Homeland Security Advisory Council
Public Conference Call to Deliberate/Vote on
HSAC Task Force on CyberSkills
October 1, 2012 4:00pm EST
Meeting Minutes

PARTICIPANTS:

Judge William Webster	Ambassador James Jones
Governor Matthew Mead	Larry Cockell
Norman Augustine	Mohamed Elibiary
Leroy Baca	Ellen Gordon
Wilson Livingood	John Magaw
Bonnie Michelman	Jeff Moss
Annise Parker	Ben Shelly
Lydia Thomas	

Judge Webster: Thank you very much. Good afternoon. This is William Webster, Chairman of the Homeland Advisory Council, and I hereby convene this meeting. This is a public meeting of the Advisory Council and we appreciate those members of the public, the government, and the media who have joined us today.

I also would like to welcome the members of the Homeland Security Advisory Council and the members of the HSAC's Task Force on CyberSkills, who are on the call today. Our purpose today is to be briefed and deliberate on the recommendations from the Task Force on CyberSkills.

The Task Force was helmed by co-chairs Jeff Moss of ICANN, and Alan Paller of SANS Institute. On behalf of HSAC I thank all of the members of the Task Force for all your efforts, the subject matter experts for their input, and the Transportation Security Administration that hosted their meeting this summer.

I'll now turn the floor over to Jeff Moss, who will provide brief introductory remarks prior to turning the call over to HSAC's Member Alan Paller, who will brief the HSAC on the report. Jeff, proceed.

Jeff Moss: Thank you, Judge. I'd like to invite Alan Paller, my co-chair on this task force to provide his introductory remarks at this time. Alan?

Alan Paller: Thank you Jeff and Judge Webster. I'm honored to be here with the HSAC. About 115 days ago on June 6, Secretary Napolitano announced the formation of a Task Force on Cyber Skills. And she gave the task force two mandates.

The first was to find ways that DHS can foster the rapid development of a national work force, capable of meeting current and future cyber security

challenges, and the second, just as important, to outline how DHS can improve its capability to recruit and retain the very sophisticated cyber security talent it needs for its mission.

And the Secretary gave the Task Force broad access inside DHS, to both existing Department efforts as well as proposing what still needs to be done. The report identifies models and resources throughout government and the private sector that will enable action to meet the cyber skills mandate.

I believe if they are implemented, and I think the entire Task Force believes this as well, the recommendations will not only expand the national pipeline of men and women with advanced cyber security skills, but will also enable DHS to become a preferred employer for the talent produced by that pipeline, positioning the Department to help make the United States safer, more secure and more resilient.

I was very pleased and honored to work with Jeff Moss as his co-chair, and I'm going to turn it back over to Jeff, who is a member of the HSAC to take you through the report in greater detail.

Jeff Moss: Great, thanks Alan. The Task Force sought to identify both the short and the long-term recommendations that the Department could make. Some of these recommendations the Secretary could act on immediately, while others will take further planning and resources.

We organized this whole project into five over-arching objectives, and then in each objective we had supporting recommendations. So what I'm going to do is I'm going to go through the five objectives one at a time, talk briefly about the types of recommendations that would be used to support them, and then we'll move on to a questions and answers session.

The first objective was to ensure that people given responsibility for mission critical cyber security roles, and tasked at DHS, actually have the ability to demonstrate that they have proficiency in those areas. So we're moving to a model where people have to demonstrate critical skills.

The first three recommendations dealt with adopting and maintaining the list of what is considered mission critical tasks, and the skills necessary to support them, developing a training scenario that will allow the Department to evaluate the staff in each of these mission critical tasks, so we know their proficiency level, and then adopting a sustainability model that assesses the competency and progress of the existing and future mission critical work force, giving them a ladder or a career path that they can see.

This should help them in their career development planning. The second objective you'll notice was to help DHS employees develop and maintain

advanced cyber security skills, and to provide a high class work environment to help support the Department's recruiting efforts. This means Objective 2 was a two part recommendation.

And it dealt with developing a new Department-level committee, and this committee would be charged with the developing and overseeing the cyber security work force, improving the hiring process and making mission critical cyber security jobs for the federal civilian work force more enticing in every dimension.

This would include services, skills, growth potential, sort of creating a total value proposition, so that if you were being attracted to work in the DHS environment, you would know what you're getting into from a career development standpoint: skills, expectations, and what your requirements to meet certain job descriptions and titles are.

The third objective we had dealt with was rapidly expanding the pipeline of highly qualified candidates for these technical mission critical skills - jobs within DHS, by establishing innovative partnerships with both community colleges and universities, and organizers of cyber-related competitions, puzzles and other federal agencies.

So the recommendations in this section included establishing a two-year community college-based program that identifies and trains a large number of talented men and women. And the idea is raising the eligibility criteria for universities and colleges, in determining the national centers of academic excellence and scholarship for service for the SFS schools, and to ensure that the graduates are prepared to perform technical missions upon graduation.

So this would include launching a major sustained initiative to enhance the opportunities also for veterans to be trained and hired for mission critical cyber security jobs. Now, we can talk about this a little bit in detail later, but in essence what we're asking the SFS schools to do is increase their threshold and notch up their requirements. We hope that this would then better produce people with hands on skills, capable of entering the DHS workforce immediately after graduation.

Second, the Task Force focused on improving their criteria for four-year cyber security degrees, and called for more innovative partnerships with universities regarding outreach, including internships, with the goal of developing a pipeline of qualified cyber-security people so we can better develop and hire them into the workforce.

We also wanted to call out and identify community colleges and the military as good outlets for rapidly developing a large number of highly skilled cyber

security professionals. We view those as two promising outlets for finding future talent.

And the fourth of the five objectives that was proposed by the Task Force is to have the Department focus most of their immediate recruiting efforts in cyber security on hiring, training and human capital development, ensuring the Department builds a team of approximately 600 federal employees with mission critical skills.

We set this target of 600 technical specialists based on comparison with other large financial organizations and government agencies such as the Department of Defense (through interviews), but we anticipate that the number that will actually be needed will be adjusted when the Department completes their enterprise-wide review that is currently under way, and that will determine the numbers and competencies of its existing technical workforce, and its future and current workforce requirements.

So you can almost think of the 600 as a temporary placeholder until the Department completes its review. Specifically, the Task Force requested that the Department apply a large majority of its direct hire authority related to information technology to bring on people with mission critical skills, as well as specifying the mission critical skills and levels of proficiency needed during contracting procedures.

We felt that the standards we proposed to apply to the federal full time workforce should also be applied to the contracting workforce, and the newly developed descriptions of critical skills should be used to inform the contractor hiring process.

The fifth and final objective we dealt with was the establishment of a Cyber reserve program to ensure a cadre of technically proficient cyber security professionals is ready to be called upon in emergencies, specifically (unintelligible) two things. The first was an immediate establishment of a pilot DHS Cyber Reserve program that ensures that DHS cyber alumni and other talented cyber security experts outside of government are known and available to DHS in times of crisis.

This critical skills directory could be coordinated with other cyber-related task forces such as the Electronic Crimes Task Force to help in an emergency. Knowing who the experts are and how to reach them would save valuable time should there be a national emergency.

The second and longer term recommendation is in the area of the next 90 days: have DHS form a working group to determine how this program may be implemented long term. And we recommend exploring such questions as: how large should a Cyber Reserve program ultimately grow? What would a call-up

of this reserve look like? What is the business case for such a reserve? Does Congress need to grant DHS new authorities to create such a reserve program?

So those are our five recommendations. But before I turn the call back over the Judge Webster I want to ask HSAC Member (Larry Cockell) if he has any additional observations about what the report that he would like to add. I know (Larry) was instrumental in several of these areas, and without his input, our recommendations would have looked slightly different. So (Larry), you have anything to add?

Larry Cockell: Thanks Jeff. I'd like to make a couple of brief remarks about the approach that the Task Force undertook to reach these objectives and recommendations, and to note that we were mindful at all times that it made sense to look for existing models and resources already in government that could be leveraged to help satisfy some of the cyber skills requirements identified by the Secretary.

On Objective 5, this developed late in the deliberations of the Task Force, the concept of creating a Cyber Reserve surfaced as a viable opportunity to address several areas identified in the Secretary's tasking, primarily, how can DHS collaborate with the private sector to create a secure and resilient cyber space?

And she also proposed that we identify ways in which the federal government can productively engage academia and the private sector to maintain a vibrant exchange of cyber expertise. Having spent a number of years in government and now being in the private sector, I found this to be a viable option to pursue, and understand more intimately now that I am in the private sector the value of partnerships in solving some of the Homeland Security's missions.

So with so much of the nation's critical infrastructure managed outside of government, this Cyber Reserve would create a mechanism to tap into the expertise resident in the private sector, and significantly enhance the Department's capacity to quickly respond to cyber threats that could cripple our critical infrastructure.

The Cyber Reserve promotes the Department's philosophy on forging strong partnerships. It would offer substantial rewards in the form of improved information sharing about sensitive cyber risk, build a roster of industry experts who would be accessible to the government in time of need, and recognize there is a real benefit to maintaining contact with cyber security professionals transitioning from government roles to the private sector, so that the government shouldn't lose that expertise simply because the jobs change.

The Task Force report also outlined, as Jeff said, an existing network in 25 metropolitan areas around the company, as a platform that could serve as a low cost rapid deployment launch pad for the Cyber Reserve program. DHS

components currently participate in Electronic Crimes Task Forces that are strategic alliances of private industry, academia and other local, state and federal law enforcement officials working together to protect the nation's critical infrastructure.

The concept of the working group was to explore it as a viable option based on the time that this recommendation surfaced in the Task Force's work, and I hope the Department pursues that as an opportunity. Jeff, thank you and thank you to the Council for an opportunity to make these remarks, and I'll turn it back over to you.

Jeff Moss: Thank you, Larry, for your input. Yes, that was a pretty exciting recommendation at the end there, and I really hope to take the ball and run with it, because I think there's a lot of long-term benefit to be had. Okay, at this time I'm going to hand the call back to Judge Webster, who will move us into a question and answer phase.

William Webster: Are there any questions on the recommendations before we proceed to voting on the recommendations? This is, in other words, the Q&A period, and this is your opportunity to ask questions. So please identify yourself and go forward.

Matt Mead: Judge Webster, this is Matt Mead.

William Webster: Yes, Governor.

Matt Mead: And I want to compliment the Task Force for their work and their thoughts. Certainly they - it's apparent they put a lot of thought and effort into this. I do have just a couple of questions. One is, as I look through the five objectives, it looks like there may be some significant cost associated with that, and I don't know if that has been fleshed out yet or not.

And then along with that, one comment struck me: that DHS will be so supportive that qualified candidates will prefer to work at DHS. And I'm wondering how that plays in the larger picture with federal law enforcement, Secret Service, FBI, and the Department of Defense.

In other words, is DHS competing against those folks for these types of positions? Is there an opportunity to share some of this plan with other agencies as well? We certainly need these folks. There's no question about the importance of it. So that's the first question.

The second question is, I think that reaching out to the private sector is a grand idea, and very useful in a number of different ways. I was just wondering how that would work in times of a crisis. Would those folks have security clearances so they could immediately come on board, how that will practically work.

And perhaps the Task Force hasn't ironed all that out, but any comment on that I would be interested in. Thank you, Judge Webster.

William Webster: Thank you, Governor. Which of you gentlemen would like to take that one on?

Jeff Moss: So why don't I talk initially about the cost, and then I think we'll divvy out the questions to Alan and Larry.

William Webster: All right.

Jeff Moss: On the first issue of cost, we explored that initially, and our goal at the beginning was to try to be revenue neutral. And then as our recommendations were further refined we realized that was not going to be possible. And so yes, there is a cost associated with attracting and retaining top notch security talent.

And this goes to your second point of what is the level of competition between DHS and other federal agencies. And there are definitely federal agencies that compete better than DHS does. And part of the goal of this report is to make DHS competitive with others, such as the private sector and NSA in particular.

And I'd like to have Alan providing his input and Larry talk about how we view reaching out in a time of crisis.

Alan Paller: I would just add two little pieces to what you were talking about. The most important one I think was in our charter from the beginning, and that is, our job was not to fix the DHS cyber security manpower problem at the expense of anyone else.

It was first to build a national pipeline so large that DHS could get its share, but others will also be able to partake in that pipeline, because DOD and the banks and the power companies and the state and local governments are having exactly the same problem recruiting the top technical talent.

So if the development of the pipeline works well, DHS will get its share but it will, in fact, build such a large pipeline, (in the thousands) and in fact, over time in the tens of thousands of that, even though DHS will get a share, so will the others who need it. And that brings up the cost.

We wanted to - we didn't see a way for DHS to pay for all of that. And so we spent a lot of time with other agencies that had compatible goals. And for example the Department of Veterans Affairs is extremely interested in using its post-911 GI bill resources to ensure that veterans get access to advanced

high-velocity education so that they can take on many of these jobs, and similarly the Labor Department's program for trade adjusted support for education of workers, they're very interested.

So I think the costs are real, but I think the costs are covered by money - the costs for the development of the pipeline are covered by money that is already out there that hasn't necessarily been going to the cyber security jobs, that might have been going to other jobs.

Jeff Moss: Larry, did you want to talk about how we envisioned this would work in a time of crisis?

Larry Cockell: I'm happy to, Jeff. One of the key aspects of thinking through this Cyber Reserve would be to understand that the expertise to manage a cyber emergency would likely be resident in the private sector. And if the government could tap into those resources, in a manner that recognizes they are probably the individuals most familiar with the impacts on their industries, and the recovery requirements after an attack on our critical infrastructure, it would accelerate the government's work to respond and appropriately contain an emergency.

The question about security clearances was one that we also tried to envision, Governor, and one of our first target pools was people leaving government. And because we recognize it's a highly competitive space to be technically proficient as a cyber security professional, of when leaving government, those people will take skills that potentially were developed in government and take them to the private sector.

And in return, if we could convince them to lend their resources, or their abilities back to government in a national emergency, the benefit to the government would be to have an accessible pool of experts, and at the same time, as they leave government, their security clearances could be extended.

For those individuals who do not transition from government with security clearances, a number of them, through collaborative efforts already have security clearances, and those who would be interested in lending their services or expertise to government in an emergency would be granted security clearances.

We also thought through the burden of government maintaining security clearances for people who operate in the capacity of a Cyber Reserve. So there would need to be an agreement that they would be accessible to the government through a roster that could be developed, similar to one that's already maintained in the Electronics Crimes Task Force environment.

It would be a mastery of skills inventory that their proficiency would either be recognized in advance, or they could demonstrate their proficiency in order to be granted the security clearance.

Matt Mead: Judge, thank you and thank you for the response from the folks. Thank you.

Jeff Moss: Are there any more questions?

(Silence)

All right, Judge, it doesn't look like there's any more questions.

William Webster: Any last minute questions?

(Silence)

At this time I'd like to ask the HSAC to move to approve the Task Force on Cyber Skills Recommendations Report, and transmit it to Secretary Napolitano.

All member of the HSAC in favor of adopting the report, please say aye.

HSAC Members: Aye.

William Webster: Any members opposed, please say no.

(Silence)

Very well, by voice mail vote it is unanimously adopted. Now we're going to bring this public session to a close. Members of the public who would like to provide comment, that includes the media, provide comment to the Homeland Security Advisory Council, may do so in writing, by post to The Homeland Security Advisory Council, U.S. Department of Homeland Security, 1100 Hampton Park Boulevard, Mail Stop 0850, Capitol Heights, Maryland 20743, or by email at HSAC@DHS.gov.

Those comments are appreciated, and they will be reflected in the meeting's minutes. Thank you for your attendance. I declare this October 1, 2012 meeting of the Homeland Security Advisory Council adjourned.