Written Statement of Senator Jim Talent

I want to thank the co-chairs for inviting me to share my thoughts on the state of the National Security Innovation Base (NSIB). I also want to commend you and the full Committee leadership for creating this task force. The existence of this bipartisan task force committee will signal to the Department of Defense how seriously the Congress takes the health of the NSIB, and that signal has value even apart from the legislation that will result from your work.

I'm sure you invited me because former Deputy Secretary Bob Work and I are currently co-chairing a task force on the NSIB for the Reagan Institute. We're pleased to have Congressman Banks on that task force, as well as Mr. Kim, Ms. Murphy, and Mr. Gallagher. Secretary Work and I will be eager to share with you our specific conclusions and recommendations after we issue our report in a month or so, but for now I think I can be most helpful in offering four general observations to help you frame your own investigation.

First, it's important for your task force to come to a common definition of the National Security Innovation Base. You can't direct and motivate the NSIB if you're not sure what it is, or if you don't understand the characteristics and incentives of the various actors in it.

Our Task Force spent a whole session on this issue and will in our report suggest a definition something like the following:

The NSIB is an enormous, pulsating and chaotic ecosystem of public and private actors including but not limited to the national security agencies, the National Laboratories, the great research universities, the traditional defense primes, the huge global tech companies, startup tech firms, and the venture capital community that regularly invests in groundbreaking research and technologies that are relevant to our national security.

The segments of the system both cooperate with and compete against each other. They have different goals, incentives, cultures and characteristics. In their efforts at innovation the private firms in the NSIB are working towards commercial ends and are often unaware, or at least not fully aware, of the national security implications of their work.

In contrast, China has a top down innovation system where all the actors, including the nominally private ones, are yoked together in harness to the authoritarians in Beijing. Our NSIB should not and cannot be like theirs, yet at the same time the government does need to coordinate and build partnerships within the system towards common goals.

During the Cold War, national security innovation was driven by DOD funding and conducted in government labs or by a relatively small set of private companies who could be expected to adjust to the culture and processes of the government. In today's NSIB much of the most important research is dual-use – driven by private actors for commercial purposes – which means the government will have to do a fair amount of adjusting itself to the commercial world.

So your task, as senior political leaders, is to focus the ecosystem on national security priorities, create a more comprehensive security consciousness among the private actors, and coordinate the segments enough to get the necessary synergies -- all without straightjacketing the creativity of the ecosystem or sacrificing the freedom, openness, and risk positive culture that is one of the NSIB's greatest strength.

It will be a difficult, delicate, long term and absolutely vital project.

My advice to the task force as a former Member is to be certain to take the time to learn from the various segments in the NSIB ecosystem and especially from the private actors in the tech world and the universities. Ask the players on the ground about the obstacles to partnering with the government and how the DOD can structure incentives so that the ecosystem more or less naturally bends its activities towards the technological priorities of the government.

The point is to push the ecosystem towards better integration and common goals at least mostly by aligning incentives rather than through highly prescriptive mandates.

Second, you are going to have to deal constantly with the natural tension within the NSIB between security and innovation – between defense and offense, if you will. Examples of this tension abound. We want our tech companies to be vibrant, benefit from capital market flows and gain market share; but we worry when they partner with foreign companies or accept foreign investment. We want to attract top level technical talent into our NSIB; but we know the PLA and Chinese intelligence agencies are very good at planting agents and infiltrating institutions to steal our technology. We want to partner more closely with allied countries in developing new technology; but that means giving those countries more freedom to have and handle our technology, with the attendant security risk.

My own belief, after months of work in our own task force, is that the government should build higher fences around fewer things. In other words, we need to do a better job of identifying and fencing off the really vital technology that only American actors control and can develop, while allowing the ecosystem freedom to share or sell technology that, as a practical matter, our national competitors can get no matter what we do.

My instinct is that Beijing is so good at stealing or appropriating the technology of others, and has devoted so many resources for so long to developing that capability, that we should plan on the assumption that offense will be more effective than defense, in the long run, in winning this competition.

But however you resolve the tension, it's important for the political leadership to recognize that there are important equities on both sides, that trade offs will be necessary, and that whatever you decide you must set clear rules that the whole ecosystem can understand. Uncertainty is the enemy of both security and innovation.

Third, I'm sure you are planning to inquire carefully into the efforts DOD is already making to energize and use the capabilities of the NSIB.

Our task force was particularly impressed with two DOD programs working to harness tech innovation—and innovators—to solve problems: Defense Digital Service and Hacking for Defense. The former approaches the problem from the inside out; the latter from the outside in. Both programs are shaking up the DOD enterprise by:

- Reinterpreting and reimagining mission challenges in useful ways;
- Bringing the best civilian tech talent to bear on behalf of national security;

- Breaking down cultural barriers, pulling the tech and defense worlds together, and creating a recruitment pool of tech talent for the future;
- Leveraging the knowledge of private tech leaders to seek out the best problem solvers for particular challenges;
- Introducing the DOD to other parts of the NSIB ecosystem (e.g. the academy, tech entrepreneurs);
- Acclimating our warfighters to thinking from a tech point of view about solving problems; and
- Blazing the trail in navigating around existing DOD processes to bring new innovation and energy to the Department.

Programs like these, which operate at the grass roots, are good ways to coordinate the NSIB ecosystem without straightjacketing its independence and dynamism. They may not be easy to scale, but if you study the characteristics that have made them successful, they can be models for similar efforts. The more visible successes you create in any part of the NSIB, the more likely it is that the ecosystem will see the value in these partnerships and spontaneously begin producing them without stimulus from the government.

Fourth and finally, one vital role for Congress to play is to give clear permission to the DOD to take greater risk with its procurement dollars where innovation is concerned. That is not a natural thing for the Department. Innovation is a risky business, whereas government is typically, and appropriately, risk averse with public funds.

When our task force visited Silicon Valley, I was greatly impressed by the attitude of tech investors. They knew that many of their investments would produce little return, and they accepted that as a necessary aspect of creating hugely successful enterprises with the investments that did succeed. They advised us that venture capital would invest much more, and much more often, in new and groundbreaking defense companies if programs like DIU had more discretion to give fewer, larger contracts to newer companies over a shorter time horizon.

In other words, if the Department is to succeed in getting breakthrough successes, it must have permission to fail. Of course we want due diligence to be done; of course we want public funds to be spent thoughtfully and purposefully. But we also want and need much greater private investment in national security throughout the NSIB ecosystem, and that will not happen if the government cannot acculturate itself to a higher level of risk.

I hope you will find ways to reassure those you oversee that you will have their backs when they take intelligent gambles on promising technology. In fact, your message to the Department should be: if all of your experiments succeed, it means that you are not experimenting nearly enough.

I thank the Co-Chairs again for the opportunity to testify and look forward to your questions.