Testimony of

Steven R. Chabinsky

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

"*Strengthening Public-Private Partnerships to Reduce Cyber Risks to our Nation's Critical Infrastructure* "

March 26, 2014

Introduction

Good morning Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee. I am pleased to appear before you today to discuss cybersecurity partnerships among the federal government, states, and the private sector to secure critical infrastructure. In particular, I have been asked to describe my views on partnerships with Federal agencies to increase security and resiliency, including the Cybersecurity Framework and other provisions outlined in the Executive Order issued by President Obama on February 12, 2013.

Background

I have spent over fifteen years committed to reducing the security risks associated with emerging technologies. Most of my efforts have been with the Federal Bureau of Investigation, where I last served as Deputy Assistant Director of the Cyber Division, after having organized and led the FBI's cyber intelligence program and having served as the FBI's top cyber lawyer. Today, I am the General Counsel and Chief Risk Officer of the cybersecurity technology firm CrowdStrike, as well as an adjunct faculty member of George Washington University and the cyber columnist for *Security* magazine. The observations and conclusions I am sharing today in my personal capacity are the culmination of a career spent in government, industry, and academia. It was over 15 years ago that I started to cut my teeth on issues relating to public/private partnerships, then in my capacity as the Principal Legal Advisor to the multi-agency National Infrastructure Protection Center. From that time forward, I have had the privilege of collaborating with the dedicated, patriotic men and woman who have comprised, among other groups, InfraGard, the National White Collar Crime Center (NW3C) and the Internet Crime Complaint Center (IC3), the National Cyber-Forensics & Training Alliance (NCFTA), the Financial Services Information Sharing and Analysis Center (FS-ISAC), and the National Cybersecurity and Communications Integration Center (NCCIC). With that background, what follows are some of my direct observations about the challenges and evolution of our public/private efforts.

The History of U.S. Public-Private Partnerships for Cybersecurity

For quite some time now, government and industry have been investing substantial time and money on public/private cybersecurity partnerships. Indeed, it was back in 1998 that Presidential Decision Directive 63 introduced us to the term "Information Sharing and Analysis Center," or ISAC. Government agencies began to facilitate the creation of sector-specific and multi-sector groups, all with eager anticipation that, by working together, the government and the private sector would prove unstoppable. We believed that through public/private partnerships we could gather, analyze, sanitize and disseminate just the right amount of timely and actionable intelligence to allow the good guys to better defend themselves *while the government identified the bad guys and brought them to justice*.

Noble intentions aside, early in the history of U.S. public/private cyber partnerships, we confronted a host of legal questions that demanded answers. Private sector companies asked whether information sharing partnerships would violate antitrust laws. "No," said the Department of Justice in 2000. Not as long as the information sharing exchanges are open on a non-discriminatory basis to sector members, and are limited to information about security program best practices and the identification of vulnerabilities.

The private sector then expressed concern about the Freedom of Information Act, asking whether the government is required to disclose sensitive information it receives from its industry partners. Again "no," this time from federal courts, which began to hold as early as 1992 that the government can withhold security information from FOIA disclosure as long as the information sharing was voluntary and the company normally would not provide that information to the public. Congress then passed the Critical Infrastructure Information Act of 2002 to statutorily protect certain information from being released under FOIA.

Next came issues of trust, the emergence of legally binding non-disclosure agreements, time-consuming background checks, a review of government classification procedures, consideration of the sticky problem of global companies wanting to share sensitive government threat and vulnerability information with their security officers abroad, as well as our government wanting to share sensitive U.S. business vulnerability information with the law enforcement and intelligence agencies of other countries. Then there were the actual partnership meetings, during which time a significant number of people emerged as free riders who shared nothing and only participated for a chance to mingle and develop business.

As for those participants who truly came to make a difference, the General Accountability Office found that the majority of industry's expectations of working with the government was not being met with respect to the receipt of timely and actionable cyber threat information or cyber alerts. Finally, victim reluctance to report computer intrusions to law enforcement become further exacerbated when the Federal Trade Commission began to eye the corporate victims of cybercrime as "defendants" who

engaged in unfair or deceptive trade practices for lacking effective security, all but eviscerating a decade's worth of confidence building measures by the Department of Justice which had offered constant reassurance that the government's approach is not to blame but to help the victims of cybercrime.

Lessons Learned form Public/Private Partnerships

Fifteen years of lessons-learned have led me to reach a number of conclusions. First, I have found that the most promising joint government/industry outcomes have been and likely will remain at the strategic level rather than at the tactical level. This includes, for example, the sharing and co-development of risk management plans and security best practices, as well as conducting joint incident response training exercises. The Cybersecurity Framework is a shining example of such an effort, prepared by NIST after having worked with over 3,000 individuals and organizations on standards, best practices, and guidelines. I applaud NIST's efforts, and I recommend that every corporate officer and director read the Framework and consider applying its straightforward approach to cybersecurity enterprise risk management.

Second, although we now know that information sharing initiatives between the government and the private sector have inherent limitations when it comes to collecting and disseminating large quantities of time sensitive data for tactical purposes, they are well suited to support collaborative efforts where the parties work together strategically to identify and substantially resolve specific, high-risk, continuing problems. In this regard, a seminal work of public/private collaboration remains the 2009 FBI, FS-ISAC, NACHA joint publication on Automated Clearinghouse Account Hijacking. In that instance, the FBI briefed financial services industry representatives on each of the Bureau's major financial cybercrime cases; the FS-ISAC determined from that what information was timely, unique (meaning not already known by the industry), and relevant for its members; and, together, the FS-ISAC and NACHA recommended solutions that were cost effective and capable of eradicating a problem that otherwise was nearing half a billion dollars in fraud. The key was collaboration, rather than the mere pushing of information. The FBI and industry worked together to identify both the problem and the solution set. Unfortunately today, some five years later, there are indications that it is far more common for government agencies to send information to industry sectors without a coordinated approach as to the information's timeliness, uniqueness, and relevance, and without first obtaining and including industry recommendations on how recipients can best make use of the information and track its utility. As a result, industry is concerned that government information sharing is becoming a numbers game in which the passage of large quantities of "indicators and warning" is viewed in and of itself as a metric of success regardless of outcomes.

Third, while the government often warns the private sector about ongoing or imminent cyber intrusions, more must be done in partnership with the private sector to focus on raising the costs to the attackers. It is time for the government and industry to join

forces to develop and implement technologies and policies that focus less on the vulnerability mitigation aspects relating to information assurance, and more on the threat mitigation aspects of hacker detection, attribution, and punitive response necessary to achieve sustained security. By way of analogy, if foreign fighter planes were on their way to the United States, everyone would be thankful for a government warning to relocate to a bomb shelter. Perhaps sheltering would last for five minutes, or five hours, or even five days, as the government engaged in aerial combat against the threat. But, in cyber, some foreign economic espionage intrusion campaigns have lasted for over ten years, and industry is not seeing from the government an effective plan to confront, repel, and defeat the intruders. To similar effect, Distributed Denial of Service (DDoS) attacks allegedly by North Korea in 2009 and by Iran in 2012 and 2013 have been viewed as the private sector's problem to weather, rather than a confrontation that demanded government engagement.

Fourth, in recognition of the global aspects of both the cyber problem and its solutions, the government and private sector must work together to envision and then drive strategically effective international standards, norms, research and development and multilateral relationships that better position threat deterrent models for the long term. Yet, since 1997, our government has taken concerted actions to privatize and reduce U.S. governance of the Internet. As a result, despite the right aspirational language in the President's 2011 International Strategy for Cyberspace, it is not evident how "the United States will ensure that the risks associated with attacking or exploiting our networks vastly outweigh the potential benefits." To date, the inescapable truth is that the risks associated with attacking and exploiting U.S. networks have been negligible, and the private sector has been left largely on its own – under the threat of government regulation and class action lawsuits no less – to defend itself against all enemies.

The Need to Reassess Our Public/Private Cyber Partnerships

1) <u>The Need to Focus on Threat Deterrence Instead of Vulnerability Mitigation</u>

In light of the fact that our increased cybersecurity efforts have not led to a leveling off (no less a reduction) of the threat, it makes sense to question our strategy and to get back to basics. In particular, we would do well to consider how we have successfully reduced security risks in other settings and then try to apply those concepts here.

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 is most often achieved because potential aggressors are deterred out of 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, fortresses, 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. As stated in Verizon's 2013 Data Breach Investigations Report, "breaches are a multi-faceted problem, and any one-dimensional attempt to describe them fails to adequately capture their complexity." On the technical side—the web servers, e-mail servers, databases, firewalls, routers, embedded network devices, internal networks, global remote access, custom applications, off-the-shelf applications, backup and storage areas, and all telephone, PBX, and VoIP systems require attention. On the human side, the physical infrastructure must be protected, employee accesses and permissions must be restricted, and connections to business and corporate partners (often operating under different legal regimes) have to be managed. Of course, these are just the basics, and each aspect of cybersecurity must be monitored and updated regularly, as the technologies, users, and adversaries change constantly.

In order to reduce the likelihood of harm, information security professionals deploy a wide range of defensive controls. In the risk management community these are commonly referred to as *technical* controls. Examples of technical controls include password access, endpoint activity monitoring, firewalls, and intrusion detection and prevention systems. Technical controls are particularly well suited to reduce the time necessary to detect unlawful activity and to substantially limit the consequences of a successful breach. Still, although technical controls often are a necessary component of security, they are seldom sufficient. Security professionals also commonly deploy *physical* controls (such as locks on doors) and *administrative* controls (such as acceptable computer use policies and pre-employment background checks). To get a better feel for the difficulties of being a cybersecurity professional, it is worthwhile to consider, at the 30,000 foot level, the following seventeen different categories that NIST recommends network defenders review (keeping in mind that each of these is then broken down further into more discrete, tactical methods):

1. access control;
2. awareness and training;
3. audit and accountability;
4. certification, accreditation, and security assessments;
5. configuration management;
6. contingency planning;
7. identification and authentication;
8. incident response;
9. maintenance;
10. media protection;
11. physical and environmental protection;
12. planning;
13. personnel security;
14. risk assessment;
15. systems and services acquisition;
16. system and communications protection; and
17. system and information integrity.

Continuously reviewing and implementing the technical, physical, and administrative controls within each of these seventeen categories is a never-ending and costly process, which ultimately will not eliminate cyber risk entirely.

Making matters worse, as industry and government agencies continue to spend greater resources on vulnerability mitigation, they finds 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 devise 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 that is increasingly destructive.

2) <u>The Need for the Government to Provide for the Common Defense</u>

Compounding the unrealistic push for industry to build impervious systems, our government has grown increasingly reliant upon the owners and operators of our networks to be primarily responsible for defending themselves. By way of example, the public/private partnership efforts set out in Presidential Executive Order 13636 are for the government to share enough cyber threat information with specifically targeted U.S. private sector entities “so that these entities may better protect and defend themselves against cyber threats.” In this manner, our government cybersecurity strategy risks morphing into a game of hot potato where, instead of the government fulfilling its traditional role of stopping the threat actor, our agencies now quickly pass information along to the targeted victims and wipe their hands of it. Remarkably, the government appears to expect that corporate America will stop well-resourced, determined, sophisticated actors using a defensive paradigm that is exorbitantly expensive, has proven ineffective over time, and has no precedent of success against persistent threats.

For this reason, we should remain skeptical of government efforts that redirect, rather than supplement, our law enforcement and intelligence resources away from their traditional focus on our adversaries. Despite a sincere effort to declassify and deliver thousands of reports to targeted victims, there is little or no support for the proposition that the private sector can convert this information into a meaningful defense of our critical infrastructure against potential acts of terrorism and foreign aggression. The same holds true with respect to government warnings of cybercrime. 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."

3) The Need to Incorporate Threat Deterrence into Alternative Architectures

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 can accept the same USB thumb drive and fall victim to the same

malware as a common computer in a public library. 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.)

4) The Need for Public/Private Partnerships Relating to Emerging Threats

The 9/11 Commission famously reported its belief that the 2001 terrorist attacks revealed four kinds of U.S. Government failures: "in imagination, policy, capabilities, and management." These words come to mind when considering the lack of public/private partnerships that focus on identifying and countering emerging threats.

Although the government undoubtedly recognizes the need to be predictive and preventative in the area of security there is insufficient collaboration, for example, 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.

On the government side, the multi-agency Purposeful Interference Response Team (PIRT), managed by the Department of Defense, acts as the federal coordination body for cases of suspected purposeful interference with space systems. Still, the full extent of purposeful interference issues and coordinating opportunities appears to be broader than the PIRT's mandate, funding, and authorities. As stated in 2012 by U.S. Navy Admiral Jonathan Greenert: "Inexpensive jammers, signal detectors, computer processors, and communication systems make it easier today for unfriendly states, terrorists, and criminals to affect our ability to use the EM-cyber environment." The same year, Department of Homeland Security (DHS) official Robert Crane expressed that "we must seek ways for protecting radio frequencies with the goal of rapidly identifying, locating, and mitigating interference sources when they occur and ensuring communications, information and navigation capabilities are secure, resilient, and rapidly restored after an incident." DHS seems particularly well suited

to lead such an effort by coordinating 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.

Conclusion

There is no doubt that cyber threats present considerable risk to our economic and national security interests, and that these threats continue to grow at an alarming rate. Despite billions of dollars of investment in cybersecurity defensive efforts, and the prospect of spending billions of dollars more, many experts see no hope on the horizon that the overall cyber threat against our country will level off, no less begin to decline. It is my professional opinion that this downward spiral is not inevitable and that we can improve our security considerably. However, it also is my professional opinion that improving our security posture requires that to a certain extent we reconsider, rather than simply redouble, the nature of our efforts.

Fundamentally, we need to ensure that our cybersecurity strategies, technologies, market incentives, and international dialogue focus greater attention on the challenges of more quickly detecting and mitigating harm in high risk environments, while in parallel locating and penalizing bad actors. Doing so 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. Instead, 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 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, immediately necessary, and the reason people purchase alarm systems, that they call the police to stop the felon. 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 prevent it from happening again. It is my hope for the future that the blame for, and the costs of, cybercrime will fall more squarely on the offenders than on the victims, that in doing so we will achieve greater threat deterrence, and that businesses and consumers will benefit from improved, sustained cybersecurity at lower costs.

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 Senior Vice President of Legal Affairs, General Counsel, and Chief Risk Officer for CrowdStrike, a big data cybersecurity technology firm that specializes in continuous threat detection, cyber intelligence, and computer incident response. Steve also serves as an adjunct faculty member of George Washington University, and as the cyber columnist for *Security* magazine. Before joining CrowdStrike, Mr. Chabinsky had a distinguished 17-year career with the government, culminating in his service as Deputy Assistant Director of the FBI's Cyber Division. Prior to that role, Mr. Chabinsky organized and led the FBI's cyber intelligence program, and was the FBI's top cyber lawyer. Mr. Chabinsky also served in the Office of the Director of National Intelligence (ODNI), where he rose to become Acting Assistant Deputy Director of National Intelligence for Cyber, Chairman of the National Cyber Study Group, and Director of the Joint Interagency Cyber Task Force.

A graduate of Duke University and Duke School of Law, Mr. Chabinsky began his legal career as an associate with Simpson Thacher & Bartlett in New York, and as a law clerk for the Honorable Dennis Jacobs of the United States Court of Appeals for the Second Circuit. Mr. Chabinsky is the recipient of numerous awards and recognitions, including the National Intelligence Distinguished Service Medal. In 2012, he was named one of *Security* magazine's "Most Influential People in Security." He can be followed on Twitter @StevenChabinsky.