I would like to submit the following in response to the above request for information.

I recently became certified in cyber security and am looking for a position. So I believe I have a very granular, ground up view of some of issues, upon which NIST has requested comments. I would like to discuss some of the obstacles I have faced with suggestions to improve the process.

I am William Gamble. I have been a lawyer for thirty years. I have practiced most areas of regulatory law including tax, securities and banking. Besides my law degree, I also have a masters in law (LLM) in tax and an EMBA. I have also studied the regulatory environments of many countries including most emerging markets, specifically China, Russia and others. I have written three books on these topics in addition to hundreds of articles. My work included analysis of the economic and political structures of these countries as well as their legal infrastructures. These countries, for different reasons, are often the source of both nation state and private criminal attacks.

According to Forbes, there will be a 45% increase in the Cyber Security market place per year for the next five years. There were 209,000 job openings in cyber security in 2015. According to Cisco, there are one million openings worldwide and that number will rise 600% by 2019. This gap cannot be filled with just recent graduates. The difficulty and complexity of the material does not make it accessible to many people. To find and train potential individuals will require finding and training people from other professions.

To become a cyber security professional, I tried first to see if there were government programs. There were, but they were restricted. I went to my local community college. No programs. No state programs. There were some programs at technical schools for $15000. Instead I bought the books, studied and took the tests. I now have three certificates: CompTIA A+, Network+, Security+. I am presently preparing for the CompTIA CASP. As part of my preparation I am using CISSP materials.

Since I am also a lawyer, I have studied the many, many areas of intersection between law and cyber security. Recently new cyber security regulations have been promulgated by the following agencies SEC, OIG, NCUA, FFIEC, FINRA, CFPB, FTC, FCC and others. This list barely scratches the surface. It does not include the 47 states with disclosure or privacy laws, HIPAA health care issues, new court rulings or changes in US/EU privacy and technology treaties. It is not just the US. Cyber security laws have also changed in Canada, Australia, India and China. I have reviewed all of these laws and will soon give a presentation to my local OWASP chapter.

Legal risk in this area is also rising. The OCR has begun phase 2 audits and recently levied its largest fine ($5.1 million) for a HIPAA violation. The SEC just levied a million dollar one, as did the FTC for a COPPA violation. These are just the regulatory threats. There are also civil suits for violation privacy and other laws. Internet of Things will bring enormous questions about product liability. These are especially important for medical devices. Then there are issues with cloud contracts and cyber security insurance (see below) to name a few.

Despite my accomplishments, I am having trouble finding work. There are positions. Many seem to go vacant for months. Of course I understand why employers will not discuss their reasons for rejecting my applications and I do not specifically know them, but I can make some suppositions and recommendations.

1. Experience: Although I have years' experience with the law, I am new to IT. Every employer obviously wants someone with experience to fit right into a position. I have read that 37% of companies are open to someone without experience but with my background But there is a problem. As soon as any potential candidate gets the experience, they become valuable and could easily find another position. It is also difficult for me to get experience. I do not have all the various software nor some of the appliances. Might I suggest either a hands on training program or internships? These could be funded by either the government or a consortium if IT firms who need people.

2. Clearance: I live in a city next to a large Department of Defense facility. There are numerous IT security jobs at this facility or with some of the many contractors. Some are quite junior and I am already over qualified. However, I cannot get these jobs because they require a security clearance. According to Former Deputy Secretary of Defense John Hamre, the national security clearance process as it exists today is "elaborate and woefully insufficient." Beside after the OPM hack, most of this information is in the hands of the Chinese. Worse, by limiting potential candidates, the process insures that these positions remain unfilled, which puts America's most valuable assets at risk. We need programs to accelerate or eliminate this restriction. I have been a member of three state bars and about five federal ones. I am hardly a risk.

3. Training programs: There weren't any training programs for former entrepreneurs. What was available was for a particular class of unemployed. For example, the program I applied for was for people who had been laid off in the last recession. This is hardly a helpful limitation if government and industry need people to train for jobs in cyber security, especially for highly educated people from other professions.

4. Federal Jobs: I have applied for jobs with other agencies, but these seem exceptionally inconsistent. I apply and then receive a notice that the position has been cancelled. Then a few months later, it apparently has been funded, because the notice suddenly reappears. In a competitive market I cannot see how this process allows any possibility of getting the best employees at market rates.

5. Cybersecurity Insurance: From a recent review of the cases, it seems to me that the growth of cyber insurance has two issues; the risk and the terms. First, there needs to be a better determination on the actual liability. The second is to define the terms. I believe that at present there are about sixty carriers offering this type of insurance. But what they cover and how much they charge for it varies widely. Also thanks to the Supreme Court's recent case of Spokeo v. Robins 135 S.Ct. 323 (2014), the probability of large class action settlements has substantially diminished. Most of the costs for the recent hacks of Target and Home Depot were spent on attorney fees of about $6 million. In other breach settlements, there is also a large fee for identity protection costs. Home Depot was $6.5 million. But the actual damages for plaintiffs from these breaches has not been large, probably due to the problems of monetizing credit card numbers. This all may change with the potential for large individual settlements for product liability as we see more products using the internet of things. The present reality is that the largest settlements stemming from cyber security issues are actually government fines. The OCR, which is tasked with enforcing HIPAA rules, has issued more fines in 2016 than in all of 2014 and 2015.

6. International Markets: The largest potential for international markets will be in emerging markets. Unlike the US, the awareness of cyber security risks is rather low. A recent example was the HummingBad malware. The HummingBad malware has reportedly infected 10 million android devices. It makes money installing fraudulent apps and then charging the user often very little. It is interesting to note that this infection is most prevalent in China, India, the Philippines and Indonesia. This infection proves that if the malware is spread to enough devices, it can generate substantial cash flow. Also unlike developed countries, emerging market IT devices are usually limited to mobile telephones rather than laptops or desktops. No doubt emerging market mobile phones will be a growth area for hackers. It could also be a growth area for cyber security. As these economies slow, it will also increase the availability of trained IT professionals who will undoubtable turn to cyber-crime if regular employment is unavailable.

William Gamble, JD, LLM, EMBA, CompTIA A+, Network+, Security+

Member Florida Bar