Testimony of

Steven R. Chabinsky

Before the
United States Senate
Committee on
Homeland Security and Governmental Affairs

“Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape”

May 10, 2017

Introduction
Good morning Chairman Johnson, Ranking Member McCaskill, and distinguished Members of the Committee. I am pleased to appear before you today to discuss cyber threats facing America. In particular, the Committee has asked that I provide an overview of the cybersecurity landscape from the threats of "criminal, malicious, industrial espionage, and warfare actors." The Committee also asked that I share my views of how the country should approach cybersecurity threats moving forward.

My Background
For almost twenty years, I have been committed to reducing the security risks associated with the misuse of emerging technologies. After joining the FBI in 1995, I became Principal Legal Advisor to the multiagency National Infrastructure Protection Center in 1998. From there, I continued to serve as the FBI's top cyber lawyer and, in 2006, I joined the ranks of the Senior Executive Service and was charged with the responsibility of building and leading the FBI's cyber intelligence program. I later served as Acting Director of the Joint Interagency Cyber Task Force and as the senior cyber advisor to the Director of National Intelligence, followed shortly thereafter by my selection as Deputy Assistant Director of the FBI Cyber Division. In 2012, I joined the cybersecurity technology firm CrowdStrike, becoming its first General Counsel and Chief Risk Officer. During this period, I also developed and taught a *Cyber Law and Policy* graduate class at George Washington University, and volunteered as a senior advisor to the DoD-led Purposeful Interference Response Team.

Last year, I served as one of twelve members of the non-partisan White House Commission on Enhancing National Cybersecurity. We issued our *Report on Securing and Growing the Digital Economy* ("White House Cybersecurity Commission Report") this past December.

Today, I am the global chair of the Data, Privacy, and Cybersecurity practice at White & Case, an international law firm with 40 offices in 28 countries. I also have been selected to serve on the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. In addition, and since 2013, I have been the cyber tactics columnist for *Security* magazine. I focus my column on cyber risk management techniques, to include most prominently the NIST Cybersecurity Framework.

The observations and conclusions I will share today are in my personal capacity, and are the culmination of a career spent in government, industry, media, and academia.

I. We Are Losing.

We have heard it all before. The cyber threat is real and growing. Our vulnerabilities are real and growing. Our reliance on technology is real and growing. The harm from cyberattacks is real and growing. Consumer cyber risk is real and growing. Corporate cyber risk is real and growing. Government agency cyber risk is real and growing. The risk to our national security is real and growing. The amount of time, money, and talent that our country is diverting from other issues and devoting to cybersecurity is real and growing. All of these problems are real and growing, and they are getting worse.

In short, we are losing. The nation that invented the Internet, and so many of the connected technologies the Internet has made possible, increasingly is falling prey to it.

Why is this happening? With so many companies and agencies doing so much, how can America be losing the cybersecurity battle, and how do we set things right?

There are two primary lines of thought. There are those, the majority in fact, who believe we are pursuing the correct overall strategy, but that we are failing -- for any number of reasons -- in its tactical execution. Those who believe our strategy is sound are likely to focus on measures that network owners and operators can take, but currently are not, to better protect themselves. Examples of this line of thinking include both federal and state demands asking "more" of the millions of businesses and individuals that use the Internet: more cyber risk management plans and programs, more critical infrastructure regulation, more information sharing, more – indeed continuous – network monitoring, more software patches, more workforce development, more data breach lawsuits, more lessons learned, and more money spent.

But there is another line of thought, and it is the one to which I subscribe. There are those, like I, who believe we are pursuing a failed strategy, and that doing more of the tactics that underlie that failed strategy is an exercise in futility with diminishing and even negative returns. For those of us who believe that the strategy itself is to blame, there is a deep frustration at seeing our problems grow worse in the face of our well-intentioned national effort. It is like seeing somebody pushing harder and harder to open a door, when instead they should be pulling.

Those who believe, as I do, that our strategy is to blame, seek a paradigm under which we no longer insist that millions of American businesses and individuals constantly do more to protect themselves from the growing list of organized crime groups and hostile powers. We recognize the inevitability of targeted cyberattack, and are more likely to consider those who suffer computer breaches to be victims, rather than culprits. We believe that the government's primary role is to protect its citizens (and business interests), rather than to better enable citizens and businesses somehow to protect themselves against foreign aggression, and against all odds. In short, we seek strategies that remove the major responsibilities and costs of cybersecurity from the end-users of technology, in favor of higher level, international, public/private solutions that inure to the common good. We want the United States government to lead this security effort with stronger vision, urgency, and unstoppable resolve, and to do so in

coordination with and to the economic benefit of industry. We believe this is possible, but it will require a new way of thinking.

II. Who and What Are We Up Against?

I am convinced that given enough time, motivation, and funding, a determined adversary will always be able to penetrate a targeted system. What follows is a representative sample of the nature of the threat.

A. Criminals Seeking Financial Gain

It is important at the outset to demonstrate that today's cybercrime is organized, evidencing skill and logistics that really can seem like the movies. Take for example the international group that, in 2012 and 2013, hacked into the computer system of a credit card processor, found the database containing prepaid debit cards, changed security protocols, increased balances, eliminated account withdrawal limits, and distributed card numbers to members throughout the world. Essentially, the crew's heist was limited only by the amount of money in the ATMs they robbed, as well as an individual's physical capacity to carry thousands of $20 bills. Which leads to the following question: If an organized cyber group hacked into a credit card processor, created debit cards, distributed them to casher cells in 24 countries, who then conducted 36,000 transactions, how much money would they steal in 10 hours? The answer: approximately $40 million.

Depending on the region of the world, cybercriminals also can find safe harbor in working with government intelligence officers. This past March, the Department of Justice indicted four defendants, two of whom were officers of the Russian Federal Security Service (FSB) and who are charged with protecting, directing, facilitating, and paying the two other criminal hackers. Their alleged crime was breaking into Yahoo's email system and stealing information from approximately 500 million accounts. According to Federal prosecutors, the FSB was interested in gaining access to the accounts of Russian journalists, U.S. and Russian government officials, and a number of private sector employees. Meanwhile, one of the criminals decided to use his access to turn a profit by facilitating a spam campaign.

Not that foreign countries are above engaging in financially motivated hacking. North Korea is the number one suspect behind last year's attempt to rob Bangladesh Central Bank of nearly one billion dollars. Although the intruders were unable to fulfill that tall an order, they did manage a payday that exceeded $80 million.

B. Malicious Actors Not Seeking Financial Gain

One of the more troubling episodes we witnessed recently was the rise of Internet of Things (IoT) botnets, and the potential to use them to conduct disruptive attacks against

Internet infrastructure. One security company recently estimated that hackers hijacked more than 2.5 million IoT devices in 2016, primarily by using source code that was released for a piece of malware known as Mirai. In October of last year, a distributed denial of service attack was launched against a company called Dyn, which is a Domain Name System provider that helps other companies resolve the common domain names of websites to their corresponding IP addresses. Once Dyn was flooded with DDoS traffic (some of it said to have been generated by infected baby monitors of all things), it had a domino effect that impacted the services of over 70 companies, including popular media and ecommerce sites. The clear lessons learned are (1) that we have been quick to deploy billions of IoT devices, with billions more on their way, having little to no security; and (2) that we are only as secure as our third party infrastructure (together with our and their response and continuity plans).

C. State-Sponsored Industrial Espionage.

The private sector continues to find itself having to defend against foreign military and intelligence services seeking to steal their intellectual property. Sometimes these thefts are clearly related to anticompetitive desires, in which competing products are brought to market through state-owned companies or closely affiliated privatized firms. At other times, the theft of trade secrets may be tied to the national security concerns of the sponsoring country, as may be the case when military equipment plans are stolen. Still at other times, the stolen property can have a dual use (such as engines), or be viewed as so economically or societally important to the country that for the nation it is viewed as a matter of national security (such as may be the case with oil refinement techniques, or pandemic-related health research).

Regardless, incidents of foreign-sponsored espionage are never far from the headlines. A recent security report found that, of more than 600 data breach incidents they tracked in the manufacturing sector in 2016, over 90 percent could be defined as state-affiliated espionage. Meanwhile, on April 27, 2017, the Department of Homeland Security released an Incident Report that warned of an “emerging, sophisticated campaign” that has been going on for roughly a year targeting victims in information technology, energy, healthcare and public health, communications, and critical manufacturing. Although attribution has not definitively been made, early indications point to a foreign espionage campaign.

D. Cyber Warfare.

Our critical infrastructure networks are run by computers known as industrial control systems or, simply, control systems. These systems are designed for accuracy, extreme environmental conditions, and real-time response in ways that are often incompatible with the latest cybersecurity technologies, inconsistent with consumer grade hardware and software, and in conflict with common network protocols. As a result of these performance factors and limitations, engineers traditionally have been

responsible for the design, operation and maintenance of control systems, rather than IT managers. Yet, despite their uniqueness, control systems are increasingly reliant upon common network protocols, and connectivity often exists between control systems and enterprise networks, to include the Internet. The result? Critical infrastructure throughout the world is connected to the Internet, creating ready targets for cyber warriors.

Just this past February, Ukraine accused Russian hackers of continuing to target their power grid and financial system. This comes after a December 2016 hack into multiple energy distribution companies in Ukraine, also allegedly by Russia, which left tens of thousands of people without electricity for hours. According to reports of the event, Ukrainian energy company employees arrived at work only to see their computers taken over, with the cursers literally moving around monitors under someone else's remote control. 30 substations are said to have been taken offline in this way.

Closer to home, consider as a possible harbinger of things to come in the United States the rolling blackouts in 2003 that left 55 million people without power. The extent of the failure resulted from a software glitch that, unknown to systems operators, left the control room without any audio or visual alarms for over an hour. The operators thought everything was okay because the computers told them everything was okay.

In another example, known as Operation Aurora, as a proof of concept Idaho National Laboratory physically destroyed a hulking 2.25MW diesel generator in 2007 by way of a cyberattack, causing the machine to shake violently, erupt with smoke, and shoot out shrapnel as far as 80 feet away. And then there was the 2010 Stuxnet worm, in which malware targeted Iran's nuclear centrifuges in order to sabotage the country's ability to enrich uranium gas. Foreign countries and terrorist organizations most certainly have taken note of cyber vulnerabilities within the energy sector.

III. What If Everyone Implemented The NIST Framework?

NIST's Cybersecurity Framework is a thoughtful, elegant, and simply stated document, but don't let that fool you. Attempting to implement it is enormously difficult and costly. This is not because the NIST Framework is poorly crafted, quite the opposite. The majority of security professionals appear to agree that the NIST Framework is about as good as you can get. Its goals are certainly easy to understand, but they are operating in a complex risk environment. As a result, understanding what is expected under the Framework and being able to achieve it are two different things.

By way of analogy, imagine for a moment being provided with the following list of five requirements to implement a space mission:

1. Rocket ship required to reach the moon is established
2. All astronauts are informed, properly suited, and trained
3. Resilience requirements to land on moon without damage are established
4. Adequate capacity to ensure return to Earth is maintained

5. Resilience requirements to land on Earth without damage are established

Clearly, each of these steps is a lot easier said than done, and the list reads like a joke. However, should you think this comparison to cybersecurity is farfetched, pause to consider the details and the enormity of the challenges behind each of the NIST Cybersecurity Framework's 98 specifically recommended outcomes (which, no less, must be achieved while under attack):

1. Physical devices and systems within the organization are inventoried
2. Software platforms and applications within the organization are inventoried
3. Organizational communication and data flows are mapped
4. External information systems are catalogued
5. Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value
6. Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
7. The organization's role in the supply chain is identified and communicated
8. The organization's place in critical infrastructure and its industry sector is identified and communicated
9. Priorities for organizational mission, objectives, and activities are established and communicated
10. Dependencies and critical functions for delivery of critical services are established
11. Resilience requirements to support delivery of critical services are established
12. Organizational information security policy is established
13. Information security roles & responsibilities are coordinated and aligned with internal roles and external partners
14. Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
15. Governance and risk management processes address cybersecurity risks
16. Asset vulnerabilities are identified and documented
17. Threat and vulnerability information is received from information sharing forums and sources
18. Threats, both internal and external, are identified and documented
19. Potential business impacts and likelihoods are identified
20. Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
21. Risk responses are identified and prioritized
22. Risk management processes are established, managed, and agreed to by organizational stakeholders
23. Organizational risk tolerance is determined and clearly expressed
24. The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
25. Identities and credentials are managed for authorized devices and users
26. Physical access to assets is managed and protected
27. Remote access is managed
28. Access permissions are managed, incorporating the principles of least privilege and separation of duties

29. Network integrity is protected, incorporating network segregation where appropriate
30. All users are informed and trained
31. Privileged users understand roles & responsibilities
32. Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities
33. Senior executives understand roles & responsibilities
34. Physical and information security personnel understand roles & responsibilities
35. Data-at-rest is protected
36. Data-in-transit is protected
37. Assets are formally managed throughout removal, transfers, and disposition
38. Adequate capacity to ensure availability is maintained
39. Protections against data leaks are implemented
40. Integrity checking mechanisms are used to verify software, firmware, and information integrity
41. The development and testing environment(s) are separate from the production environment
42. A baseline configuration of information technology/industrial control systems is created and maintained
43. A System Development Life Cycle to manage systems is implemented
44. Configuration change control processes are in place
45. Backups of information are conducted, maintained, and tested periodically
46. Policy and regulations regarding the physical operating environment for organizational assets are met
47. Data is destroyed according to policy
48. Protection processes are continuously improved
49. Effectiveness of protection technologies is shared with appropriate parties
50. Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
51. Response and recovery plans are tested
52. Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
53. A vulnerability management plan is developed and implemented
54. Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools
55. Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
56. Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
57. Removable media is protected and its use restricted according to policy
58. Access to systems and assets is controlled, incorporating the principle of least functionality
59. Communications and control networks are protected
60. A baseline of network operations and expected data flows for users and systems is established and managed.
61. Detected events are analyzed to understand attack targets and methods

62. Event data are aggregated and correlated from multiple sources and sensors
63. Impact of events is determined
64. Incident alert thresholds are established
65. The network is monitored to detect potential cybersecurity events
66. The physical environment is monitored to detect potential cybersecurity events
67. Personnel activity is monitored to detect potential cybersecurity events
68. Malicious code is detected
69. Unauthorized mobile code is detected
70. External service provider activity is monitored to detect potential cybersecurity events
71. Monitoring for unauthorized personnel, connections, devices, and software is performed
72. Vulnerability scans are performed
73. Roles and responsibilities for detection are well defined to ensure accountability
74. Detection activities comply with all applicable requirements
75. Detection processes are tested
76. Event detection information is communicated to appropriate parties
77. Detection processes are continuously improved
78. Response plan is executed during or after an event
79. Personnel know their roles and order of operations when a response is needed
80. Events are reported consistent with established criteria
81. Information is shared consistent with response plans
82. Coordination with stakeholders occurs consistent with response plans
83. Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
84. Notifications from detection systems are investigated
85. The impact of the incident is understood
86. Forensics are performed
87. Incidents are categorized consistent with response plans
88. Incidents are contained
89. Incidents are mitigated
90. Newly identified vulnerabilities are mitigated or documented as accepted risks
91. Response plans incorporate lessons learned
92. Response strategies are updated
93. Recovery plan is executed during or after an event
94. Recovery plans incorporate lessons learned
95. Recovery strategies are updated
96. Public relations are managed
97. Reputation after an event is repaired
98. Recovery activities are communicated to internal stakeholders and executive and management teams

And to what end? Unfortunately, we lack sufficient metrics to determine whether and to what extent the NIST Cybersecurity Framework and similar international standards are cost-effective. In fact, we lack the metrics to determine whether and to what extent they are effective at all in the face of today's evolving threat. If vulnerability mitigation was

inexpensive and easy to implement, one might be inclined to have everyone do it under the theory that it couldn't hurt; but, that is not the case.

IV. Can Trying to Become Impenetrable Make Things Worse?

As industry and government agencies continue to spend greater resources on vulnerability mitigation, they find themselves facing the problem of diminishing economic returns and perhaps even negative economic returns.

With respect to diminishing returns, information security professionals typically recognize cost effective benefits when applying baseline cybersecurity efforts. However, as companies direct their resources either against low probability events, or on pursuing all available defenses regardless of the ease with which an adversary can counter them, the amount of protection received for each dollar spent becomes progressively smaller and ultimately is worth less than the expenditure.

Imagine for example trying to protect a building by spending two million dollars on a 20-foot brick wall. Meanwhile, an adversary can go to a hardware store and for less than one hundred dollars buy a 30-foot ladder.

Far worse though than the concept of diminishing returns is the concept of negative returns, in which well-intentioned efforts actually make the problem worse. Although it often is difficult to convince good people that they are responsible for escalating a problem, consider our brick wall again. What if the defender spent ten million dollars to build an eighty foot wall? Instead of a buying a ninety foot ladder, the adversary might decide to use an explosive device to get through the wall, perhaps even killing people in the process. Comparing the brick wall to cybersecurity, there is reason to believe that our strategy often has the unintended consequence of threat actors escalating their capabilities and methods, and proliferating advanced malware, to include ransomware, which is increasingly destructive.

V. A Better Approach: Shift the Burden Away from End Users

It is not possible or optimal for every person and every company to be on the frontlines of cybersecurity. Instead, we should focus on fewer, higher level solutions that benefit everybody.

Shifting the burden away from end users will require a sustained international effort to tackle common Internet and communications ecosystem threats, such as eliminating botnets that infect millions of victims and can take down power grids. As stated in the White House Cybersecurity Commission Report, "to the maximum extent possible, the burden for cybersecurity must ultimately be moved away from the end user—consumers, businesses, critical infrastructure, and others—to higher-level solutions that include greater threat deterrence, more secure products and protocols, and a safer Internet ecosystem." It is worth expanding upon these concepts.

A. We should ratchet up threat deterrence.

In order to get security risks under control, whether in the "physical" or cyber worlds, security experts rely upon the levers of vulnerability mitigation, threat reduction and, should the first two fail, consequence management.

In the physical world, threat reduction – achieved primarily through threat deterrence – has been our predominant approach, and it has been largely successful. Throughout the physical security spectrum, whether describing the safety of nations, businesses, or individuals, safety most often is achieved because potential aggressors are deterred out of the fear they will be brought to justice, and actual aggressors ultimately are brought to justice. By way of contrast, our physical safety is not primarily reliant upon missile defense shields, gates, and body armor.

Yet, in the area of cybersecurity, vulnerability mitigation has been our nation's predominant approach, both for securing private sector and government systems. We have retained this focus on vulnerability mitigation despite it being well understood that securing networks is a daunting task even for the most experienced. It also would appear that while relying upon a vulnerability-mitigation-first strategy could work to protect static, isolated environments (such as fortresses and missile silos), there are no obvious examples of it working in dynamic environments when they are expected to interoperate with threat actors (such as the Internet).

It is my conclusion then that the bad guys, whether criminal or military, will not relent unless we improve our abilities to detect, identify and penalize them using all elements of national power. Doing so will require significantly maturing our strategies to focus on how the government and the private sector can coordinate and enhance our Diplomatic, Information, Military, Economic, and Law Enforcement (DIME/LE) options in order to deter or punish significant cyber threat actors. Similarly, the government and the private sector must resolve how to work together to jointly defend the nation in cyberspace.

We also must supplement our law enforcement and intelligence resources to focus on our adversaries. As an international group of scientists led by the University of Cambridge succinctly wrote in 2012, "we should spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more in response – that is, on the prosaic business of hunting down cyber-criminals and throwing them in jail." For this to occur, we will need to reconsider how we fund cybersecurity efforts. Currently, the U.S. federal IT security budget is roughly $18 billion. Meanwhile, law enforcement funding is counted in the millions of dollars, with relatively few of the FBI's 35,000 employees trained as cyber intrusion Special Agents.

Our underfunding threat deterrence also hurts the private sector, which largely has been left to fend for itself. One financial institution disclosed that it planned to spend $600 million and dedicate 2,000 employees to cybersecurity last year.

Shifting our primary focus away from vulnerability mitigation in favor of threat deterrence would align our cybersecurity efforts with the security strategies we use in the physical world. In the physical world, vulnerability mitigation efforts certainly have their place. We take reasonable precautions to lock our doors and windows, but we do not spend an endless amount of resources in hopes of becoming impervious to crime. In fact, after taking routine measures, vulnerability mitigation has a relatively low return on investment. As a result, to counter determined thieves, we ultimately concede that an adversary can gain unlawful entry but, through the use of burglar alarms and video cameras, we shift our focus instead towards instant detection, attribution, threat response, and recovery. When the alarm monitoring company calls a business owner at 3 a.m., it does not say, "We just received an alarm that your front door was broken into. But, don't worry, we've called the locksmith." Rather, it is only obvious that the monitoring company calls the police. It is surprising then and suggests a larger problem that, in the world of cyber, when the intrusion detection system goes off the response has been to call the Chief Information Security Officer, and perhaps even the CEO, to explain what went wrong and to have them prevent it from happening again.

B. We should pay for a safer Internet ecosystem

Taking care of problems at the source, before they spread to consumers, businesses, and critical infrastructure, only makes sense. By way of analogy, when faced with the Flint Michigan water crisis, a federal state of emergency was declared, and solutions are being put in place to repair and upgrade the city's water system and to replace the pipes. Nobody would imagine opting instead for a solution to require every home and every business operating in Flint to purchase their own state of the art water filtration system along with the experts needed to continuously monitor and upgrade them.

To move forward with purpose, the Federal government should publish a Request for Proposal seeking innovative solutions. Financially incentivizing the private sector to solve the problem should be considered a budget priority, with perhaps as much as ten percent of our roughly $600 billion defense budget being set aside for the advancement of higher level cybersecurity solutions. In addition, we should consider expanding the telecommunications model we have in place to Connect America, which created a fund to expand rural access to voice and broadband, by implementing a program to Protect America by establishing a fund to extend cybersecurity across all of America. We often hear leaders say the private sector is on the front lines of cybersecurity. I agree, and it is well past time we pay them to defend us.

Similarly, we should promote alternative architectures that focus on threat deterrence. When thinking of cybersecurity, it is worth considering the Nineteenth Century findings of Charles Darwin. Despite the seeming simplicity of the well-known phrase "survival of the fittest," Darwin did not mean to suggest that survival of the fittest should always be considered in terms of health or strength. Rather, the fittest must be considered in terms of being the right fit for a particular purpose. Survival typically requires adaptability in areas other than health or strength, and adaptability can occur by chance

or by design. With due consideration of our economic and national security, as well as the health and welfare of the public, our government should be working with the private sector -- by design -- to adapt our security in a manner that best promotes our survival.

Unfortunately, at best we appear to be leaving decisions about the cybersecurity of our nation's critical infrastructure, and potentially therefore our nation's survival, either to chance, to prevailing market forces, or to the world community.

At worst, our declining security actually has occurred by our own design. Consider for a moment that, to date, the design elements of our policies, technologies, and resource allocations have focused on functionality, interoperability, bandwidth, speed and, more recently, anonymity and privacy. Our design elements have not focused on the security of our critical infrastructure. These choices – notably applied to a manmade, controllable environment – are directly responsible for the depth and breadth of our current unfavorable cybersecurity situation. Yet, despite our design choices, network security professionals routinely are being asked to do the impossible in the form of building trusted, impenetrable, dynamic, interoperable networks out of untrusted components, within untrusted environments, using untrusted supply chains, that rely upon untrusted vendors and untrusted users.

We would do well to take Darwin's findings to heart, and begin to use our public/private partnerships in part to explore alternative models in which hardware, software, protocols, and policies are adapted to better suit the wide range of global use scenarios relating to security and privacy. For example, it is hard to imagine that to this day computers that are used for transmitting classified information (or for enriching uranium for that matter) can accept the same USB thumb drive and fall victim to the same malware as a common computer in a public library. My regular car cannot even accept a diesel pump at the gas station.

We should establish public/private partnerships to determine whether trusted networks require a combination of distinct design elements, to include enhanced identity management, maximized intrusion detection and attribution capabilities, and prioritized actions to locate and penalize bad actors. Similarly, uniquely defined networks operating internationally, with common Terms of Service, might assist nations (and perhaps even non-governmental organizations) agree on principles for transborder access to data in order to prevent imminent danger to life, limb, or property.

Regardless of the solution space, the international and multi-disciplinary aspects of these considerations require substantial government leadership and private sector initiative (similar to the origins of the Internet itself.) To get started, we just might find that the critical infrastructure networks that are in need of the greatest security are, by coincidence, networks that require the least privacy, providing fertile ground for developing systems that not only are hardened, but that better promote authentication, detection, attribution, and global norms that penalize their breach.

C. We should promote market transparency of security.

Products, protocols and systems should be secure by design and by default, their complexity reduced, and their security capabilities disclosed. For starters, and as expressed in the White House Cybersecurity Commission Report, the Internet of Things is of particular concern, and we should pursue strategies "to achieve security by default in all connected devices and to ensure that the consumer and integrator alike know what security capabilities are, or are not, contained in these devices."

One possible approach is for the Federal government to foster the development and adoption of security labels on products, similar to nutrition labels on food, and linked to a clear rating system. We also must focus on reducing system complexity, in order to push back on the trend, which the Commission observed, that "[a]s the size and complexity of software and computing systems continue to grow, more vulnerabilities are exposed and introduced into environments that are increasingly difficult to manage."

D. We should focus on emerging threats to wireless capabilities.

The 9/11 Commission famously reported its belief that the 2001 terrorist attacks revealed four kinds of U.S. Government failures: "imagination, policy, capabilities, and management." Although the government undoubtedly recognizes the need to be predictive and preventative in the area of security there is insufficient collaboration to counter the vast emerging risks presented by purposeful interference.

Many of our nation's essential functions are highly dependent upon wireless communications across the electromagnetic (EM) spectrum. The disruption of GPS location and timing information in and of itself could have cascading effects on the synchronization of computer networks (to include those responsible for financial transactions), vehicle tracking, coordinated movement of people and cargoes, law enforcement offender tracking, surveying, precision agriculture, and a host of other disparate services. Additional disruption capabilities, such as through radio frequency jammers, could create "quiet" zones around wireless networks and end-users, preventing the transmission of vital communications from reaching their intended recipients.

DHS seems particularly well suited to lead an effort that coordinates actions across the government and with the private sector to better detect, collect, centralize, analyze, and respond to purposeful interference events. Strengthening public/private partnerships to address these and other emerging threats would further reduce the cyber risks to our critical infrastructure.

E. We should develop and share better metrics.

As the White House Cybersecurity Commission Report expressed, “Most current efforts to measure cybersecurity effectiveness focus on the actions taken by an organization, rather than on those actions’ effectiveness.” The Commission therefore recommended the establishment of a Cybersecurity Framework Metrics Working Group to help address that gap, and recommended that “NIST should provide fact-based metrics to establish whether and to what extent use of the Framework is effective.” These points cannot be emphasized enough. We currently are spending billions of dollars on projects for which the value proposition is unknown, and we likely are losing fleeting opportunities to better address the risk.

F. We should promote legal certainty and harmonization

Regulators also should get their respective acts together by harmonizing their rules around common metrics-based cybersecurity principles, as well as with one another, and by producing cost-estimates of adequate compliance schemes. Congress should favor national approaches to Internet privacy and cybersecurity over the current patchwork of state-by-state laws, which introduce cost, legal uncertainty, and transactional delay to interstate and international commerce.

The United States as a whole should then promote international standards that foster security, privacy, and interoperability in ways that make it easier for businesses to innovate and operate with certainty across geopolitical boundaries.

VI. Conclusion: There is Room for Optimism, If We Change Course.

I am convinced that the cyber threat is an existential threat that challenges our democracy and significantly alters our nation's potential. I am convinced that how we rise to the cybersecurity challenge will determine whether our nation's best days are ahead of us or behind us. I am convinced that we currently are going in the wrong direction and that, if we keep doing what we are doing, the overall cyber threat against our country will continue to grow to unsustainable levels.

At the same time, I am convinced our downward spiral is not inevitable and that we can improve our security considerably. However, doing so will require that we reconsider, rather than refine and redouble, the nature of our efforts.

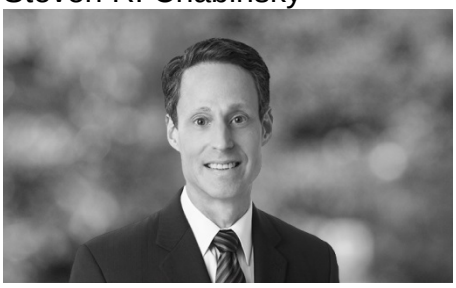
It is my hope for our future that the blame for, and the costs of, cybercrime, cyber espionage, and cyber warfare, will fall more squarely on the offenders than on the victims, and that in doing so we will achieve greater threat deterrence; that we will call upon those businesses and standards bodies that drive the Internet and communications ecosystem to bring forward and implement internationally orchestrated measures that provide higher level, innovative security solutions for the shared benefit of all technology users, and that we readily pay the private sector to do so as a key profit center for them; and, that we build more rigor and transparency into hardware and

software security functions, to enable sophisticated purchasers to use market forces to drive more secure product development.

Ultimately, it is my hope that businesses and consumers will benefit from improved, sustained cybersecurity at lower costs and with less user responsibility; and, above all, that our nation will remain secure so that our country's best days still lie ahead.

Thank you for the opportunity to testify today. I would be happy to answer any questions you may have.

Steven R. Chabinsky



Steven Chabinsky is the global chair of the Data, Privacy, and Cyber Security practice at White & Case LLP, an international law firm, and the cyber tactics columnist for *Security* magazine. He previously served as a member of the non-partisan White House Commission on Enhancing National Cybersecurity, the General Counsel and Chief Risk Officer of CrowdStrike, Deputy Assistant Director of the FBI Cyber Division, and the senior cyber advisor to the Director of National Intelligence. While at the FBI, Mr. Chabinsky also organized and led the FBI's cyber intelligence program, and prior to that was the FBI's top cyber lawyer. Mr. Chabinsky is the recipient of numerous awards and recognitions, including the National Intelligence Distinguished Service Medal. He can be reached at chabinsky@whitecase.com, and can be followed on Twitter: @StevenChabinsky.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu