4PrivacyMatters is conducting research involving ideas and security solutions at the intersection of cybersecurity, artificial intelligence (machine learning), and the privacy of "things." We are also beginning a cybersecurity and privacy outreach program in collaboration with local and state groups, its launch scheduled for early 2018. With a focus on the Internet of "things" (IoT), our research has uncovered two keys relevant to Executive Order 13800. These are: (1) that a broad citizen appreciation of cybersecurity is essential to cybersecurity at all levels, and (2) that currently-neglected behavioral analysis of data has a valuable role to play.

The IoT has seen massive growth in both the consumer and government sectors. Moreover, analysts estimate that within ten years, the market for "things" will balloon to several trillion dollars and more than 20 billion devices. Through the IoT, interconnected devices collect and exchange data. The connection forms a network which can be privately localized or broadly spread. Each of the devices becomes an access point to the other devices and network as a whole.

For consumers, smartphones, tablets, and other smart devices such as thermostats and watches offer myriad benefits. They promise massive boosts to efficiency and collection of data previously unknown. Through analysis of this data – manual or automated via machine learning – individuals can monitor the critical functions of their homes and bodies to identify dangers (e.g., energy inefficiencies, low power, insufficient exercise) before they arise and plan in advance to resolve them.

At the same time, the IoT opens up a danger that the interconnected devices can be weaponized. Data can be stolen from insecure devices and recent studies have found that many devices retain factory defaults with limited accessibility to change these defaults. As one example, theft of health tracker data can mean theft of highly personal data such as user mobility, and in turn be used to strategically perpetrate robbery and assault. These consumer devices can also be transformed into weapons that temporarily shut down service, as was done in the Dyn DDoS attack in October 2016. In this attack, ordinary consumer devices with insufficient cybersecurity (e.g., home security cameras) were hacked into and used to shut down United States Internet service for much of the northeast United States.

For critical government systems as well, the IoT is coming to play a large part. The Department of Homeland Security has identified 16 critical infrastructure sectors essential to the functioning of the United States including industrial control systems, supervisory control and data acquisition systems, process control systems, and building automation and control systems. Analysts estimate that industrial applications of "things" will soon encompass more than half of the IoT market, making their security paramount.

Consumer devices in the IoT and critical infrastructure devices must be appropriately secured in the near future as cyberspace becomes the primary frontier for attack. The immaturity of the IoT is partially responsible for the present insecurity of devices that has resulted in high-profile attacks such as the Dyn DDoS of October 2016 and global WannaCry attack of May 2017. To this end, broad consumer education about basic protocols, such as changing factory passwords, is essential.

Education can take many forms and further approaches are listed at the end of this response. Overall, given the impact that consumer devices can have on the nation as a whole, widespread collaborative efforts are required. This means collaboration between federal, state, and local government, industry, and local communities. Some means of education include federal, state, and local public service announcements as well as designation of particular citizens as "consumer cybersecurity champions" who perform outreach services. More broadly, all levels of government should encourage data science training with funding and development of programs that go even beyond the recent HMG Cyber Schools Programme in the UK.

Education efforts will also require the cooperation of corporations. In designing consumer and industrial "things," these companies will have to create user-friendly devices that make possible the implementation of security measures and also provide competent customer service. Additionally, new startups such as 4PrivacyMatters, well-established companies, and nonprofits should all work together with local and school groups to spread best practices. Because of the wide reach of the IoT, strengthening the security of consumer devices will strengthen the nation's cybersecurity as a whole.

Moreover, a deeper focus on behavioral analysis promises a new line of defense that is currently neglected. Particularly of value to trained professionals working in the private sector and with critical systems, behavioral analysis in this case entails monitoring expected versus actual behavior. One instantiation of this was previously proposed by 4PrivacyMatters and involves use of Firmware Over-the-Air (FOTA) updates as a checkpoint for "thing" behavior. Identifying aberrant behavior, as determined through AI (machine learning techniques), can help simplify the complicated features into a streamlined process and alert human operators that intrusion or some other nefarious move has taken place. Via best practices for containment and analysis, operators can then minimize risk and fix gaps on similar devices so as to bolster holistic cybersecurity.

Increasing citizen education about cybersecurity and adding systematic behavioral analysis to cybersecurity protocols are significant means of strengthening the nation's security on the whole. 4PrivacyMatters will be continuing its research into the IoT and privacy protection. We look forward to remaining engaged in cybersecurity efforts.

Response to Question 8: What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the Nation's cybersecurity workforce, taking into account needs and trends? What steps should be taken:

i. At the Federal level? – Data science and analysis techniques are the foundation for cybersecurity in the IoT and in general. Hence, they should be encouraged through funding and systematic training that collaborates with the tech industry, educators, and other rungs of government. A broadly collaborative effort is essential.

ii. At the state or local level, including school systems? – Data science should be widely encouraged through systematic programs that touch all of society, since all of society interacts with smart devices. This interaction can be training through school systems (perhaps with

elective programs) or designated extracurricular efforts. It can include public service announcements via radio, television, smartphone, and email. To lead local efforts, individuals might be designated as "consumer cybersecurity champions" who are tasked to interact with their local communities. To perhaps bear some of the costs and to provide up-to-date engagement, willing startups as well as established companies should collaborate in these efforts.

iii. By the private sector, including employers? – Willing companies and nonprofits involved in the IoT should collaborate with federal, state, and local governments to develop and implement education programs about data science and appropriate cyber hygiene. Internally, individuals responsible for privacy/cybersecurity might be further required to attain certification as currently offered by NIST, the International Association of Privacy Professionals, and other existing programs.

iv. By education and training providers? – For the trainers, existing certifications should also apply. For education of the public, programs might also be offered in streamlined forms such as MOOCs (massive open online courses) offered through Udemy or other widely accessible platforms.

v. By technology providers? – In encouraging data science and collaborating with other groups responsible for cybersecurity, tech providers will also be able to provide more secure products and services. Successful implementation of societal cybersecurity programs will require the collaboration of all parties involved.