Remarks from Amit Yoran at the Army Cyber Institute on May 2015

Thank you. How did I get lucky enough to snag the last speaking slot of the day and the opportunity to stand between you and the event's closing remarks?

In 1991, I was fortunate enough to attend West Point's first ever InfoSec class, and have been passionately engrossed in this field ever since. In that time, I have had some remarkable opportunities to serve and be exposed to the dynamics of this very fluid discipline in both the public and private sector.

Public-private partnerships offer a constructive opportunity for cooperation in our efforts against our common cyber adversaries. That said, I'm frankly skeptical about any chance of success until we acknowledge and address the obvious – we have some fundamental trust issues here, which stem at their core from a lack of clearly defined roles and responsibilities in this highly dynamic cyber domain.

Candidly, government and private sector have different and often conflicting objectives and agendas in cyber, pitting them against one another. In truth, the cyber issue so broadly affects every aspect of modern life, that there are frequently conflicting objectives and agendas even within and across the various agencies of the government itself. More on these issues shortly.

Without clearly defined roles and responsibilities, it is unlikely that we will ever develop appropriate expectations of one another, and even less likely that we will develop the sense of trust that is a fundamental ingredient to any constructive public-private partnership. The cyber need is great and we naturally have a great sense of urgency. This yields a domain in which cyber operations become the de facto policy - outpacing public policy discourse and any informed public debate of legal frameworks and interpretation.

The result can be nothing but mis-spent precious cyber dollars, mis-set expectations and then the inevitable public backlash upon the eventual disclosure of government cyber operations and policy. Where will this end? Quite frankly, I don't know. But I do know that the only long-term winners in this situation are clearly our adversaries, which regularly prove themselves more intelligent and creative than we care to admit.

As a precursor to defining any successful public-private partnership, we must lay the groundwork through the establishment of expectations of one another, and a common understanding of roles and responsibilities as a foundation for trust.

I will spend a few moments outlining some inherently governmental functions in the cyber domain. Now please bear in mind that I have been allotted 30 minutes for my remarks, so I can graciously blame any exclusion or omissions on my part to brevity.

Let me start with the intelligence community. It may sound odd for me to advocate for the government to play a role in intelligence collection given the Snowden fallout of the past couple of years but it is a critical component of every nation's security.

A key area of intelligence collection should include improved functionality around attribution in cyberspace. Effective clandestine activity in cyber can also yield insight into adversary effectiveness and ongoing compromises. The intelligence community should also be clearly focused on the foreign threats. Intelligence efforts must be clearly separated from information assurance efforts. Clear boundaries of authority and responsibility are needed here.

Yes, we have great skill in our IC, and Intel should inform Information Assurance efforts, but there can be no confusion about authorities, responsibilities or purpose of use. Right now the Cyber Command is collocated on the NSA campus and led by a singular individual, an unnatural conflict of mission, great as he or she may be. The Department of Homeland Security has effectively outsourced so much of its mission to the NSA. There are fundamental flaws in system design.

We must recognize that there is a clear and distinct conflict of interest between intelligence objectives and those of system operators. Simply put, intelligence organizations prioritize the intelligence and counter-intelligence missions. In cyber, they focus on monitoring adversaries, determining their methods and techniques, tracking their activities to a point of origin, determination of compromise scope, attack intent, and adversary's objectives.

While these are very important, they frequently conflict directly with the information assurance objectives of system owners and operators, who are primarily concerned with system defense and protection, and in the event of compromise, a speedy restoration to a functional and assured state. This distinction in core objectives is critical because it represents the difference between programmatic emphasis on information gathering, or system resilience and availability.

For instance, intelligence and law enforcement entities often prioritize attack attribution, while almost no meaningful emphasis is placed on attribution by those defending systems. Rather than sharing information with operators and better informing them as to how they can defend and monitor themselves, today's intelligence and law enforcement mindset around cyber by definition limits information exchange.

Government, and Intelligence and Defense communities in particular, cannot and should not be in the business of defending private sector networks and systems, even in those critical infrastructures. Such monitoring and defense programs would face significant cost and technical scalability impediments. We must remember the purpose for a monitoring program. Are we in fact monitoring to enable better defenses? Who makes the decisions to inform the defense upon compromise? How would decisions be made as to which traffic from which actors to block? How might government defensive methods introduce delay or network performance degradation?

For many critical systems a delay of even one hundred milliseconds can be deemed unacceptable. At the aggregate level, neither defense, intelligence or any government agency knows the purpose of traffic or purpose systems which they were deployed. Only the owner of a system or data set knows the true business purpose for which it is employed, and only they can make an informed risk decision as to its operation.

More importantly, taking on some of this function leaves the owners and operators of systems to believe that they don't have the true responsibility of defending their networks and managing their technology and business risk. "The government will protect me mindset" is a most dangerous slippery slope of learned self-helplessness.

According to the new DoD cyber strategy, "the DoD must be prepared to defend the United States and its interests against cyberattacks of significant consequence…significant consequences may include loss of life, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact…."

It's a rightfully so very broad charter and mission statement. It also leaves way too much leeway for interpretation for any of us to feel comfortable, and it leaves room for great confusion on lanes of responsibility, lack of transparency, and puts public-private engagement at great risk of mistrust.

I've spoken already to some of the challenges facing us on the law enforcement side. The government is the only entity that has the authority to enforce rules and laws when broken by nation-states, criminal enterprises or individuals. Despite the public fascination with hacking back, the universal and consistent interpretation on such actions by every attorney and legal scholar indicate that it is a clear violation of U.S. law. It can also cause great chaos at the operational level.

Let me turn now to legislation and regulation. The government has responsibility to develop and pass thoughtful legislation that provides for public safety. Many of these authorities exist in the government's sector-specific agencies, but these authorities have had mixed adoption when it comes to the cyber domain. While regulatory frameworks can be helpful, dictating specific technologies to achieve security is nonsensical - as those regulations become dated and worthless before the ink is dry. Think of the uselessness of requiring AV, IDS or SIEM specific technologies. They constitute an absurd waste of valuable security spend and expertise, and distract from the real task at hand.

Finally, and perhaps most significantly on this topic, the government has regulatory authority and bears responsibility to help facilitate free markets. Free markets cannot function without transparency. In our case, transparency into breaches, whether they affect personal identifiable information or not. Transparency into what the threat environment actually looks like, to the extent government has that insight and is willing to share it. Transparency into what investor risks actually look like. Transparency into what good security and effective protective measures are. And transparency so that corporate decision makers and investors can truly understand the risks they face, and be held accountable for the decisions they make and their ultimate successes and failures. Where market imbalances exist, which seems clearly to be the case in cyber, Government can provide incentives, liability relief, tax policy, clear articulation of responsibilities, and numerous other mechanisms worth considering.

Through the Department of State, the government must engage with other nation-states and the international community to develop international cyber norms of behavior. This effort has just begun in earnest, and it may take precious decades, but its importance cannot be overstated if we are

ever to see rule of law in cyberspace. On this front, the government can impose changes in trade policy, and has numerous foreign policy tools at its disposal, including the use of force and armed conflict.

The recent Executive Order calls for the blocking of property and financial transactions of perpetrators of malicious activity in cyberspace, a not insignificant step for the government. The body of knowledge in and around deterrence theory is significant and should be put to use in this domain, where to date all governments and cyber criminals operate with near perfect impunity.

As one of the world's largest consumers of technology, the government has an opportunity to define and set security standards for itself. Government requirements to protect its own information and information systems are almost an exact duplicate of those requirements needed to protect private industry and critical infrastructure systems. With its sophisticated understanding of the threat and exploitation, the government can define the functional requirements for more secure and resilient systems. With this definition available, private industry and entrepreneur efforts will deliver, let us have no doubt.

In NIST, the government has a role in helping industry form national and international standards, which improve interoperability, create greater determinism, and play a very significant role in the cyber challenges facing us. In mastering new and complex science disciplines, the government has also traditionally played a significant role in funding fundamental research.

I want to be very explicit on this topic -- the government should not be developing a set of disastrous GOTS capabilities where the government cyber monitoring and defense needs align with that of private industry. Private industry is combating professional cyber criminals and nation-states. Developing technology is the role of the private industry, where innovation and entrepreneurship and billions upon billions are being invested in cyber R&D. Where foundational research may not be practical or have near to mid-term application, it is unlikely to get the attention it needs from the economic investment mindset of private industry.

And one more role of government that is particularly important in our great and free society - ensuring privacy, civil rights and civil liberties are respected. For the past 15 years, we have used external threats as excuses to encroach upon traditional rights to privacy and civil liberties. We must not allow this practice to continue as our battles move deeper into the digital theater.

The government is once more considering the mandate for all service providers to be able to access information which they transport or services they provide. For decades, intelligence collection and law enforcement surveillance have been augmented and enhanced by the increased adoption of digital technologies, all at a non-trivial cost of the very freedoms and privacies that our service academies were founded to protect, and that we all hold so dear.

According to senior national security and intelligence executives, the mandate for law enforcement backdoors serves "little to no national security value." Terrorists and others have long since learned not to rely on the services where the provider [and government] has access to their content.

Current policy leanings in this direction are greatly misinformed and ill-advised, and would have little impact other than degrading privacy, civil liberties and the viability and competitiveness of U.S. corporations and economic interests - which we should not forget still struggle mightily in overseas markets as a result of the Snowden disclosures.

Such policy will also weaken the security available to those defending their systems, where the deck is already stacked against them, and inexcusable mistake by every measure.

The role of the private sector seems much more straightforward.

As the owners and operators of the nation's infrastructure, we are responsible for securing it – the private sector needs to take responsibility for its own cyber defenses. Whether we're used to accounting for it or not, the efficiency gains of technology use are not risk-free. Private industry has a responsibility to know, understand, and manage that risk effectively. The cost of using technology and doing business means protecting your enterprise and information.

Secondly, developing critical technologies and driving innovation in the area of cyber security are critical roles of the private sector. For too long the private sector has settled for iterative innovation in cybersecurity while our adversaries are advancing at an exponential pace. We understand how great the challenge is. We must innovate at a scale to meet it.

Finally, the private sector must take an active role in the cyber strategy and policy debate. The outcomes of those debates directly affect us, as they do the entire world. The time for sitting idly on the sidelines has passed us by.

The concepts I have laid out may seem like common sense to many of you. I have probably stirred a visceral anger among others. That's OK. The important thing is that we begin the debate and establish clear and transparent expectations on various actors and processes in the public and private sector – something I consider to be a foundational building block for public-private partnerships.

Many of the partnerships to-date, and even some of the President's new cyber initiatives, are focused on information sharing, and when done correctly, there can be value to the participants. That said, so many of these sharing concepts are left at the apple pie level and don't get into the meaty and meaningful topics which will define their ultimate success or failure.

Who is being asked to share? What are they being asked to share? Specifically when and how are they being asked to share it? How will this shared information be used? How will it be protected from disclosure, both legally and operationally? Who will have access to it? What are the liabilities and assurances which can be provided in support of the answers to these questions? And most importantly and fundamentally, why? Why should this information be shared? What is the value proposition for the sharing or disclosing party?

Whether you're in the government or private sector, you can only put yourself in the middle of a process or PowerPoint slide for so long without adding value to its other participants before they lose interest. The government has great expertise and value it can contribute in this domain, but it requires

some creativity and out of the box thinking about how things can be done differently. To state the obvious, we haven't gotten it quite right yet.

# # #