

ONE HUNDRED FOURTEENTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
COMMITTEE ON ENERGY AND COMMERCE  
2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115  
Majority (202) 225-2927  
Minority (202) 225-3641

March 27, 2015

Dr. Gregory E. Shannon  
Chief Scientist  
CERT Program  
The Software Engineering Institute at Carnegie Mellon University  
4500 Fifth Avenue  
Pittsburgh, PA 15213-2612

Dear Dr. Shannon:

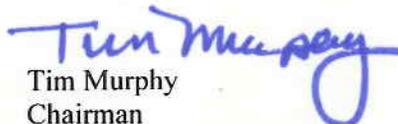
Thank you for appearing before the Subcommittee on Oversight and Investigations on Tuesday, March 3, 2015, to testify at the hearing entitled "Understanding the Cyber Threat and Implications for the 21st Century Economy."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Friday, April 10, 2015. Your responses should be mailed to Brittany Havens, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, D.C. 20515 and e-mailed in Word format to [brittany.havens@mail.house.gov](mailto:brittany.havens@mail.house.gov).

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Tim Murphy  
Chairman  
Subcommittee on Oversight and Investigations

cc: The Honorable Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations

Attachment

## Attachment 1—Additional Questions for the Record

### The Honorable Tim Murphy

1. Each witness provided a slightly different perspective on cyber threats and the challenge of cybersecurity, extending from the past, to the present and future.
  - a. Are there areas where you feel there is a common view or shared theme and what is it?
  - b. If there was one fundamental message you want Congress and the public to understand about cybersecurity, what would it be?
  - c. Are there specific issues or areas of this issue that do not receive an appropriate level of attention?
2. As the promise of innovation connects more of our lives to cyberspace – from smart pacifiers to cars that communicate with each other – cyberspace becomes, in theory, a limitless attack surface.
  - a. How do we manage the risks presented by “smart devices” and the Internet of Things while also enjoying the benefits and convenience they offer to society?
  - b. As more devices connect to cyberspace and interact with one another, what challenges does this present for how security professionals or companies anticipate potential vulnerabilities or risks?
  - c. How do we assess the security of individual products relative to the security of the system as a whole?
  - d. In such an interconnected world, how do you draw the line between a potential vulnerability and a realistic vulnerability? In other words, just because something is possible, how important is it to assess the probability that it will occur?
3. Quite a few respected technologists – at Google, and also at the Institute of Electrical and Electronics Engineers Computing Society – have theorized that in the future, the Internet will be so integrated into our daily lives that it will become “invisible” and provide “seamless intelligence.”
  - a. Can you expand a little more on how exactly a world with an “invisible” Internet would work?
  - b. Do you agree with these predictions? Why or why not?
4. No matter how much money a company invests in security software, training and other cybersecurity measures, they still remain vulnerable to the insider threat. This can range from the intentional actor – such as a disgruntled employee stealing information or letting the

bad guys in – to inadvertent actors – such as an employee clicking an infected link in a targeted phishing email.

- a. Will companies ever be able to prevent internal threats – employees lowering the proverbial draw bridge – regardless of whether their actions are intentional or unintentional?
  - b. If it can never be eliminated, does it come down to managing risk? Are there proven strategies to minimize this risk?
  - c. How significant of a challenge is this to those evaluating the cost benefit of security measures?
5. Information sharing, though it has its benefits, is still a reactionary solution. Someone has to first suffer an attack before that threat information can be shared, and oftentimes the attackers change their signatures from target to target.
- a. How does information sharing help reduce the gap between cybersecurity capabilities and threats to cybersecurity described in Dr. Lin’s testimony?
  - b. There is a lot of focus on signatures when it comes to information sharing.
    - i. Are signature-based defenses effective? Why or why not?
  - c. How does information sharing fit into the broad picture of the cybersecurity challenge?
    - i. Does it offer opportunity beyond improving our defensive capabilities?
6. Is it possible to quantify the benefits of the Internet and information technology relative to the cost of security?
- a. In other words, is it possible to calculate the economic benefits of these technologies relative to the economic costs of cybersecurity, including prevention and response in the event of a breach?
  - b. How about the social, cultural or other less tangible benefits?
  - c. Is there value in this?
7. Discussions about cybersecurity often focus on prevention or keeping actors out of system - Is this the right way to approach this issue?
- a. If there is no guarantee the bad guys wont get in, should the emphasis shift to a focus on resilience rather than prevention?
  - b. Why is the concept of resilience important to effective cybersecurity?

- c. How does resilience support a risk-based approach to cybersecurity?
  - d. In your written testimony, you mentioned the Cybersecurity Capability Maturity Model (C2M2) in your submitted testimony. Can you expand upon this program and how differs from other options, such as the NIST Framework?
8. In Dr. Lin's written testimony he stated that "complexity is the enemy of cybersecurity."
- a. Do you agree with this assessment?
  - b. Is it possible to reduce this complexity?
    - i. If yes, what are the consequences?
    - ii. If no, why not?
9. In the last few years, there have been several significant compromises and vulnerabilities discovered in regards to digital certificates and Certificate Authorities, two of the best well-known being the compromise of DigiNotar and the recent Lenovo/Superfish revelations. This raises questions as to whether the digital certificate model is providing an adequate level of security for users of the Internet.
- a. What are the weaknesses in the digital certificate model?
    - i. How significant are these weaknesses?
    - ii. Can these weaknesses be eliminated or adequately mitigated?
  - b. Are Certificate Authorities subject to any form of oversight?
    - i. If so, by whom and how does this function?
    - ii. If not, would enhanced oversight help address the weaknesses examined in Question 1? Why or why not?
  - c. Are there alternatives to the digital certificate model?
    - i. If so, what are they?
    - ii. If not, how can the current digital certificate ecosystem be improved?
10. In your written testimony you stated that we currently "do not know" how to stop all serious cyberattacks while at the same time allowing for the efficient function of electronic commerce.
- a. Why don't we know? Is it that we currently do not have the technological expertise, or that technology has yet to evolve to a mature enough state?

- b. If the cause is that we do not currently have the technological expertise, how do we develop such expertise?
  - c. If the cause is that the technology is not yet mature enough, what are the steps we need to take to accelerate that maturity?
11. In your written testimony you describe the need for “meaningful feedback” for what works if we are to encourage adoption of more effective safeguards or systems of security.
- a. Can you elaborate on what you mean by meaningful feedback?
  - b. Can you give an example of how effective feedback could work in the real world for a small or medium business, given all the complexities and offerings in the marketplace?
  - c. What progress has been made for developing a source of reliable information and measures of effectiveness?
  - d. Is developing measures of effectiveness even possible in certain areas of cyberspace, given the size and complexities the networks?
12. In your written testimony you describe the need for medium-term solutions involving “richer data” to improve “situational awareness.”
- a. What are the challenges to developing a better sense of situational awareness?
  - b. How does improved situational awareness affect the cost of cyberspace safeguards and security practices?
  - c. As improvements in awareness occur in some portions of cyberspace, how do we translate that to prevent development of new vulnerabilities as cyberspace technologies expand?
13. In your discussion of long term needs included in your written testimony, you note that there is no “silver bullet” but there are opportunities to increase the amount of energy required for successful attacks.
- a. Can you please expand on what you mean by “energy based” barriers to cyber attacks?
  - b. What would be an example that a layman could understand?
  - c. From your perspective, what progress is being made on this front and where is it most likely to develop – defense programs, private innovation?
  - d. What in your view is the potential for the United States to achieve breakthroughs on this front, versus other nations?

14. In your testimony, you talked about repositories of “pre-hardened” components such as programming libraries. Specifically, you said that such repositories would allow developers to access components that have been tested and approved, therefore increasing the security and quality of the technologies they design.
- a. How would such a repository be created?
  - b. What organizations, both public and private, would need to be involved?
    - i. Who would be responsible for such a repository?
  - c. Would a repository such as this be expensive to create and manage?
    - i. If so, how could those costs be managed?
  - d. Who would be responsible for testing and approving the components that are made available through the repository?
    - i. Does such a repository raise liability concerns, if a “tested and approved” component is later found to be deficient?
    - ii. If so, how could the repositories address and account for that liability?
  - e. How exactly would developers use this repository?

**The Honorable Markwayne Mullin**

1. It seems like whenever we start talking about the challenges that come with responding to any emerging industry or emerging threat, the issue of workforce development is front and center. With something like the engineering industry, we know we need to engage more students in STEM education, should we be treating the IT industry in the same way?