REMARKS BY SPECIAL ASSISTANT TO THE PRESDENT AND WHITE HOUSE CYBERSECURITY COORDINATOR MICHAEL DANIEL

Gartner Security and Risk Management Conference
June 23, 2014

As Prepared for Delivery

Good afternoon everyone. It's a pleasure to be here at the 2014 Gartner Security & Risk Management Conference.

My name is Michael Daniel, and I am the Special Assistant to the President and Cybersecurity Coordinator at the White House. In my role, I lead the federal government's development of national cybersecurity strategy and policy and oversee the implementation of those policies on behalf of President Obama.

Today, I would like to talk about why cybersecurity is such a hard problem and how we are trying to make progress in spite of that. And from my vantage point here in Washington, we are making progress. I'll readily admit that progress on cybersecurity policy often feels very slow – to those of you in the business world, it might look like we are standing still. That can feel especially frustrating, when everyone here – the ones closest to the action in cybersecurity – see the gravity of the threat and how fast the adversary is moving. But I can say that, in the past year, we have started to make real progress. Real progress in building the common foundation for our collective security, and real progress in developing the strong partnerships that are so critical for future improvements in cybersecurity.

At one level, cybersecurity should be an easy problem. After all, the vast majority of intrusions rely on known, fixable vulnerabilities. So the bad guys usually get in through a vulnerability we know about and we could have fixed. So what's the deal?

Clearly, that means the problem isn't actually so simple, or we'd have fixed it already – and I could work myself out of a job. I want to talk today about three reasons I believe the cybersecurity problem is so hard, and then three concrete steps we are taking from a policy perspective to tackle those hard problems. These may not be the only reasons, but without addressing these issues, our efforts will likely continue to struggle.

OLD CHALLENGES AND INCENTIVES

The first hard problem stems from the fact that we clearly do not understand the economics of cyberspace. I come to this conclusion because of one glaringly obvious point: The challenges we face are not new**,** and many of the solutions are readily available.

These are issues – cyber hygiene, information sharing, and identity management, to name a few – which we have known about and discussed for years. Granted – the adversary's tactics evolve, and the impact of malicious behavior in cyberspace is growing exponentially as we hook more things up to the internet – but many of the same fundamental weaknesses in our collective armor

remain. And we know how to fix most of these vulnerabilities from a technical point of view, but we can't get people to implement them.

It's not like we don't collectively understand these facts. Yes, we can always do more on education and awareness, but cybersecurity problems are now well-known across a large portion of society. And it is clearly in everyone's best interest to be good at cybersecurity.

So the logical conclusion has to be that we don't fully understand the economics and psychology of cybersecurity. We haven't fully confronted these problems in terms of human behavior and motivation, as opposed to technical solutions. Until we really understand the human factors – and change our approaches as a result of this understanding – we will continue to fail at solving this problem. Technology cannot compensate for bad business practices in cybersecurity.

EVERYBODY CARES

The second hard problem ironically stems from the success of the Internet and cyberspace. The vast extent and impact of cyberspace – the fact that it touches everyone and pretty soon virtually everything – is changing how many people think about it.

When the internet was first built, critical infrastructures were not connected to and didn't rely on the internet. Nobody cared about privacy protocols, because people didn't live their lives on-line. And security was still largely based in the physical world. Users didn't worry about the security of the underlying code and how it functioned – only that it worked. Governments didn't understand the Internet, didn't use it much, and didn't see why they should care about it. So nobody minded that technologists set up the Internet to be governed in a highly decentralized way, outside of government-based structures.

Now, ***everybody*** cares about these things – at least to some degree. And this makes it really hard to take collective action. Governments are waking up to the fact that they really need to care about the internet and how it works – for all sorts of reasons, good and bad – from our point of view.

As a result, what used to be decided by technology experts, or by an informal agreement among internet service providers, is now the intense focus of a highly political process. That means decisions that were once easy in internet governance are now much harder. Given how important the internet has become to everyone that difficulty isn't going to change any time soon.

NO INTERIOR TO CYBERSPACE

The third hard problem, not surprisingly, stems from the structure of cyberspace itself. As we think about how to counter the threat in cyberspace, one factor about the nature of cyberspace becomes particularly relevant. Traditionally, the argument has been that cyberspace has no borders, and the lack of borders is both a strength – after all, the free flow of information drives huge economic benefits – and a problem – because it allows malicious actors great freedom of movement.

But I think these arguments are not entirely correct. There are borders and boundaries everywhere in cyberspace – everywhere that networks, routers, servers, and the like touch – there are borders. And we are just creating more borders as we build the "Internet of Things." Instead of borders, what cyberspace lacks is an interior – there is no "inside" to a network when you really think about it. Everyone "lives" and operates at the border. The very nature of cyberspace and its interconnectedness means that everything and everyone touches an edge or a border in some way.

This reality has some profound implications for how we organize ourselves a society to protect ourselves in cyberspace – and how I try to carry out my cybersecurity role. For example, in the physical world, we assign the mission of "border security" to the U.S. federal government. But if everyone lives right at the border in cyberspace, then it's not physically possible to assign the "border security" mission to just one group or element of our society. Protecting cyberspace is, by its very nature, a mission shared by all. This reality makes organizing for cybersecurity incredibly complex, because it requires cooperation across boundaries in the physical world that are difficult to bridge – between government agencies, within the private sector, and between the government and the private sector.

If we all live and work at the border, how we communicate with one another – in our role as sentries and responders – is more important than ever. Developing broad partnerships to shore up our individual portions of the border is critical to both individual and collective success.

If these are the problems – economics and psychology, now everyone cares, and a lack of interior, how do we address them? How can we really make progress?

EO 13636 FRAMEWORK

First, to address the economics and psychology problem, we are trying to take a different approach.

Starting in the summer of 2012, we began a dialogue with the private sector regarding alternative paths, using a voluntary approach, and focusing on a way to make it easier for companies to assess their cybersecurity – to do it in a way that would make the problem and solutions understandable to decision-makers and to base it on how businesses operate. That approach resulted in the executive order on improving cybersecurity protections for critical infrastructure.

Written over the fall of 2012, President Obama signed EO 13636 on February 12, 2013. The EO has a lot packed into it for a short document, but it really directed Federal agencies to do three things to raise the baseline level of cybersecurity in critical infrastructure:

1) Increase information sharing with the private sector and our external partners;
2) Initiate a transparent, inclusive process to harness the best thinking in the government and private industry on basic cyber best practices and standards; and to
3) Protect privacy and civil liberties while doing these things.

The EO charged the National Institutes of Standards and Technology (NIST) with leading the Framework development process. I'm happy to report that participation in the process was robust; we ended up with over 4,000 comments on the Framework. As a result, I can truly say that this is your Framework – it represents the best consensus of the community regarding how to do cybersecurity. And that's because industry, academia, privacy advocates, the cyber-geeks – um, I mean the *cyber intelligentsia* – really stepped up and provided thoughtful input, and made the Framework relevant and comprehensible to decision-makers.

And the way NIST worked – facilitating, distilling, pulling together the incredible knowledge and capability within the private sector to create the Framework – really is a model for how government needs to work in this area.

So what does the Framework do?

The Framework references globally recognized standards and practices to help organizations understand, communicate, and manage their cyber risks.

The Framework also offers guidance for how organizations can address privacy and civil liberties as part of their efforts to secure themselves.

The Framework as three key benefits:

First, the Framework's greatest strength is that it is deeply rooted in how businesses actually manage risk in the real world. In taking a **risk management approach,** the Framework recognizes that no organization can or will spend unlimited amounts on cybersecurity. Instead, it enables a business to make decisions about how to prioritize and optimize their cybersecurity investments. And it focuses on enabling organizations to factor people into the process.

Second, the Framework offers a **flexible benchmarking tool** for a wide range of organizations.

- For organizations that don't know where to start, the Framework provides a road map.
- For organizations that are already sophisticated, the Framework offers a yardstick to measure against – and to use in communicating with partners and suppliers.

Finally, the Framework creates a **common vocabulary** that can be used to effectively communicate about cyber – among different sectors, different business functions, and different organizational levels. The Framework is emerging as an important tool for technologists to communicate with organizational leaders on managing cyber risks.

I also would note that the recent response to the Heartbleed vulnerability served as a great real-world example of the Framework in action. In responding to Heartbleed, the federal government worked through all of steps outlined in the Framework (Identify, Detect, Protect, Respond, Recover) and is so doing validated its efficacy as an approach to cybersecurity.

This is really a major turning point in the cybersecurity discussion. We believe that we now have a new shared vocabulary about cybersecurity that will allow CEOs, governors, and policymakers around the world to set baselines and improve upon them.

The Framework is a good step toward beginning to address the economics and psychology of cybersecurity.

SHAPE THE FUTURE

In addition to the Framework, we are working on another solution to address the problem of managing our border-filled landscape with no interior. We are focusing on ways that we can make the internet more secure by default by focusing on passwords.

Everyone knows passwords are terrible, yet they remain the most prevalent security method.

One of our big priorities – and one where we think there is a major role for the private sector to play – is the President's *National Strategy for Trusted Identities in Cyberspace* (NSTIC). In a nutshell, NSTIC is an effort to work in partnership with the private sector to catalyze a marketplace – the "Identity Ecosystem" – where all Americans can soon choose from a variety of new types of identity and authentication solutions to use online in lieu of passwords.

If we are serious about closing off the most commonly exploited vectors of attack, we simply have to start with the password – and work to build a market for stronger authentication technologies that consumers and businesses can easily use and trust.

Beyond the weaknesses of passwords, there are a lot of transactions that are not online today in both government and the private sector because there is no easy way to formally confirm identities. To be clear, the goal here is not solely to replace the password. It is to create a marketplace where the market incentivizes the continual update of authentication technologies as better methods come along. At risk of overusing a cliché, the one constant in cybersecurity is change. Our expectation has to be that the technologies we deploy are modular and standards-based so our solutions can evolve as rapidly as our adversaries' attacks are evolving. In NSTIC, the President has challenged the private sector to create solutions to address this.

NSTIC seeks to address this not only through new technologies, but also by directly tackling some of the barriers that the marketplace has, to date, failed to overcome: interoperability, liability, usability, and privacy are among them. A privately-led Identity Ecosystem Steering Group has formed to address these barriers, and is currently working to create a framework of standards and policies that can underpin the identity ecosystem.

Not only is NSTIC a great example of a way we can make cyberspace inherently more secure, it is an example of a strong public-private partnership approach. And projects that industry and government have piloted under NSTIC are starting to come to fruition now. This is not vapor-ware. These are real, workable solutions that are emerging, and this represents an opportunity to make progress on a really hard problem.

So NSTIC and the identity management issue is one example of how we can flip the economics of cyberspace to make the ecosystem favor the defenders. We need more interest in these kinds of solutions, and we need more of them.

INTERNET GOVERNANCE

Finally, to address the issue that now *everyone* cares about how the internet works, we are actively addressing internet governance issues.

We are working with other governments and international organizations on preserving the freedoms and openness of the internet, while trying to increase the security and reliability of this collective resource.

To that end, we are using the United States' *International Strategy for Cyberspace*, to further implement a positive agenda for Internet governance, an agenda that reflects our global leadership role in securing an open, interoperable cyberspace.

A key part of this agenda is the multi-stakeholder approach to Internet governance. Now, that's a mouthful of a phrase – but this is a critical concept for all of us.

The multi-stakeholder approach means that everyone can and should have a voice in how we manage this collective resource – not just governments. Think about that for a minute – we've never tried managing something truly global using this kind of approach before. And that means that everyone needs to actively participate in that discussion, and support the forums where the necessity of a broad base of stakeholders is recognized and valued.

This approach to managing the Internet is what gives it power, dynamism, and growth potential. And it is under threat.

It is not enough to assume that the status quo that has enabled the Internet to thrive as an open interoperable platform will simply endure. We face a real risk that the multi-stakeholder approach – which has enabled the Internet to bring citizens greater transparency, dissidents a protected voice, and economies increased growth – may soon change, and not for the better. Some governments see the Internet as a thing to be controlled and are calling for an intergovernmental approach to do just that.

Those of us who are already benefitting from the free flow of information and commerce know that this approach would fragment the internet, slow the pace of innovation, and hamper global economic development.

So rather than retreat from the multi-stakeholder approach, now is in fact the time for the U.S. to redouble our support for it. Now is the time for us to make clear that we are "all-in" on this governance framework, making it truly global in fact – not just in theory.

So how do we do that? First, we agree that internet governance needs some updating. The organizations, institutions, and other stakeholders that form the Internet governance ecosystem have called for this multi-stakeholder process to evolve.

For our part, the United States has begun the process to transition key Internet domain name functions to the global multi-stakeholder community. As the first step, the Commerce Department is asking The Internet Corporation for Assigned Names and Numbers (the nonprofit organization that coordinates the Internet's global domain name system) to convene global stakeholders to develop a proposal to transition the current role played by the Commerce Department in the coordination of the Internet's domain name system. We are actively supporting transition of this function to a non-government entity, which is consistent with U.S. support for the multi-stakeholder model of Internet governance.

Second, we – all of us – must take steps to enable the internet's continued success. The United States is actively supporting the tools that enable the openness of the cyber ecosystem. We are doing this by taking a number of specific actions:

- We are supporting the development and maturation of national computer incident response teams (CIRTs) through training, enhanced information sharing, and resources.
- We are promoting ***norms of behavior for states in cyberspace*** that respect fundamental freedoms of expression and association, respect intellectual property rights, build trust and reduce the risk of miscalculation and escalation among States, and protect individuals from arbitrary or unlawful interference with their privacy online.
- We are helping the developing world build its capacity to participate fully in the economic benefits of the internet.
- We are improving our own support to fighting international cyber-based crimes through proactively reforming our process for providing digital evidence to other countries. We are going to step up to make that process more efficient, transparent, and responsive – for both U.S.-based companies and foreign government partners. But we are going to do this while preserving appropriate protections for privacy and civil liberties.
- And finally, we are implementing confidence building measures – like increased sharing of cyber threat information – to strengthen our partnerships with other nations.

But we are only one stakeholder in this great cyber ecosystem, we still need others to do their part. We need the private sector to be vocal and proactive in supporting multi-stakeholder Internet governance and building capacity to support broader participation, too.

<u>NO INTERIOR</u>

So how are we addressing the third problem I mentioned, the lack of interior and the shared nature of cyberspace? In effect, each of the efforts I have described today tackle that problem in different ways.

- The Framework was developed collaboratively between government and many different companies – it is shared.

- The NSTIC is a great example of public-private partnership. Although the government has started this solution, to be successful, it must evolve to become private sector driven and maintained.
- And the multi-stakeholder approach to internet governance is inherently a shared endeavor. By strengthening on this approach, we are fundamentally acknowledging that cybersecurity is a shared mission that crosses all sorts of boundaries.

CONCLUSION

We have indeed made progress. Cybersecurity is an inherently hard problem – for at least the reasons I cited and probably many more. But over the past few years, we have started efforts that I think can actually alter the cyber landscape in some foundational ways.

- The Framework provides a way to raise the level of cybersecurity in our critical infrastructure. It gives us a lexicon to have long overdue conversations between the government and the private sector, between private sector companies, and within companies.
- NSTIC offers a real way forward to killing off passwords on replacing them with something much better, something more secure and that protects privacy.
- And reinvigorating and making the multi-stakeholder approach to internet governance truly global can give an effective voice to everyone who cares about the internet: governments, civil society, businesses, and individuals alike.

But in security, there is no such thing as "done." There is only "better." So we still need to focus on continuing to make progress.

We need all of you to continue to provide feedback and make the Cybersecurity Framework a living, community-owned document.

And we need you to encourage all of your fellow sentries on the boarder – that is, your business partners and suppliers – to adopt the best practices for security that we have all identified, and support our collective security and resilience.

We need the identity ecosystem envisioned by NSTIC to become real.

And we need all stakeholders to stand up to preserve the free flow of information and commerce by supporting the multi-stakeholder approach to governing the internet.

And by doing these things, we can – together – make out future better.

Thank you.