. We know what they're connected to.

But some of these ranges in fact are operational. Some of them are training. Some of them are actually system testbeds for particular systems, they're targeted for a particular system. We have, for example, a test environment for the Joint Strike Fighter that's targeted exactly to support that one system in all of its complexity. We have similar testbeds for those as well. Sometimes those are called ranges as well.

Last——

Senator HAGAN. Is that included in the 60?

Mr. LEMNIOS. It is, it is.

There are roughly 11 or so ranges that are configurable in some fashion to do network assessments. There are some ranges that integrate classic network and RF capabilities. So it's a broad scope.

Last week I had the opportunity to visit the DARPA cyber range with two of the DARPA program managers—one of the DARPA program managers and an office director. And I had an opportunity to spend a day down in Orlando looking at what's called the National Cyber Range. What was interesting for me there was really two points. The first is that that was the first demonstration of how we could build a range that is separate from the network, that could be isolated and cleansed once a malicious attack is embedded in that environment.

It's also—it also had a very unique approach that allowed us to compose testing in a very natural way. We could build a test environment in software and actually run tests in parallel.

As I looked at that, the question was, well, how do we translate the results of that. I think what that's telling us is a way that we might think about operating some of our other ranges, and we're certainly taking that lesson now.

So we're operating these as a way to validate new concepts, and I think that work will certainly continue to be critically important.

Senator HAGAN. Dr. Gabriel?

Dr. GABRIEL. So let me start by answering your question about—our performers in general use a variety of different test ranges. But since Zack mentioned the National Cyber Range, I think it's important to point out that the focus of the cyber range was to develop the architecture and the tools that could be demonstrated and used elsewhere, and we've just begun to do that.

This last year of our involvement, of DARPA's involvement in the cyber range, is to take it through its operational test phase and sort of shakeout. But already we have had the two key elements demonstrated, which are multiple classification levels, so everything from unclassified to Top Secret, as well as rapid and cost- effective reconfiguration and cleanup.

We have had two operational tests, I think, since December. We had one in December, one in January. Both of them have shown the ability to take a system, configure it, do the test, and then tear it down for the next one and completely clean it from the previous one. We've taken that cleanup time from what would normally take months to days, so increasing the pace at which testing can be done as well as the range of classifications that that testing can be handled at.

Senator HAGAN. While we're on that subject, I understand we spent about $140 million I preparing this range.

Dr. GABRIEL. Over about 3 years, that's correct.

Senator HAGAN. I wasn't quite sure how many years.

Dr. GABRIEL. Yes.

Senator HAGAN. And that it's intended to transition I some manner to U.S. CYBERCOM. Can you give me the status of that transition plan, and have you received confirmation from General Alexander about taking over that for U.S. CYBER?

Dr. GABRIEL. Well, we've been working with CYBERCOM and in particular General Schmiddle, who is the deputy. In fact, one of the two tests, operational tests that we're talking about, was done by

U.S. CYBERCOM. They were using the test range. So we are continuing the discussions and we are—we believe that that will be our transition path.

Senator HAGAN. Once again while we're on this, Dr. Wertheimer, do you know—what's your thoughts on whether U.S. CYBERCOM will become the day to day owner and operator of this range? And are the resources adequate to continue maturing the range capabilities?

Dr. WERTHEIMER. I'm afraid, Senator, I have no knowledge.

Senator HAGAN. Okay.

Mr. LEMNIOS. Senator, if I could just add one thing. I think when we talk about continuing that range as an entity, I view the real value of that range as the architecture that was demonstrated and the software that's now been developed, for which the government has intellectual property and can be—so it's really the control and the design and simulation layer that's been demonstrated on that range, that we can now apply to other ranges.

Whether or not we use that cluster of processors and memory, that's interesting, but the real nugget there is the control architecture that's been demonstrated, how we can apply that to the Department's ranges for reconfigurability, for multi-level testing. We're going through that assessment now.

One path would be to in fact use the range that exists in Orlando as one of the Department's ranges. Another path would be to say, well, let's declare success on that, it was a DARPA project, it demonstrated the IP; let's take that IP and then apply it to other ranges that the Department operates globally. And we're looking at the trades between those two and I can see value in each of those paths.

Senator HAGAN. Evidently our first vote has started. Do you want to take five more minutes?

Senator PORTMAN. Yes. Let me just, if I could, follow up on a couple things that have been said. Great questions and appreciate the answers, and go back and ask a fundamental question here in the open session about what are we able to do.

I thought it was interesting, Dr. Peery, in your comments you twice said that you believe that we can dramatically change the equation for our adversaries. And what you meant by that was the cost equation. In other words, we can do things to make it more costly for them to hack into our systems or to attack through cyber, maybe cyber and electronic warfare.

But you didn't say that we can stop them. And in open session here—maybe we can get into this more in closed session—what do you think of that as a general matter? Is this a question of making it more costly, and if that's the case do some of our adversaries have resources to be able to circumvent whatever defenses that we are putting in place if they have adequate resources?

Dr. PEERY. Let me just make a global statement that we are in an environment of measures and countermeasures. It's no different than electronic warfare. It's no different in some cases than kinetic warfare. We will build capabilities, we are building capabilities, that put the adversary at risk. In some cases they're designed to put the adversary in a position where they are more vulnerable, and protect our equities in large areas.

But you've also got an adversary, certainly nation- state adversaries, that are doing the same thing. And then you have another community that's doing the same thing for other reasons. So it is—this is not an environment for which we can say there are zero defenses and zero consequences. There's always going to be a probability to detect, false alarm rate curve that we've got to think through. We've always got to think through what's the consequence of our action, what's the likely response, and how do we define what that redline actually looks like. We can talk more about that in closed session.

But it will be—it certainly is an environment where for every concept that's deployed, a countermeasure is deployed by an adversary. You see this in your private lives. We see this in our private lives with nothing more than the firewalls, now the embedded network systems that we all have on our private systems. And those have matured over time.

For each of those maturations that have occurred, additional levels of attack and sophistication have come into play. Now it's no longer just your desktop system; it's now your mobile system. And now the attacks aren't just spam attacks. They are tailored to your actions. So it's very much an environmental—Dr. Wertheiemer and I have talked a lot about this. It's very much an environment where we have to continually up the game and get ahead of the threat.

The last thing I'd point to is we started in computer network defense years ago with a perimeter defense strategy, a firewall strategy. We then moved to an environment where we have on the commercial side embedded agents that look at network traffic. Eventually, we're moving to a point where no longer will we be looking for particular attacks, but we will be designing systems on the commercial side that actually morph autonomically, actually change their features and change their operating roles, to respond to threats before those threats present themselves.

The private sector is working in that domain. Every one of these is a plateau, but that doesn't actually end because you've got an adversary that's working to counter each of those.

Senator PORTMAN. Speaking for Dr. Peery, who I'm going to ask to speak for himself in a moment here, when he says we can dramatically change the cost equation for our adversaries, I perhaps misunderstood that to have it mean a cost in terms of a budget and a commitment of resources to it. What you're referring to, at least from what I infer from what Secretary Lemnios is saying, is that the cost is sometimes the countermeasure. In other words, that if someone or some nation-state chooses to engage in this, there is a resource cost, but there's also a potential cost to their security. Is that what you were referring to?

Senator HAGAN. Let me interrupt. I think we have about four minutes and then we'll need to adjourn——

Senator PORTMAN. We're in open session here——

Senator HAGAN.—and go to the closed session after the vote.

Senator PORTMAN. If you'd rather talk to this in closed session or you feel you need to, I understand.

Dr. PEERY. I think I can answer this fairly quickly. First, it's not an "or." It's both. It's both the countermeasures and it's actually their cost of doing business. And I just want to—I think we've got the wrong mental model here. I don't think we would think that we could keep spies out of our country. I think we've got this model for cyber that says we're going to develop a system where we're not attacked.

I think we've got to go to a model where we assume the adversary is in our networks, it's on our machines, and we've got to operate anyway. We've got to protect the data anyway. That's where I think the research needs to be headed, is assuming they're in our systems, because if they're not doing it by coming through an Internet gateway then they're going to do it through supply chain. There's where the costs increase significantly.

Senator PORTMAN. Thank you. A sobering end.

Thank you Madam Chair.

Senator HAGAN. For sure.

We will adjourn and then after the vote we will resume in closed session. Thank you.

[Whereupon, at 4:12 p.m., the subcommittee adjourned.]