Testimony of Kevin Keeney
"Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape"
May 10, 2017

My name is Kevin Keeney and I was asked to testify before this committee due to the multiple hats I wear in the Cyber Security ecosystem. I'm here representing myself and my opinions are mine alone. I work full-time for Monsanto as the Director of their Cyber Incident Response Team (CIRT). My team there is made up of ten highly qualified cyber analysts on two different teams, one dedicated to the function of Cyber Security Monitoring (reactive) and the other to the function of Threat Hunting (proactive). I also work part-time for Missouri National Guard at the Chief of Operations for MOCYBER. The MOCYBER team is made up of 39 Army and Air National Guard members. We are broken down into three teams: A notional Mission Defense Team (MDT) with 10 positions that MG Danner has authorized to be created with no manning or funding, a Defensive Cyber Operations – Element (DCO-E) with 10 positions that has been part of the Missouri Army National Guard since 1999, and a partial Cyber Protection Team with 21 positions that will officially begin to form on 1 October 2017. Just like the notional MDT, MG Danner has allowed the positions to be filled in advance, understanding the threat we face as a nation. A threat which will not wait on our nation's current timetables.

I would like to thank the Committee for considering the issue of Cyber Security and the threats we face as a nation. I am particularly happy to hear that the committee members see an opportunity for the National Guard to bridge the gap between the public and private sector. I am humbled that you have invited me here today as a witness before the panel.

My goal is to provide some information about MOCYBER, and what it has been doing for the State of Missouri and nation. In addition, I hope to share some insights about the threat actors I am facing in my two roles. I am also aware that the panel is interested in discussing the Cyber workforce.

In the summer of 2009, I re-joined the Missouri National Guard with the goal of building the Missouri National Guard's Cyber capability. MG Danner was keenly interested in this effort, and empowered me and others to recruit and retain the best and brightest. MOCYBER has had its share of success and I believe it can be repeated at scale. Here are the two tenets that have enabled us:

1. Remember the "Special Operations Forces Truths"
    a. Humans are more important than Hardware
    b. Quality is better than Quantity
    c. Special Operations Forces cannot be mass produced
    d. Competent Special Operations Forces cannot be created after emergencies occur
    e. Most Special Operations require non-SOF assistance

2. Build a culture of Innovation
    a. In the Military problems abound
    b. Think big
    c. Start small

These tenets are what enable MOCYBER to recruit and retain people willing to travel from seven states to drill with us. They enable an environment where enlisted and officers collaborate as technical equals, freely and openly, to solve complex problems. This freedom to operate led my team to create ROCK (http://rocknsm.io), an open source project that has attempted to address the problem of Military personnel showing up at a Critical Infrastructure or Key Resource (CI/KR) provider to lend a cyber hand. In short order, ROCK has been adopted in the commercial sector, active duty military, and multiple federal agencies. All of this has been done with zero funding from the U.S. Government. It has been done on my soldier and airmen's personal time. Their passion to defend the nation is unmatched.

The threat actors I face in my corporate life are online extremists (hacktivist and eco-terrorists), industrial espionage (Nation States), and the occasional criminal. Since leaving the public sector in 2011, I've been surprised by how much I encounter Nation State actors in private industry. The challenges in dealing with extremists and criminal threat actors can be dealt with in most corporate environments through the use of traditional security countermeasures. However, with Nation State threat actors we as a country are far behind because we are defending against them the same way we do other threat actors while they are conducting warfare. It also goes well beyond just hacking and into more disciplined, strategic, and carefully curated espionage- we have nations playing the long game.

My hope is that this committee, Congress, and our country as a whole can start openly embracing the National Guard's role in defending the nation through closer integration of USNORTHCOM and the Department of Homeland Security. The nation's largest threat is to the private sector, not the public. The National Guard is uniquely postured to bring highly skilled operators and analysts to bear on both sides. The government and military need to move beyond trying to secure itself and move into an active and supporting role in defending America, just as it does in all other war fighting domains. We need to remove the seams between the military, government, and the private sector. The Internet-at-large doesn't work this way--fencing off public and private sectors--and we must defend it as it is, and not how we are organized.

Although the current Cyber Surge by the U.S. military is going well, it doesn't go far enough. It is not flexible and dynamic, which is specifically what is needed to address the problems we face. Recruiting, training, and retention all fight against each other which leads to a constant and chaotic talent churn. In addition, it has completely left out the most critical element of our society- the private sector which provides the tax base. This is where the wealth of our nation exists. The National Guard has, since before the origins of our nation,

provided for the defense of it communities. Let's reignite that strength that comes from within our communities.

My Specific recommendations:

Write legislation that creates and funds a new uniformed service called U.S. Cyber that is responsible for security of our Internet, not just .mil or .gov, and consolidate all cyber personnel, equipment and missions under it. This will enable a single organization to provide the needed focus on recruiting, training, doctrine, retention and care for its service members. U.S. Cyber should be made up of no more than 50% active, and no less than 50% reserve forces. Transitioning between the active and reserve should be as simple as applying for an opening and being accepted. The ability to move from Title 10/18/32/50 seamlessly is essential. This will achieve what all other warfare domains have- unity of command and unity of effort.

Effects achieved through the creation of U.S. Cyber:

1. Standards for recruiting and retention can be specifically tailored to the needs of U.S. Cyber service. Mental stamina is paramount, but being a double leg amputee has no impact on a potential recruit's ability to be trained.
2. U.S. Cyber service will be able to select from a broader sector of the population, which will enable more stringent selection for mental flexibility, problems solving skills, and aptitude.
3. U.S. Cyber can apply resources at tactical, operational, and strategic levels as needed without fighting for resources across multiple services.
4. Cyber effects can be provided to the entire nation to include the private sector, other uniformed services, intelligence communities, and National Command Authority in a synchronized, de-conflicted, and efficient manner.
5. The study of cyber as a warfighting domain and creation and testing of its doctrine would not be narrow as it is today.
6. New insights into our capabilities, our adversaries, and how they relate would be gained, as well as a more complete understanding of the problems that still need to be solved. Proper resources can then be advocated for and applied to the most important issues.
7. Deduplication of cyber training schools across all uniformed services. This cost savings would enable the creation of world class cyber ranges and realistic opposition forces.
8. Better trained cyber operators that can conduct fluid and full spectrum warfare, not just complete a checklist.
9. In the long term, significant cost reductions can be achieved through deduplication of facilities, personnel, and training.

While there is much to gain from the creation of a new uniformed service, there are some areas of focus that would need to be addressed:

1. In the short term, other strategic programs would receive less or zero funding. In the long term, in-fighting between the services about cyber missions would be reduced. This saved energy could be better used furthering the warfighting domain they are responsible for.
2. Possible degradation of cyber capabilities during the transition of cyber resources to U.S. Cyber.
3. Could temporarily weaken other instruments of national power, as information is known to be the underpinning for diplomatic, military and economic power.

In summary, the creation of U.S. Cyber could close the cyber capabilities gap more quickly than the current strategy. We need to build the foundation for a future that will most certainly include more, and not less, reliance on information dominance. The conflicts we have recently witnessed in the Ukraine and the South China Sea are well-executed examples of hybrid and full-spectrum warfare. If we are going to win against a peer, or near peer adversary, we must build a unified cyber force that can fight and win as an equal stakeholder in the battle. It is essential that we begin acting upon what we know is happening within our borders- the rampant theft of the Intellectual Property created and owned here in the United States. As Americans, we have the duty and honor to defend that. Thank you.