Testimony for Cyber Subcommittee of SASC on 14 November 2018.

My name is Francis Landolf and I was privileged to serve in a 30 year career at the National Security Agency. I was hired as a cryptomathematician and spent most of my technical career as a signals analyst. My first positions in leadership were leading large signals analysis organizations and later leading the consolidation of the signals analysis activities across the SIGINT directorate. The last position I held before retiring was leading the Cryptanalysis and Exploitation Services (CES) mission there. This is different from the cryptanalysis mission before or after, in that in addition to cryptanalysis and encrypted signals processing, my organization also performed all unencrypted signals processing. If you think of the major functions of SIGINT as being: 1. Collect Data, 2. Render the Collected Data consumable by Intelligence Analysts, 3. Consume the processed data to produce finished intelligence and 4. Disseminate the finished intelligence to customers, the mission of CES was the second function in that intelligence production chain, rendering collected data consumable: if data is encrypted, process so some or all of the underlying data is revealed. If the data is compressed, multiplexed, encoded or had any other process done to it for transmission, we analyzed those processes so that we could undo them and reveal underlying information so that intelligence analysts could consume it and produce intelligence. It was during my tenure as an analyst and later as a leader of the signals analysis and cryptanalysis missions at NSA that the agency had to first transition from Soviet-centric, proprietary analog communications to digital communications and later, the real transformation in communications, and that is the transition from circuit switched communications to commercial, standards based packet switched communications and convergence to the Internet.

Most missions in the government do not have such a large number of technically savvy government employees capable of developing software and systems as NSA. Rather they depend on their industrial base to develop the technologies and systems needed to perform their missions using completion contracting. NSA is different. NSA uses contractors extensively, in level of service based contracting, mainly to augment the large government workforce that leads and guides the development of new SIGINT systems and capabilities. That makes NSA technically adept but leads to problems in integrating commercially available products that serve mission applications and are the product of private sector innovation. I believe that cybersecurity is one such situation. It seems very clear that, for example, the $7.7B in venture funding in 2017 for cyber represents an enormous investment in innovation that would be impossible for NSA to match. By building their own products that perform cybersecurity functions without integrating commercial cybersecurity products, the agency is not taking advantage of that sizable investment in commercial innovation in cybersecurity. Therefore I believe that the private sector is out-innovating the Agency in many areas and the pace is accelerating.

The Defense Department is directly affected. NSA has long been rightly recognized as the center of expertise in the US government in cyber. NSA's leadership played a major role in persuading successive Presidents and Secretaries of Defense to create and invest heavily in military cyber command and in the national importance of cybersecurity. The Nation is indebted to the NSA for this vital role as a catalyst. Unfortunately, however, for too long the Defense Department assumed that NSA would also provide the technology and capabilities needed to secure the Department from cyberattack. This led the DoD to overlook and neglect what the commercial sector has been producing for the last 15 years or so. Silicon Valley and other technological hotspots around the country are continuously generating innovative security solutions that DoD fails to notice or procure in timely manner. The DoD lags significantly behind the mature state of the art in commercial technology. Since retiring from government service, I have worked in multiple capacities helping new small companies grow and attempt to find government customers. I am now or have served as an advisory board member for panels at the National Security Agency, the Cyber Incubator for startups at the University of Maryland Baltimore County, a non-profit technology group known as Mission Link in Northern Virginia that tries to help young companies do business with the government and the Virginia Tech Hume Center in Arlington. I have also been a Member of the Technical Advisory Group for the Senate Intelligence Committee and am a Senior Fellow and Member of the Board of Regents for the Potomac Institute for Policy studies. I have observed as a rule that companies with exciting new technical approaches to cybersecurity, backed by prestigious and savvy venture capital investors, struggle to get meetings with the defense department, much less a chance to demonstrate their products and make sales. This is true even when there appears to be genuine government interest. The time and effort required to close a deal is too great for small companies, especially where an equal exertion yields far more success in financial services or other commercial sectors. Indeed, I have met with multiple venture capital firms that actively steer their companies away from even trying to market the government. Savvy companies seeking investment know to not to use DoD business as a likely source of revenue during their fund raising pitch to potential investors. I don't mean to pick on the DoD: while NSA and DoD present unique challenges for the cybersecurity industry in particular, but more generally small, new companies where much of the commercially based innovation is taking place, there are plenty of generic barriers to government acquisition of commercial solutions, which I would be happy to discuss during the Q&A. There are however some encouraging signs. DoD's civilian leadership, now spanning two administrations, and Congress now recognize the tremendous potential for commercial technology to solve vexing problems not only in cybersecurity but a host of new information technologies including the Internet of Things, machine learning, analysis of exascale data sets,  and cloud computing. Congress and the pentagon are beginning to streamline and provide more flexibility to acquisition processes, establishing outposts such as DIUx, and create acquisition organizations with a mandate to increase the pase of technological experimentation, adoption and fielding. I have some ideas and recommendations for how NSA and DoD could improve their approach and processes, which I will outline here and can pursue in greater depth during the Q&A

(1) NSA needs to embrace the innovation happening in the commercial sector and choose to focus less on building their own solutions with government and contract labor and more on helping DoD be a smarter buyer.  NSA should adopt the role of a sort of "consumer reports" for cybersecurity – performing objective evaluations of commercial cybersecurity products, not just products incorporating encryption technologies, rating and comparing them, and advising DoD on best-of-breed and promising new technological trends.

(2) Create a Virtual Technology Demonstration Lab and designate some operational subnetworks for test and evaluation of new products and services - This would serve the purpose of being part of a Technology on-ramp and lower the cost for companies to demonstrate their products in an environment that simulates or actually replicates the actual mission environment into

which they would be deployed. The synthetic Lab could be done in one of the commercial providers of CLOUD Services.

(3) Create a process to harness the good-will of former senior department officials that leave for private sector positions and become aware of technological innovation that could assist the department mission. These “adjunct technology scouts” would provide input on technology and products that would address mission needs that they encounter in their work “after government”.

(4) Insure that technologist and mission owners are educated on the use of section 804 of the 2016 NDAA and extend this provision. The law is called Middle Tier Acquisition (MTA) and is a rapid acquisition interim approach that focuses on delivering capability in a period of 2-5 years. The interim approach was granted by Congress in the FY16 National Defense Authorization Act (NDAA) Section 804 and is not be subject to the Joint Capabilities Integration Development Sysytem (JCIDS) and DOD Directive 5000.01 but expires Sep 2019 unless extended. The approach consists of utilizing two (2) acquisition pathways: **(1) Rapid Prototyping** and **(2) Rapid Fielding**. It does this by streamlining the testing and deployment of prototypes or upgrading existing systems with already proven technology. This law could serve as a much needed part of the on-ramp for new innovative technology, but likely will not be invoked much because of lack of knowledge and understanding of it and its intended purpose and provisions.

(5) Mandate Buy vs. Make analysis for all cyber capabilities that are built by the government and their contractors rather than purchased.