CYBER SECURITY: PROTECTING AMERICA'S NEW FRONTIER

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

NOVEMBER 15, 2011

Serial No. 112–80

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE
71–238 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

LAMAR SMITH, Texas, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
DENNIS ROSS, Florida
SANDY ADAMS, Florida
BEN QUAYLE, Arizona
MARK AMODEI, Nevada

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
MIKE QUIGLEY, Illinois
JUDY CHU, California
TED DEUTCH, Florida
LINDA T. SÁNCHEZ, California
[Vacant]

SEAN MCLAUGHLIN, *Majority Chief of Staff and General Counsel*
PERRY APELBAUM, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*
LOUIE GOHMERT, Texas, *Vice-Chairman*

BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
J. RANDY FORBES, Virginia
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
SANDY ADAMS, Florida
MARK AMODEI, Nevada

ROBERT C. "BOBBY" SCOTT, Virginia
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
SHEILA JACKSON LEE, Texas
MIKE QUIGLEY, Illinois
[Vacant]

CAROLINE LYNCH, *Chief Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

NOVEMBER 15, 2011

CYBER SECURITY: PROTECTING AMERICA'S NEW FRONTIER

TUESDAY, NOVEMBER 15, 2011

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to call, at 10:03 a.m., in room 2141, Rayburn House Office Building, the Honorable Louie Gohmert (Vice-Chairman of the Subcommittee) presiding.

Present: Representatives Gohmert, Scott, Deutch, Forbes, Marino, Gowdy, Lungren, Jackson Lee, and Goodlatte.

Staff present: (Majority) Caroline Lynch, Subcommittee Chief Counsel; Arthur Radford Baker, Counsel; Sam Ramer, Counsel; Lindsay Hamilton, Clerk; Vishal Amin, Counsel; (Minority) Joe Graupensberger, Counsel; Veronica Eligan, Professional Staff Member.

Mr. GOHMERT. The Subcommittee will come to order.

Welcome to today's hearing on cyber security. I would especially like to welcome my witnesses and thank you for joining us today.

I am joined today by the distinguished Ranking Member of the Subcommittee, Bobby Scott, and by the most recent Chairman Emeritus, Mr. Conyers, who as I understand will be coming shortly.

I want to welcome everybody to the hearing on "Cyber Security: Protecting America's New Frontier." The Internet revolutionized our society in many ways. While its benefits abound and extend from our largest corporations to remote rural regions throughout the Nation, individuals in the United States and abroad have unfortunately been able to exploit the Internet for criminal means.

Cyber crime often is faceless and has proven to defy traditional investigative prosecutorial tools. As a result, the frequency of cyber crime is growing rapidly and now includes many international criminal syndicates and is threatening our economy, our safety and our prosperity.

Even more worrisome are the national security implications of cyber intrusion. We in Congress are concerned that we are witnessing the opening salvos of a new kind of conflict waged in cyberspace.

As we learned in the Wikileaks case, one individual with access to classified data can threaten America's national operational security, and as we saw from China's cyber attack on Google and other

companies, America's edge in innovation and technical superiority can be compromised by competing countries who make theft of intellectual property a national strategy.

As recently reported in the Fiscal Times, China's brazen use of cyber espionage stands out because the focus is often corporate and part of a broader government strategy to help the develop or help develop the country's economy.

Quote, I've been told that if you use an iPhone or a BlackBerry everything on it—contacts, calendar, emails—can be downloaded in a second. All it takes is someone sitting near you on a subway waiting for you to turn it on and they have got it, said Kenneth Lieberthal, a former senior White House official for Asia who is at the Brookings Institution.

One security expert reported that he buys a new iPad for each visit to China and then never uses it again.

The problem remains that the United States government does not own the networks through which all data flows, as totalitarian regimes like China do. Your government and industry must team up at times to secure the networks and create digital shields to protect our country and our business.

The Administration has recently released a cyber security initiative proposal which aims to make changes to the cyber security structure and laws of the United States. We will look at the proposal today and we have a distinguished panel of experts here to help guide the Committee on what changes should be made to protect citizens from cyber criminals.

One thing is clear. We have learned that computer crime is just as important as ordinary crime and should be treated just as harshly by our criminal justice system. The risks to our national infrastructure and our national wealth are profound and we must protect them.

Besides our national security, we have something in this country as precious as wealth—our civil liberties. When it comes to cyber crime, Americans are fully engaged on the issue of protecting our civil liberties and privacy. They are correct to be so concerned, and we on this side of the aisle share their concern.

Sometimes it seems like a dilemma. By using Facebook and other websites, Americans are putting more of their private lives on the Internet than ever before. Yet, more Americans are concerned about privacy than ever before.

But it is understandable the more Americans rely on the Internet for their work, their entertainment, their relationships, the more productive and connected they become. But they also become vulnerable in new ways.

It is truly a new frontier for our country and this Committee is determined that this new frontier will not be a Wild West. Our challenge is to create a legal structure flexible enough to protect our interests while allowing the freedom of thought and expression that made this country great. I am convinced we can thread this needle.

I look forward to hearing more about this issue and thank all of our witnesses for participating in this hearing. It is now my pleasure to recognize for his opening statement the Ranking Member of the Subcommittee, Congressman Bobby Scott of Virginia.

Mr. SCOTT. Thank you, Mr. Chairman.

I am pleased that we are conducting a hearing today on the important issue of cyber security. It is a critical issue. It is critical that we work together in Congress with the Administration and with the business community and with private advocates to find ways to enhance the security of our government information systems, our business computer networks and the personal use of the Internet.

Last spring, the Administration sent to Congress a comprehensive cyber security legislative proposal. I was, frankly, disappointed that they called for mandatory minimum sentences for certain crimes of damaging critical infrastructure computers because mandatory minimums have been found to waste the taxpayers' money, do nothing about crime and require sentences that often violate common sense.

Resolving the significant issues relating to cyber security including protecting network access and operating aspects of our critical infrastructure is a very challenging problem.

We must not shrink from the challenge but sentencing individuals who have been convicted of serious crimes is also a serious challenge as it requires individualized determination of what the person actually did, the harm they caused and the circumstances of the crime.

And that's why Congress actually did something right in this area when it created the U.S. Sentencing Commission whose job it is to establish sentencing guidelines to be used by judges in imposing appropriate sentences. Calling for mandatory minimum sentences shrinks from the challenge of doing this right. While the crime involved may involve—may indeed be serious, imposing mandatory minimum sentences on everyone will not make us more secure.

The code section of the offense violated does not often—often does not accurately reflect the seriousness of the crime. This practice ultimately leads to injustice, cynicism and distress in our criminal justice system and the imposition of sentences that make no sense at all.

Another issue that we need to talk about is the provision requiring notification of the government of certain breaches of sensitive personal information stored in the computer networks of businesses. The bill requires that an entity as of yet unnamed in the Department of Homeland Security shall be notified and that entity should also notify the FBI and Secret Service.

Both of these agencies have specialized expertise that may be called upon depending, for example, whether the crime is one that threatens national security or the integrity of our financial systems.

We need to hear more from the Administration and these agencies on how this would—how this coordination would take place.

In addition, it is important that we examine whether the laws have maintained an appropriate focus on behavior we all believe rises to the level of criminal—Federal criminal liability. The Computer Fraud and Abuse Act was originally enacted to deal with intrusions into computers, what we now call hacking.

Since that time, we have expanded the scope of the law on several occasions which has led to a disturbing expansive use in recent years which have generated concerns on both sides of the aisle.

For example, now it is possible for someone to be prosecuted for violating the user agreement in a social networking site. One of our witnesses is the distinguished law professor who has written extensively about these concerns.

I hope this hearing will give us a chance to discuss these issues and the best approach for refocusing our efforts in this area.

Finally, I note concern about proposals to expand the ability of private companies to share information with government and ultimately with law enforcement for the purpose of protecting against cyber security threats. If we allow vastly overbroad sharing of information, we actually may undermine the very privacy rights which should be at the forefront of our concern.

So I thank all of our witnesses for being with you and thank you, Mr. Chairman, for calling the hearing.

Mr. GOHMERT. And thank you, Mr. Scott.

We now will proceed and it is my pleasure to introduce today's witnesses. Richard Downing is the Chief Deputy or Deputy Chief for computer crime at the Computer Crime and Intellectual Property Section of the United States Department of Justice in Washington, D.C.

Mr. Downing supervises the section's computer crime work including the prosecution of computer hacking, identity theft and other online crimes. Mr. Downing also supervises a wide range of legislative and policy issues relating to computer crime.

These issues include the modernization of the Federal Computer Hacking Statute policy and legislation aimed at improving cyber security, the development of the electronic evidence-gathering laws and efforts to enhance international cooperation in cyber crime investigations.

Mr. Downing received his Bachelor of Arts in political science from Yale University in 1989 and his Juris Doctor from Stanford Law School in 1992.

I will go ahead and introduce all of the witnesses and so we will just take one after the other without your having to be interrupted by me.

The Honorable Michael Chertoff is co-founder and managing principal at the Chertoff Group in Washington, D.C. In addition to his role at Chertoff Group, Mr. Chertoff is also senior of counsel at Covington & Burling LLP and a member of the firm's white-collar defense and investigations practice group.

Prior to his work at Chertoff Group, Mr. Chertoff served as Secretary of the United States Department of Homeland Security from 2005 to 2009. Before heading up the Department of Homeland Security, Mr. Chertoff served as a Federal judge on the U.S. Court of Appeals for the Third Circuit.

Before serving as a judge, he was a Federal prosecutor for over a decade. Mr. Chertoff received his undergraduate degree from Harvard College in 1975 and his Juris Doctor from Harvard Law in 1978.

Mr. James Baker is currently a lecturer on law at Harvard Law School. He most recently served as an Associate Deputy Attorney

General with the United States Department of Justice from 2007 until last month, ending a 17-year career at the Department.

In 2007, Mr. Baker was a Fellow at the Institute of Politics at the John F. Kennedy School of Government at Harvard University and was a lecturer on law at Harvard Law School. From 2001 to 2007, Mr. Baker served as counsel for intelligence policy at the Justice Department where he was the head of the Office of Intelligence Policy Review.

Mr. Baker is a former Federal prosecutor. He received his Bachelor of Arts in government from the University of Notre Dame in 1983 and his Master of Arts in political science and Juris Doctor from the University of Michigan in 1988. He received—okay.

And Professor Orin Kerr—Professor Kerr is a professor of law at George Washington University where he teaches criminal law, criminal procedure and computer crime law.

Before joining the faculty in 2001, Professor Kerr was an honors program trial attorney in the Computer Crime and Intellectual Property Section of the criminal division at the United States Department of Justice as well as a Special Assistant U.S. Attorney for the Eastern District of Virginia.

He is a former law clerk for Justice Anthony M. Kennedy of the U.S. Supreme Court and Judge Leonard Garth of the U.S. Court of Appeals for the Third Circuit. In the summer of 2009 and 2010, he served as special counsel for the Supreme Court nominations to Senator John Cornyn on the Senator Judiciary Committee.

He has been a visiting professor at the University of Chicago Law School and the University of Pennsylvania Law School. Professor Kerr received his Bachelor of Science degree in engineering from Princeton University and his Masters of Science from Stanford University while earning his Juris Doctor from Harvard Law School.

All of the witnesses' written statements will be entered into the record in its entirety and I ask that each witness summarize his testimony in 5 minutes or less.

And at this time then, Mr. Downing, thank you for your patience. Please proceed with your opening statement.

TESTIMONY OF RICHARD W. DOWNING, DEPUTY CHIEF, COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, CRIMINAL DIVISION, UNITED STATES DEPARTMENT OF JUSTICE

Mr. DOWNING. Good morning, Chairman Gohmert, Ranking Member Scott and Members of the Committee.

Thank you for the opportunity to testify on behalf of the Department of Justice regarding the Administration's cyber legislation proposals.

This Committee knows well that the United States confronts serious and complex cyber security threats. The critical infrastructure of our Nation is vulnerable to cyber intrusions that could damage vital national resources and put lives at risk, and intruders have also stolen vast databases of financial information and valuable intellectual property.

At the Department of Justice, we see cyber crime on the rise with criminal syndicates operating with increasing sophistication to

steal from innocent Americans. That is why President Obama has made cyber security a high priority. The Justice Department has done its part.

For example, we have brought a series of important prosecutions, including cases against offenders from overseas, in an effort to build real deterrence.

Despite this good work, the problem is far from solved. It is clear that new legislation can help to improve cyber security substantially.

To that end, the Administration's legislative proposal contains a number of ideas and I would like to take a moment to highlight the parts of that package aimed at improving the tools we use to punish and deter computer crimes.

First, the Administration's proposal includes reasonable and focused changes to ensure that computer crimes are punished to the same extent as other traditional criminal activity.

For example, because cyber crime has become a big business for organized crime groups, the Administration proposal would make it clear that the Racketeering Influenced and Corrupt Organizations Act, or RICO, applies to computer crimes.

Prosecutors have used this statute in the past to charge the leaders of organized crime families for their roles in their criminal enterprises, even where they did not themselves commit a predicate crime such as theft or extortion.

In a similar way, RICO could be used to dismantle criminal enterprises focused on online theft and extortion and not just the people with their fingers on the keyboard.

Also, the proposal would increase certain penalties in the Computer Fraud and Abuse Act, which is the statute used to prosecute hacking offenses so as to harmonize them with analogous traditional laws.

For example, the crime of wire fraud carries a maximum penalty of 20 years in prison, but violations of the Computer Fraud and Abuse Act that involve very similar conduct carry a maximum penalty of only 5 years. Such disparities make no sense.

The Computer Fraud and Abuse Act also currently has limitations that have prevented it from being fully used by prosecutors against criminals who traffic in computer passwords, and these shortcomings should be corrected.

We propose that the scope of the offense for trafficking in passwords should cover not only passwords, but other methods of confirming a user's identity such as biometric data, single-use pass codes, or smart cards used to access an account. This new language should cover log-in credentials used to access any protected computer, not just government systems or computers at financial institutions.

Finally, some have argued that the definition of "exceeds authorized access" in the Computer Fraud and Abuse Act should be restricted so as to disallow prosecutions based solely upon a violation of an employee use agreement or a website's terms of service.

While we appreciate this view, we are concerned that restricting the statute in this way could make it difficult or impossible to deter and punish serious threats from malicious insiders.

The reality of the modern workplace is that employees in both the private and public sectors require access to databases containing large amounts of highly personal and sensitive data.

We need look no further than bank customer service representatives, government employees processing tax returns, and intelligence analysts handling sensitive material. Because they need access in order to do their jobs, it is impossible to restrict their access through passwords or other security mechanisms.

In most cases, employers communicate clear and reasonable restrictions on the purposes for which that data may be accessed.

Employers should be able to set such access restrictions with the confidence that the law will protect them when their employees exceed these restrictions. Improperly accessing personal or commercial information is a serious matter that requires serious criminal consequences.

We must not impair these prosecutions based on unsubstantiated fears that the Department will expend its limited resources on trivial cases such as prosecuting people who lie about their age on an Internet dating site.

Mr. Chairman and Members of the Committee, this is an important topic. The country is at risk and there is a lot of work to be done to stop computer crimes from victimizing and threatening Americans throughout the country.

I look forward to answering your questions here today. Thank you.

[The prepared statement of Mr. Downing follows:]

Department of Justice

STATEMENT OF

RICHARD W. DOWNING
DEPUTY CHIEF
COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION
CRIMINAL DIVISION

BEFORE THE

COMMITTEE ON JUDICIARY
SUBCOMMITTEE ON CRIME, TERRORISM, AND NATIONAL SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES

ENTITLED:

"CYBERSECURITY: PROTECTING AMERICA'S NEW FRONTIER"

PRESENTED

NOVEMBER 15, 2011

Statement Of
Richard W. Downing
Deputy Chief
Computer Crime and Intellectual Property Section
Criminal Division

Committee on Judiciary
Subcommittee on Crime, Terrorism, and National Security
United States House of Representatives

"Cybersecurity: Protecting America's New Frontier"
November 15, 2011

Good afternoon, Chairman Sensenbrenner, Ranking Member Scott, and Members of the Committee. Thank you for the opportunity to testify on behalf of the Department of Justice.

As the Committee is well aware, the United States confronts a dangerous combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and limited comprehensive threat and vulnerability awareness. Within this dynamic environment, we are confronted with threats that are more targeted, more sophisticated, and more serious.

Our critical infrastructure – such as the electrical grid, financial sector, and transportation networks that underpin our economic and national security – have suffered repeated cyber intrusions, and cyber crime has increased dramatically over the last decade. Sensitive information is routinely stolen from both government and private sector networks, undermining confidence in our information systems, the information collection and sharing process, and the information these systems contain.

Recognizing the serious nature of this challenge, the President made cybersecurity an Administration priority upon taking office. During the release of his Cyberspace Policy Review in 2009, the President declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation." The President also highlighted the importance of sharing responsibility for cybersecurity, working with industry to find solutions that improve security and promote prosperity.

Over the past two years, the Administration has taken significant steps to ensure that Americans, our businesses, and our government are building better protections against cyber threats. Through this ongoing work, it has become clear that our Nation cannot improve its ability to defend against cyber threats unless certain laws that govern cybersecurity activities are updated, including the Computer Fraud and Abuse Act ("CFAA").

Members from both sides of the aisle have likewise remained steadfast in their resolve to act on cybersecurity legislation. I want to particularly acknowledge your leadership, Chairman Sensenbrenner, in the effort to address these important threats. The Administration welcomes

the opportunity to assist these congressional efforts, and we have developed a pragmatic and focused cybersecurity legislative proposal for Congress to consider as it moves forward on cybersecurity legislation. This legislative proposal is the latest development in the steady stream of progress we are making in securing cyberspace.

The proposed legislation is focused on improving cybersecurity for the American people, our nation's critical infrastructure, and the federal government's own networks and computers. The aspect of the proposed legislation I want to discuss today is the revisions to the CFAA and related legislation.

The Administration's goals

Over the decades since the CFAA was originally passed, the Justice Department has worked with Congress to keep the statute up-to-date and effective. Over time, we have had several objectives in seeking reform of the CFAA, three of which are of paramount importance today.

Our first objective is to make the CFAA as technology-neutral as possible. Experience has demonstrated that advances in technology at times render statutes in the area of cyber crime obsolete. By drafting them in a technology-neutral way, they remain viable despite technological change. By contrast, statutes defined in terms of specific technologies not only require Congress to expend effort trying to keep them up-to-date, but potentially allow criminals to avoid punishment on a technicality. Our experience has shown that computer crime statutes can be written in a forward-thinking way that accounts for technological change, yet sets forth "rules of the road" that make clear the line between criminal and non-criminal conduct.

Second, Congress should ensure that federal law treats conduct in the online world commensurate with similar physical-world conduct. Penalties for fraud committed using a telephone should not differ, for example, from penalties for fraud committed by computer hacking.

Third, the criminal law should provide appropriately severe penalties to promote deterrence. Computer crime is a burgeoning area of criminality that is difficult to investigate and prosecute. Criminals from across the country and around the world are taking advantage of the relative anonymity provided by the Internet to compromise our critical infrastructure, obtain trade secrets, intrude into bank accounts, and steal the personal and financial information of ordinary Americans. Where ten years ago hackers were more commonly motivated by curiosity or seeking notoriety, most criminal hackers today are motivated by greed. Federal law needs to more effectively deter this spreading criminality.

Computer crimes as a RICO predicate

We propose updating the Racketeering Influenced and Corrupt Organizations Act ("RICO") to make CFAA offenses subject to RICO. As computer technology has evolved, it has become a key tool of organized crime. Indeed, criminal organizations are operating today around the world to: hack into public and private computer systems, including systems key to national security and defense; hijack computers for the purpose of stealing identity and financial information; extort lawful businesses with threats to disrupt computers; and commit a range of other cyber crimes. Many of these criminal organizations are similarly tied to traditional Asian and Eastern European organized crime organizations.

The fight against organized crime is far from over; rather, much of the focus has moved online. RICO has been used for over forty years to prosecute organized criminals ranging from mob bosses to Hells Angels to insider traders, and its legality has been consistently upheld by the courts. Just as it has proven to be an effective tool to prosecute the leaders of these organizations who may not have been directly involved in committing the underlying crimes and to dismantle whole organizations, so too can it be an effective tool to fight criminal organizations who use online means to commit their crimes. The Administration's proposal would simply make clear that malicious activities directed at the confidentiality, integrity, and availability of computers should be considered criminal activities under the RICO statute.

Simplifying the CFAA to appropriately address culpable individuals

The Administration proposal would make a number of changes to the CFAA's sentencing provisions. The goal of these changes is to eliminate overly complex, confusing provisions, simplify the sentencing scheme, and enhance penalties in certain areas where the statutory maximums no longer reflect the severity of these crimes.

First, the proposal would clarify that conspiracy to commit a computer hacking offense is subject to the same potential maximum penalty as a completed, substantive offense. Whether or not a cyber criminal is the person who actually "pushed the buttons" to commit the crime should not matter – the intent of the criminal to commit a serious computer crime is what counts. Indeed, in many of the investigations and prosecutions being handled by the Department today, the most culpable figures are not the lower-level operatives who physically execute a criminal scheme but the leaders who make the key decisions and earn the lion's share of the illicit proceeds. This proposed change would provide greater deterrence by enhancing certain penalties.

Second, we also believe that the penalty provisions in the CFAA should be simplified by removing references to subsequent convictions in favor of setting an appropriate maximum sentence for each offense. In general, the maximum would be the number of years currently designated for a second offense. This approach would eliminate needless complexity in the sentencing scheme and free federal judges to provide appropriate sentences to first-time offenders in instances where the crime was extremely serious or resulted in widespread damage.

Third, our proposal would increase the maximum penalties in several cases to give judges the authority they need to adequately punish serious offenders and to make these penalties commensurate with the same type of conduct occurring off-line. We believe that such modifications are appropriate in light of the scale and scope of our nation's current cyber crime problem.

Moreover, some of the CFAA's sentencing provisions no longer parallel the sentencing provisions for their equivalent traditional crimes. For example, the current maximum punishment for a violation of section 1030(a)(4) (computer hacking in furtherance of a crime of fraud) is five years, but the most analogous "traditional" statutes, 18 U.S.C. §§ 1341 and 1343 (mail and wire fraud), both impose maximum penalties of twenty years.

Indeed, for a serious computer crime offense, it is easy to imagine scenarios in which the appropriate sentence exceeds the current maximum. For example, were a criminal to steal a massive database of credit cards, the maximum penalty under section 1030(a)(2) for that crime is five years in prison, even though the United States Sentencing Guidelines might recommend a much higher sentence. In other words, in such situations, a federal judge would be prevented from sentencing a defendant to an appropriate prison term that will assure proper punishment and promote general deterrence.

All of these changes will empower federal judges to appropriately punish offenders who commit extremely serious crimes, ones that result in widespread damage, or both. Judges would still make sentencing decisions on a case-by-case basis, and defendants would still have the right to appeal any sentence deemed excessive or unreasonable.

Updated tools for investigators and prosecutors

Further, we believe that the CFAA currently has limitations that have prevented it from being used fully by prosecutors against criminals that steal login credentials, such as user names, passwords, or secure login devices. These shortcomings should be corrected. The Administration proposes that the scope of the offense for trafficking in passwords in the CFAA (18 U.S.C. §1030(a)(6)) should cover not only passwords but other methods of confirming a user's identity, such as biometric data, single-use passcodes, or smart cards used to access an account. It should also cover login credentials used to access to any "protected" computer (defined in the statute quite broadly), not just government systems or computers at financial institutions.

This proposal will help equip law enforcement to fight a key area of cyber crime: the theft of passwords and means of access for the purpose of committing additional crimes, such as wire fraud and identity theft. Expanding this definition will improve the ability of federal prosecutors to prosecute these offenders. It will also keep the CFAA up-to-date with changing technology. For instance, if in ten years iris scans have taken the place of passwords as the main method for managing credentials to computer systems, Congress will not have to act because the Administration's proposal would have made the CFAA technology-neutral, allowing it to adapt

to technological change.

Finally, we propose several amendments to the CFAA related to forfeiture. Key amongst these changes would be the addition of a civil forfeiture provision to the CFAA. Unlike most federal criminal statutes with forfeiture provisions, currently the CFAA only provides for criminal, and not civil, forfeiture. This forces federal prosecutors to use criminal forfeiture authority in instances where civil forfeiture would be more appropriate or efficient. The Administration also requests other modest changes to the CFAA forfeiture subsection, namely to clarify that the "proceeds" forfeitable under the CFAA are gross proceeds, as opposed to net proceeds, and allow forfeiture of real property used to facilitate CFAA offenses in appropriate cases.

The proposed civil forfeiture provision is consistent with similar provisions in federal law that have existed for decades. It should also be noted that any use of civil forfeiture authority by the government is subject to both the "innocent owner" defense – which applies when an owner claims that they are innocent of a crime and therefore their property should not be forfeited – and proportionality review under the Eighth Amendment.

Amending the statute to cover "gross" proceeds is also a reasonable clarification. Criminal enterprises should not enjoy the benefits of the ordinary accounting standards and tax rules used by legitimate businesses. All of the monies earned from the crime should qualify for forfeiture because criminals should not be allowed to "deduct" the expenses of operating their criminal enterprise. For example, a drug dealer who buys an expensive car should not be entitled to deduct the price of the car as a cost of doing business.

Enhanced deterrence for malicious activity directed at critical infrastructure

Finally, we recommend strengthening the criminal code to better deter malicious activities directed at computers and networks that control our critical infrastructures. Critical infrastructure consists of the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on national security, national economic security, or public health and safety.

America's open and technologically complex society includes, as a part of its critical infrastructure, numerous vulnerable targets. A significant portion of these are owned and operated by the private sector and state or local governments. These critical infrastructure systems are vulnerable to destruction, incapacitation, or exploitation by a variety of malicious actors, which poses grave risks to our national and economic security. Ordinary criminals could also take advantage of potential vulnerabilities in our critical infrastructure for purposes of extortion.

Specifically, computerized control systems perform vital functions for the critical infrastructure. They are vital in areas ranging from monitoring the distribution and quality of

drinking water to ensuring the safe operation of nuclear power plants. For example, in natural gas distribution, such systems can monitor and control the pressure and flow of gas through pipelines. If a criminal or terrorist seized control of those systems, he or she could potentially disrupt the energy supply or cause an explosion. As the Committee knows, the CFAA creates maximum penalties for malicious activity directed at the confidentiality, integrity, and availability of computers. While these crimes currently apply to the computers and networks that run our critical infrastructure, they do not require any mandatory minimum penalty for such conduct. While it is reasonable to believe that courts would impose appropriate prison terms if malicious activity severely debilitates a critical infrastructure system, it is possible that courts might not impose adequate penalties for activities that cause less disruption – or none at all in the case of an attempt that is thwarted before it is completed.

In light of the grave risk posed by those who might compromise our critical infrastructure, even an unsuccessful attempt at damaging our nation's critical infrastructure merits substantial penalties. The Administration has proposed a mandatory minimum sentence of three years imprisonment as one appropriate way to achieve the needed deterrence. We understand that members of the Committee have raised concerns about mandatory minimum sentencing in general. We are, as always, happy to work with this Committee to explore potential alternatives to a mandatory minimum for attacks on critical infrastructure that not only appropriately punish offenders, but also more effectively deter others who would engage in such misconduct that puts public safety and national security at risk. In whatever form it would ultimately take, the message needs to be sent loud and clear to criminals and other malicious actors that any attempt to damage a vital national resource will result in serious consequences.

Restricting substantive definitions in the CFAA will make it harder to address insider threats

Finally, on behalf of the Department I want to address concerns regarding the scope of the CFAA in the context of the definition of "exceeds authorized access." In short, the statute permits the government to charge a person with violating the CFAA when that person has exceeded his access by violating the access rules put in place by the computer owner and then commits fraud or obtains information. Some have argued that this can lead to prosecutions based upon "mere" violations of website terms of service or use policies. As a result, some have argued that the definition of "exceeds authorized access" in the CFAA should be restricted to disallow prosecutions based upon a violation of contractual agreements with an employer or service provider. We appreciate this view, but we are concerned that that restricting the statute in this way would make it difficult or impossible to deter and address serious insider threats through prosecution.

All types of employees in both the private and public sector – from credit card customer service representatives, to government employees processing tax returns, passports, and criminal records, to intelligence analysts handling sensitive material – require access to databases containing large amounts of highly personal and otherwise sensitive data. In most cases,

employers communicate clear and reasonable restrictions on the purposes for which that data may be accessed. The Department has prosecuted numerous cases involving insiders in both the public and private sectors who have violated defined rules to access and obtain sensitive information. In many prosecutions involving insiders, the "terms of service" and similar rules in employment contexts define whether the individual charged was entitled to obtain or alter the information at issue. This is almost identical to prosecutions under other statutes, in which internal procedures, agreements, and communications must be examined by a fact-finder to determine, for example, whether a particular payment was authorized, or embezzlement or fraud.

Employers should be able to set and communicate access restrictions to employees and contractors with the confidence that the law will protect them when their employees or contractors exceed these restrictions to access data for a wrongful purpose. Limiting the use of such terms to define the scope of authorization would, in some instances, prevent prosecution of exactly the kind of serious insider cases the Department handles on a regular basis: situations where a government employee is given access to sensitive information stored by the State Department, Internal Revenue Service, or crime database systems subject to express access restrictions, and then violates those access restrictions to access the database for a prohibited purpose. Similarly, businesses should have confidence that they can allow customers to access certain information on the business's servers, such as information about their own orders and customer information, but that customers who intentionally exceed those limitations and obtain access to the business's proprietary information and the information of other customers can be prosecuted.

Here are three examples of recent prosecutions under the CFAA that might have been impaired if language restricting the use of terms of service had been enacted into law:

- A police officer obtained criminal history information from the National Crime Information Center database ("NCIC"), a sensitive and tightly-controlled law enforcement database which has stringent rules and regulations restricting access for official purposes. The officer then leaked the information to a defense investigator in a drug trafficking case. This unlawful conduct resulted in the conviction of the officer under the CFAA, with the Court of Appeals noting specifically that the evidence was sufficient to demonstrate that the defendant had "exceeded his authority by accessing [NCIC] for an improper purpose." (*United States v. Salum*, 257 Fed. Appx. 225, 230 (11th Cir. 2007)).

- In 2006, a contract systems administrator for Blue Cross Blue Shield of Florida used his access to the company's computer system to snoop. He initially was curious about how much his colleagues were being paid, but he proceeded to access all kinds of information, including downloading a file with hundreds of thousands of current and former employee names and Social Security Numbers. Pursuant to agreements with his employer, the administrator was obligated to keep company information confidential and to access the

information only for purposes related to his job duties. Although there was no evidence that the employee had yet disseminated the names and Social Security numbers, Blue Cross Blue Shield incurred a cost of over half a million dollars to buy credit monitoring protection for all of the company's employees. Although the employee intensely litigated the issue of whether he had "exceeded authorized access," the court rejected his arguments, and he pled guilty to one count under section 1030(a)(2).

- Up to and through 2008, seven employees of Vangent Corporation accessed the student loan records of a number of celebrities and well-known political and sports figures, include then-candidate Barack Obama, and then disclosed this information to others, including media outlets. These employees required access to the records as part of their employment, but their employment policy prohibited them from accessing the system for non-work-related purposes. Six pled guilty to exceeding authorized access under section 1030(a)(2), and a seventh was convicted following a jury trial in 2010.

These are just a few cases, but this tool is used routinely. The plain meaning of the term "exceeds authorized access," as used in the CFAA, prohibits insiders from using their otherwise legitimate access to a computer system to engage in improper and often malicious activities. We believe that Congress intended to criminalize such conduct, and we believe that deterring it continues to be important. Because of this, we are highly concerned about the effects of restricting the definition of "exceeds authorized access" in the CFAA to disallow prosecutions based upon a violation of terms of service or similar contractual agreement with an employer or provider.

Conclusion

I very much appreciate the opportunity to discuss with you our proposals to address the threat cyber crime poses to our national security, public safety, and economic prosperity. The Administration has responded to Congress' call for input on the cybersecurity legislation that our Nation needs, and we look forward to engaging with Congress and, specifically, this Committee as you move forward on this important issue.

Mr. GOHMERT. Thank you very much.

At this time, Mr. Chertoff, we will hear from you.

TESTIMONY OF THE HONORABLE MICHAEL CHERTOFF, CO-FOUNDER AND MANAGING PRINCIPAL, THE CHERTOFF GROUP

Mr. CHERTOFF. Thank you, Mr. Chairman. Thank you, Ranking Member Scott and Members of the Committee. I am delighted to testify here today.

It is actually my first return to Congress as a witness since I left office 3 years ago and I used to testify in this room about border security.

Mr. GOHMERT. Yes, you did, and I knew you couldn't stay away.

Mr. CHERTOFF. Right. It is hard to stay away.

This is a very important look at an important topic. It is a topic that includes, obviously, concerns about criminal behavior but is much broader than that. I would argue that the issue of cyber security is now at the very top of the list of security threats faced by the United States.

We have seen multiple dimensions of the threat. Some of them involve massive acts of criminality. I remember when I was Secretary we prosecuted the theft of literally tens of millions of credit card numbers which were used to steal money from credit card companies and from individual customers.

But beyond that, we have seen the use of cyber attacks as a way of stealing very valuable intellectual property including national security secrets and these are reported almost on a daily or weekly basis.

Beyond that, there is the obvious concern about our industrial control systems which could in some circumstances be attacked in a way that might actually cause serious damage to property and serious loss of life.

We have seen examples back in 2007 and 2008 that are declassified of attacks against Estonia or Georgia, which are really part of what you could very well argue is a new way of war making.

So this has got to be dealt with in a number of different dimensions. Certainly, the criminal law is part of it but I would argue there are some other elements as well.

Broadly speaking, I would say there are three concerns we have in terms of vulnerability. One is the network itself and how to protect the network, and that is in many respects a technical problem.

But the supply chain is also a problem. We are living in a global environment in which hardware and software is fabricated around the world and our degree of confidence about whether there are malicious bits of code or other malicious tools embedded in our hardware or software is not what it needs to be.

And perhaps most significantly is the insider threat. While many people think the biggest problem with cyber security is somebody hacking across a network, experience shows that in many cases it is the insider who wittingly or unwittingly introduces malware into the system in a way that causes an enormous amount of damage.

To this end, I would commend an article written a couple years ago in Foreign Affairs by then-Deputy Secretary Bill Lynn who described a major intrusion into our defense networks as having been caused by somebody picking up a thumb drive and putting it into a laptop as an act of negligence.

So we have got to deal with all of these problems and one of my observations over the years I have worked on this issue is a tendency to believe there is a magic bullet. There is no magic bullet.

So I would argue that there are several things that we need to do. I think the current Administration proposal is a good start but it is a start. It is not an end.

First, I think we need to have tougher penalties and I in the main approve and applaud the proposals put forward by the Administration in that respect. Second, we need to make information sharing much easier.

Time and again, when the private sector suffers an intrusion, the ability to get technical assistance about the nature of what that intrusion is is hampered by uncertainties in the law about whether the U.S. government and the private sector can share information. This has got to be made much easier and much more streamlined and I think, again, the proposal here is a good start.

Third issue is how do we build standards of cyber security in our critical infrastructure. If we have a failure of critical infrastructure in, let's say, the electric grid, there will be enormous collateral consequences.

Unfortunately, the value of the damage often exceeds the value of the asset, which means that there is no market incentive for the asset owner to invest in protecting the asset. We have got to change that. Again, I think the Administration has begun with a good start in talking about having standards for cyber security.

I am concerned about two things. One, how do we enforce the standards. I am not sure naming and shaming is sufficient. And second, we are talking about a very complicated and detailed rulemaking process which may take a considerable amount of time to complete, and the problem is time is not on our side.

Finally, I conclude by observing that there is a larger national security dimension here involving the problem of cyber warfare, the actual use of cyber tools as an adjunct to military operations, and here we need to be clear about what our policy is in responding to those acts of war and we need to have a declared policy of deterrence, how we are going to prevent these from happening.

This is work that is beginning but it has got a ways to go. I would be happy to answer questions.

[The prepared statement of Mr. Chertoff follows:]

Statement for the Record

The Honorable Michael Chertoff

Co-Founder and Managing Principal of The Chertoff Group

Before the

United States House of Representatives

Subcommittee on Crime, Terrorism and Homeland Security

November 15, 2011

Mr. Chairman, Representative Gohmert, Members of the Subcommittee:

Thank you for the opportunity to be here today and to contribute to the important effort being undertaken to better secure our most critical systems and networks operating in cyberspace. These operations are essential to our daily lives, global commerce and national security – and as a result – they continue to be targeted and attacked daily by a variety of actors ranging from today's modern-day criminals interested in pure financial gain to nation states seeking stronger advantages for their own global competitiveness. In my opinion, this persistent cyber threat represents one of the most novel and seriously disruptive threats to our national security since the onset of the nuclear age sixty years ago.

Since I left government in January 2009, I have continued to work on cyber security matters and have a greater appreciation of the challenges being faced by BOTH the private and public sector. I do want to make sure to inform this Committee from the start that within my private capacity as both Co-Founder of The Chertoff Group and Senior of Counsel with Covington and Burling, LLP, I do consult with companies on cybersecurity-related issues that could be discussed here today. However, my opinion and testimony today is wholly my own. In addition, these points being presented in my written statement will also appear in a cyber-security publication to be published by the Aspen Institute later this year.

In 2008, President George W. Bush ordered the launch of the Comprehensive National Cyber Security Initiative (CNCI), a now-declassified twelve point strategy to address cyber security threats across the civilian and military, government and private domains. The Department of Defense and the Department of Homeland Security convened a group of government and business leaders to address cyber security issues, under the rubric Enduring Security Framework. Shortly after taking office, President Barack Obama ordered a review of the CNCI, and subsequently reaffirmed the mandate to proceed with a national cyber initiative. President Obama appointed a White House official to coordinate strategy and Congress has taken up possible legislation.

Despite these various government initiatives, there is in place no comprehensive strategy for cyber defense and security. Recently, Deputy Secretary of Defense William Lynn described the Defense Department's evolving

approach to defending against cyber attacks, which are escalating as a serious counterintelligence and warfighting issue. Soon thereafter, Deputy Homeland Security Secretary Jane Lute responded with an opinion piece asserting that the internet is not a war zone, and arguing for a number of measures that the private sector can undertake to reduce its vulnerabilities to cyber attacks. This was followed by a Department of Homeland Security paper that elaborated on some characteristics of a more secure cyber "ecosystem". This summer, the Department of State issued an international cyber-strategy and the Department of Defense announced a cyber security information sharing pilot with certain major defense companies. At the same time, the Administration offered a legislative proposal to promote cyber security among operations of critical infrastructure.

But while these pieces approach and characterize the challenge of threats to our cyber systems, they do not yet amount to a unified vision of the problem and solution sets. Indeed, it sometimes seems that those examining the problem are talking past each other. At one end of the spectrum are those who portray cyber risks as verging on the catastrophic, sketching cyber combat scenarios that result in extinguishing our civilization. At the other end of the spectrum, are those who claim it's all overblown, and that the issue of cyber security is about updating virus protection and good police work.

To those who have been around the security community over the last decade, this will sound much like the familiar debate about terrorism, between those who claim it's a criminal problem to be addressed by law enforcement, and those who argue that terrorists have declared a war that must be fought with military capabilities.

In fact, the dichotomy between these approaches is oversimplified in the case of terrorism, and even more inadequate to define a strategy for protecting our cyber assets. Forcing cyber security into a simplified unitary framework limits our choices and underestimates the complexity of the most novel and serious disruptive threat to our national security in decades. Cyber threats will sometimes be a central dimension of military posturing and warfighting, and when they are critical will require the response of all elements of national power. On the other hand, much destructive activity is occurring at the commercial and individual level where military-type approaches are ill suited and where the actors are largely part of the

private sector. If we debate the way forward in protecting cyber assets as a philosophical choice between "militarizing the internet" or letting the market play the primary role, we rob ourselves of the full range of resources that we might mobilize.

Our ability to fully develop and implement national strategies for cyber security is hampered also by a tendency of the government agencies who participate to examine the problem from the perspective of their own authorities and capabilities. Abraham Maslow famously said that when you carry a hammer, everything looks like a nail. Our agencies carry different tool sets and often regard problems as whatever they can fix using the tools they carry. Our intelligence agencies in particular are rightly strongly conditioned to sharply restricting their activities within the United States and as relating to United States persons. But while there are legal rules that require this, at least the nonconstitutional limitations can be modified by lawmaking if there is good reason to do so. Likewise, Congress can use legislation to affect the respective roles of the government and the private sector in incentivizing or driving certain forms of cyber behavior. The point is that our solutions to cyber threats should not be a function of what we think we can do with the rules and tools that we have; those rules and tools should be crafted based on the development of a cyber defense and security (CDS) doctrine that sets forth our strategic objectives and the roles and responsibilities of government and private institutions across all the domains touched by cyber activities.

How do we develop a comprehensive CDS doctrine? Doing so begins with an appreciation of the scope and the nature of the threats. From that understanding, we should elaborate a doctrine that sets forth our national objectives in securing ourselves and the allocation of responsibilities between government and the private sector defense. The doctrine should also address allocation of government responsibilities among agencies, delineating which objectives each is responsible for achieving. A critical feature of developing this doctrine is balancing the various goals of security, privacy, freedom and economic prosperity. With that framework set, Congress can enact or adjust the authorities appropriate to allow execution of the doctrine subject to constitutional or civil liberties constraints. This article begins the process of posing questions that must be answered to develop the strategy under the preceding template.

Threats and Consequences.

While it is fair to say that the internet is not a war zone, it could certainly become one. Moreover, war-like activity has been experienced as recently as 2007 and 2008. In the former year, Estonian government and financial institutions were the object of massive denial of service attacks aimed at disrupting and denying their ability to function. And when Russia invaded Georgia in 2008, ground movements were accompanied by cyber attacks aimed at disrupting Georgian command and control functions. Indeed, the United States-China Security Commission – a Congressionally-mandated body – has identified cyber warfare as an explicit part of Chinese military doctrine.

But the most cyber attacks are not this dramatic nor so obviously tied to classically war related activities. Recent media reporting reveals intrusions into financial institutions such as Nasdaq; theft of data from energy companies; exfiltration of data from Google; massive identity thefts and financial frauds. Much of this activity is directed from criminal groups, although nation states can also use the internet for intelligence purposes. While these are not destructive cyber activities, they can cause extremely serious personal and economic damage on a national scale. As Deputy Secretary Lynn's article last year made clear, huge volumes of sensitive commercial information and intellectual property are stolen on a regular basis. These data thefts directly affect our global competitiveness. Identity theft and credit fraud erode public trust in the internet which in turns has negative impact on investment and trade activity. On a personal level, there are heart rending stories of personal financial and reputational trauma caused by organized cyber crime and thievery.

While all of these threats can have serious consequences, the responses to each may be different in scale and type, and the appropriate allocation of responsibility will vary. Accordingly, it is helpful to disaggregate the cyber threats which we face into several categories.

Data theft involves the unauthorized and often undiscovered exfiltration of confidential or proprietary data from a system. This may include intellectual property, business sensitive information, confidential government information, and classified national security information.

Fraud involves using cyber tools to steal or deprive a victim of money, information or property (including personal information), by deceiving the victim into paying the money or furnishing the property or information under false pretenses.

Denial of service attacks interfere with access to or use of networks by overwhelming the network with data or commands so that its capacity to process additional data or commands is exceeded. This disrupts but does not necessarily damage or destroy the system under attack.

Destructive attacks damage or destroy or otherwise take control of the victim's computer systems. The consequences may range from denial of use, to corruption, to outright destruction of networks and systems, including those elements of physical infrastructure that are dependent on those systems.

Although popular culture reinforces the impression that the most significant threats are launched by attacks over the network by hacking into targeted systems, in fact devastating attacks can originate from different *vectors*. To be sure, malware can be introduced over the network by hacking remotely. But malware is often introduced through a *corruption of the supply chain* that embeds it within hardware or software. Equally dangerous are viruses that are introduced into a network by deceiving an authorized user into inviting it (for example, phishing, etc.), or through accidental or intentional compromise by an insider.

Foundations of a Cyber Defense and Security doctrine.

What are the ends of a CDS strategy? To establish a secure cyber environment within which public and private institutions can operate without excessive risk that systems will be crippled or damaged, or that valuable assets will be misappropriated or injured. But those ends coexist with other important objectives, such as fostering economic efficiency and creativity, and protecting privacy and individual rights. The development of a strategy for securing cyberspace, therefore, must balance these objectives and all consider the cost-effectiveness of various approaches. That amounts to cyber risk management.

From a defense and security standpoint, cyber risks differ from traditional security risks because of the degree to which they play out in the private sector.

Traditional consequential defense and security responsibilities are largely exercised by public authorities, such as the military or police. While private institutions may equip themselves against relatively low-level security threats, using private guards, locks and alarm systems, modern civil society does not expect – or even accept – that the responsibilities or authorities for security against major physical threats should be largely in private hands. No one suggests that civilian society equip itself with the responsibility to repel enemy invasions, and outside of private enclaves, we do not rely on private entities to police our streets.

What should be the government's responsibility and objectives in the realm of cyber defense and security (CDS)? Unlike the physical world, where major national security threats are largely – although not entirely – external, cyber attacks on privately owned networks might well be carried out – and even mounted – from or through platforms that were privately owned and domestic. Crippling of the power grid or our major financial institutions could have a catastrophic national impact, comparable to the effects of a major physical attack. But traditional perimeter military defenses would be irrelevant.

Some argue that cyber defense and security, therefore, is best left to the market and individual initiative and innovation. While it is true that the private sector has unleashed enormous creativity in developing aspects of our cyber economy, it is far from clear that market incentives will be sufficient to spur adequate investment in cyber security. Left to their own devices, few private companies would invest more in securing their cyber assets than the actual value of those assets. Yet in an interconnected and interdependent world, the failure of one part of the network can have devastating collateral and cascading effects across a wide range of physical, economic and social systems. Thus, the market place is likely to fail in allocating the correct amount of investment to manage risk across the breadth of the networks on which our society relies.

At one extreme, one could argue that the government should own a monopoly over cyber defense and security, assuming total responsibility for protecting public and private networks, and operating network defenses, accrediting hardware and software, and developing rules to reduce insider threats. At the other extreme, government would disclaim any responsibility in this sphere,

leaving the market and individual initiative to address these problems. Both of these are unrealistic.

Rather, in allocating responsibilities for CDS among government and private actors, therefore, we need to consider

(1) Who owns the network, asset, or system we seek to protect;
(2) How critical that network, asset or system is to vital or critical national interests, especially the interests of collateral or third parties;
(3) The nature and potential effects of the threat to be addressed;
(4) Whether government or private parties are best situated to respond quickly and effectively to the threat given architectural and economic features of the internet;
(5) Civil liberties and privacy constraints.

Naturally, the government's greatest role and responsibility will be directed at defense and government systems. These are owned by government agencies, and by definition most will be of national importance or at least networked to systems of national importance. As owner of military of civilian government systems, government is positioned operationally and legally to maintain awareness of what occurs in these systems, and to protect them.

Responsibility should be shared – but with a fair degree of government involvement – for those privately owned networks and systems which are deemed critical infrastructure based on interdependency or the essential nature of the services provided. Ownership and control of these networks are in private hands, but the ramifications of security failure in critical networks have much broader scope. Because the effect of intrusions into these critical systems can be magnified for interdependent third parties, merely market-based incentives may not be sufficient to drive enough investment in security for these systems. And government is a particularly important partner because it can leverage what Deputy Secretary Lynn described as "government intelligence capabilities to provide highly specialized active defenses."

But even if government is to be an active partner in managing cyber defense and security for privately held critical infrastructure, the specific methods and tools which government employs can still be sculpted to minimize intrusions on private

economic concerns and civil liberties. For the government can promote defense and security in several (overlapping) ways:

Warning and situational awareness. Alerting potential targets about detected threats. One possibility is shared situational awareness through a common operating picture of the network.

Defense. Actively blocking malware or other attack tools.

Target hardening. Taking measures to make target networks and systems less vulnerable, such as by encrypting data; using hardware and software to promote better "cyber hygiene", including access controls, limits on downloading, internal network monitoring and tracking; and validating hardware and software from the supply chain.

Investigation and forensics. Actions taken to discover penetrations that already have occurred and to investigate their source. Where practical and appropriate, this effort can include prosecution of those who have mounted the attack.

Prevention. Preventing attacks before they are launched by incapacitating the attack vector or the individuals trying to mount the attack. Incapacitation can be accomplished using legal process, cyber means or even physical means.

Resilience. Building capabilities to survive and mitigate the effects of cyber attacks by creating redundancies, traffic management tools, etc.

In the case of each of these approaches, the government can in theory choose to execute the approach itself, or to encourage, enable, and/or require the private sector to execute the approach. For example, government will want to maintain a monopoly of control over acts of prevention that involve incapacitating attackers operating from platforms or servers overseas. That means that government alone could exercise the legal authority to defend against persistent cyber attacks by attacking the offending platform either using cyber tools or even physical means.

By contrast, it is likely government would want to leave in private hands much of the responsibility for hardening or reducing vulnerabilities of private systems, albeit with the encouragement and possibly enabling from the

government. In these areas where the government is not likely to intervene directly – say in building resilience across private networks, it can still deploy a variety of measures to prompt the private sector to execute defensive or security measures. These tools include (in increasing order of coerciveness) : (1) providing actionable information and best practices; (2) creating legal incentives and immunities for private action (including liability protection); (3) monitoring and assisting in operating defenses upon invitation or consent; and (4) forcing action through regulatory mandate or disclosure obligations.

The more intrusive and coercive techniques for driving various security measures into the private sector are obviously more likely to clash with protection of private property and civil liberties. By the same token, less heavy-handed tools such as information sharing and legal incentives and immunities are far less likely to engage controversy, and should be considered in the first instance in dealing with the kinds of threats – such as data theft or computer crime -- that are relatively lower on the consequence scale. Promoting government engagement in these less controversial ways provides an early opportunity to manage down cyber risks, even which we debate the role of government in addressing more sophisticated and higher consequence cyber threats, such as national security espionage or sabotage of our cyber infrastructure.

Evolving a doctrine.

The foregoing landscape of risks, capabilities, and public and private interests provides the canvas on which decision makers must strike the balance between competing goals of security, efficiency, privacy, and free movement over the internet. Where the government assumes responsibility for executing cyber security, doctrine refines specific policy principles.

For example, if the government exercises a monopoly over the right to prevent attacks by responding with force, using either cyber or physical tools, it must decide under how and when it will trigger the response in connection with different types of threats. For example, acts of espionage or data theft – which are the modern analog to old-fashioned spying – may well be regarded as insufficient to trigger retaliatory or preemptive action because the United States government has not generally treated espionage by foreign powers as in itself an act of war

warranting forceful response. On the other hand, a foreign nation's attack on the integrity of important command and control systems or critical infrastructure may well be sufficiently consequential to warrant response in force. Indeed, as during the Cold War, one element of a response doctrine in such cases should be announcement of a declared policy of active prevention or retaliation under certain specified circumstances. Another important element of a response in force doctrine would be elaboration of the type and nature of evidence deemed sufficient to attribute an attack to a particular actor.

At the other end of the security spectrum, where government shares security responsibilities with the private sector, doctrine will be necessary to set forth with clarity the expectations of both the public and private sectors regarding their shared obligations. When the government chooses to enable private sector security measures by engaging in warning, the doctrine should set forth when, how and with what degree of assurance warning will occur. A further decision is whether by invitation the government should actually share tools for gaining situational awareness with operators of a private network.

When the government chooses to regulate, doctrine determines whether the regulation will be highly prescriptive or simply set objectives and broad metrics, leaving flexibility for implementation to the private sector. And where the government engages in active monitoring or defense, the doctrine sets forth how government agencies will treat and share information they obtain.

Finally, once whole government doctrine is set, leaders should turn to the subsidiary issue of how to allocate any responsibilities which the government bears among various agencies, including intelligence agencies, law enforcement agencies, and regulators. All too often, evolution of government doctrine begins with agencies forging policies that are designed to expand or enhance their existing capabilities or authorities. But strategy should not be the handmaiden of interagency bureaucratic competition. Only when government roles, responsibilities, and functions have been formulated does it make sense which organizations are best suited to execute these based on their intrinsic capabilities and statutory purposes.

Rewriting authorities.

After doctrine is designed, it must be matched against existing authorities to determine whether these need to be amended or new ones created. The outer boundaries are of course set by the Constitution. Within those bounds, the doctrine should reflect privacy and other civil liberties concerns. Authorities can then be constructed to protect those concerns against encroachment. In dividing authorities among agencies, a balance should be struck between, on the one hand, assignment of authority to those who are best situated to discharge responsibility and, on the other, the desire to prevent undue concentration of power and to assure institutional mechanisms to prevent abuse in an area with sensitivity about freedom of communication.

But authorities should not be drafted as a means to ring fence bureaucratic turf against encroachment. And some long held legal restraints on agency action will have to be revisited if government is to play a serious role in promoting cyber defense and security. For example, venerable and strongly-held restrictions against intelligence agencies collecting information inside the United States or involving U.S. persons are difficult to apply when agencies are ask to participate in monitoring or defending global cyber networks that route packets through the United States as a matter of network traffic management. Should the monitor's ability to function depend on the happenstance whether a hop point in the routing process is located on a United States based server? Should the restriction be modified or lifted where the monitoring is not designed to collect the content of the cyber traffic, but simply to inspect individual packets to determine whether malicious code is embedded, or to watch traffic flow patterns to look for anomalies or suspect IP addresses?

If our strategy and doctrine concludes that the government should play a role in network monitoring and shared situational awareness – at least with the consent of the network owner and operator – then it makes no sense to exclude the appropriate intelligence agencies from that mission or should their authorities be adjusted to permit those activities. In that way, the legal rules of the road are crafted to enable government to execute our national cyber strategy, rather than subordinating the optimal strategy and doctrine to a set of legal rules largely built in a different era.

Mr. GOHMERT. Thank you very much.
Mr. Baker?

TESTIMONY OF JAMES A. BAKER, LECTURER ON LAW, HARVARD UNIVERSITY

Mr. BAKER. Mr. Chairman, good morning. Ranking Member Scott and Members of the Committee, it is an honor to appear before you today to discuss the cyber security challenges that the country is facing.

I would like to focus my remarks on a very few key points today. First, as you know and as we have already discussed here this morning, the United States faces a significant cyber threat today. The threat comes from many sources, nation states, non-state actors such as organized crime groups, terrorist organizations and lone individuals.

As folks have said this morning, the money in our banks, our intellectual property and our critical infrastructure are threatened. There is a very real risk that at a time of crisis some parts of our critical infrastructure such as electrical, water, financial, transportation and telecommunications systems will not function as designed or at all.

Presently, the United States is not fully prepared to deal with the cyber threat that we face. In other words, our defensive capabilities are insufficient to address the malicious activities that are directed against the United States. This includes Federal, state and local governments, civilian and military authorities and the private sector.

At the present time, we cannot stop the theft of funds, intellectual property or personally identifiable information and we cannot ensure the malicious actors will not be able to degrade or destroy elements of our critical infrastructure at a time and in a manner of their own choosing.

Although many people in the government and the private sector are working overtime to find more effective ways to address these vulnerabilities, right now we cannot guarantee our cyber security. All we can do is mitigate the risks.

There are many reasons why we are not fully prepared to address the cyber threat today and these include technological, organizational, policy and legal issues. My written statement addresses these matters so in the interest of time I won't discuss them all now.

I will note, however, that one of the problems we must confront is that the Federal Government is not where it needs to be organizationally to address the cyber threat. There has been much progress in this sphere and the Administration's proposal contains some important provisions in this regard.

But the government is not where it needs to be in terms of clearly delineating agency roles and providing for robust but appropriate information sharing.

Next, I would like to address some of the Administration's proposals to amend the Computer Fraud and Abuse Act, or CFAA, and related provisions. Standing alone, as some have mentioned, these proposals will not address fully all of our—excuse me, all of our cyber security requirements.

They are important, however, and likely will assist law enforcement agencies and prosecutors in better ensuring that cyber crime is deterred effectively and punished appropriately. I know that

some Members have concerns about aspects of this proposal but I urge Congress to work with the Administration to find a set of mutually acceptable provisions to modify the CFAA and related laws as quickly as you can.

What Congress should not do, however, in my view, is to take steps that would weaken rather than strengthen the Computer Fraud and Abuse Act. I am concerned that some proposals to modify the terms of the existing act, in particular, those directed at modifying the scope of the term "exceeds authorized access", would have the unintentional effect of undermining the CFAA in certain respects.

I understand the concerns that some have raised about the scope of the act, that it may be ambiguous and that government overreaching could result in individuals being prosecuted for what essentially are innocent or harmless violations of the terms of service of particular websites or services.

I do not believe, however, that the case has been made that Federal prosecutors have regularly misused the CFAA, and to the extent that Congress is concerned that such abuses might occur, it strikes me that it might make more sense to use your oversight powers to ensure that enforcement of the CFAA is properly focused on the worst offenders.

But do we really want to make it harder for the government to prosecute individuals who abuse their authorized access to immense databases at financial institutions, social networking sites and email providers to steal money or sensitive personal information?

In closing, I recommend that the Subcommittee work quickly to enact some version of the Administration's proposal. Cyber security is not a problem that is amenable to simple solutions but we need to start moving in the right direction as quickly as possible. Our adversaries are not waiting for us to act.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Baker follows:]

Statement of James A. Baker
Before the
Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security
United States House of Representatives
Regarding
"Cyber Security: Protecting America's New Frontier"

November 15, 2011

Chairman Sensenbrenner, Vice-Chairman Gohmert, Ranking Member Scott, and Members of the Subcommittee: is it an honor to appear before you to discuss the cyber security challenges facing us today. As we all know, this is a very important topic and I believe that this hearing can help us make progress on improving our cyber security posture. I would like to note at the outset that I am appearing today at the request of the Subcommittee in my individual capacity and not on behalf of any current or former employer or clients. The Department of Justice reviewed this statement and does not object to its publication. I would like to focus my remarks on a few key points today.

First, as you know the United States faces a significant cyber threat today. Many others have made that point as well so I will not belabor it. The threat comes from many sources, including nation-states and non-state actors, such as organized crime groups, terrorist organizations, and lone individuals. The money in our banks, our intellectual property, and our critical infrastructure are threatened. There is a very real risk that in a time of crisis, some parts of our critical infrastructure – electrical, water, financial, transportation, telecommunications – will not function as designed (or at all). Moreover, the means that malicious actors use to gain access to computers and computer networks to enable them to steal money and data also may enable them to take complete control of a computer or a network. Such root access may allow them to burrow into that network so that it becomes exceedingly difficult to find them and to prevent them from re-accessing the network in the future at will. Malicious actors often seek to establish such a persistent presence in compromised networks.

Presently, the United States is not fully prepared to deal with the cyber threat that we face. In other words, our defensive capabilities are insufficient to address the malicious activities that are directed against the United States. This includes federal, state, and local governments; civilian and military authorities; and the private sector. At the present time, we cannot stop the theft of funds, intellectual property, or personally identifiable information, and we cannot ensure that malicious actors will not be able to degrade or destroy elements of our critical infrastructure at a time and in a manner of their own choosing.

Although many people in government and the private sector are working overtime to find more effective ways to address these vulnerabilities, right now we cannot guarantee our cyber security. That does not mean we should just give up, but it does mean that we need to make sure we are thinking about mitigating risks that we cannot

eliminate. And we need to figure out how to improve our cyber security, protect our data and networks, and continue to carry out essential functions in a compromised and probably degraded operating environment. Put differently, we need to presume that the intruders are already inside the gates and are among us. We may not be able to detect them in every instance, so we should assume that they are already here and act accordingly.

There are many reasons why we are not prepared to fully address the cyber threat. These include technological, organizational, policy, and legal issues. Let me say a few words about each of these factors.

First, there is much we can and should do from a technological perspective to improve our cyber security. We can properly configure and update network hardware and software; we can install strong firewalls and other perimeter-based security platforms; and we can implement robust access controls and monitoring systems. In some fundamental respects, however, today's communications and information technology infrastructure is inherently vulnerable. As a result, offensive cyber activities will always have an advantage over defensive ones. Let me give three examples – the zero day threat, the supply chain threat, and the insider threat.

The zero day threat is that malicious actors will develop and distribute damaging new malware that our defensive systems cannot detect and prevent from entering our networks. To be clear, "malware" is malicious software. Many of our cyber security technologies today are focused on scanning streams of communications or computer data to look for known malware "signatures" or code. The problem is that such technology detects malware signatures that someone has seen before. Our devices look for what they are programmed to look for, which are threats that we already know about. But new malware signatures are developed and unleashed all the time and it is hard to detect something that you have not seen before. Certain tools that look for anomalous behavior on networks show promise and may improve our security profile, but again they looking for patterns of behavior that have been seen before or that they are otherwise programmed to look for based on some predictive model. They will have a hard time detecting threatening behaviors that are truly novel. This is one example of why offense has an advantage over defense in cyber security.

The supply chain problem is that it is exceedingly difficult to ensure that software, hardware, and firmware that we purchase does not contain malware or other vulnerabilities – either by design or by mistake. Technology is complex and changes frequently, and it may be hard to detect built-in vulnerabilities. The insider threat is also easy to explain and difficult to address. Either intentionally or by mistake, individuals who have access to computers, networks, and data can introduce malware into systems, fail to properly configure networks using established protocols, or purloin data and intellectual property. There are ways to mitigate such risks, but not perfectly. Those are some of the technological problems we face.

Now let me discuss briefly some of the organizational and policy problems we must confront. The federal government is not yet where it needs to be organizationally to fully address the cyber threat. The roles and responsibilities of the major governmental actors – such as the Department of Homeland Security (DHS), the Department of Defense (including the National Security Agency (NSA) and U.S. Cyber Command), and the FBI – are not yet defined thoroughly relative to each other in the cyber arena. There has been much progress in this sphere, but the government is not yet where it needs to be. As a result, too much time is spent on figuring out agency roles and responsibilities on an ad hoc basis in response to a cyber incident; information about an incident is not collected or shared as robustly as it could be shared; and the full complement of investigative and analytical resources of the government are not always as fully or as promptly used as they could be used.

Moreover, it is not yet clear what role we expect the private sector to play in protecting the United States from cyber threats. This is crucial as most of the cyber infrastructure is owned and developed by the private sector. As a result, information that the private sector possesses about cyber incidents is not shared as promptly or extensively as it could be shared with pertinent actors, and the full range of private sector defensive capabilities is not utilized or coordinated fully among private sector entities or with federal authorities.

Related closely to these organizational issues are some significant policy decisions that the United States needs to make. Not only do we have to resolve questions about which actors should be involved in cyber security, we need to decide what we want them to do in providing that security. That is the biggest policy question we face as a society – What do we want to do to protect our cyber security? For example, we have not decided what role we want the government to play in monitoring private networks; what we hope to achieve as a result of such monitoring; and how we conduct such monitoring and simultaneously protect privacy, foster innovation, and promote competition. In addition to monitoring, we also have not figured out what we want military authorities – including U.S. Cyber Command – to do to protect us. The government has built that entity, but has not yet figured out how it wants to use it. For example, should the military monitor private networks in real-time and strike back at malicious cyber actors in some fashion? How accurately should the military be able to predict the collateral effects of an offensive cyber action before it strikes? And if the military does strike back, what impact will that have on the legitimate equities of law enforcement and intelligence agencies, and who is supposed to deconflict all of that? Once decision-makers and technical experts figure out what they want to do, the military and civilian lawyers can assess the legality of those actions.

Next let me turn next to the question of the extent to which the law impedes our ability to protect cyber security. In my view, the problems that we face right now in terms of our preparedness to deal with the cyber threat are not primarily legal in nature. As I have discussed, they are mainly technological, organizational and policy-based. To be sure, there are tough legal issues that we need to confront. For example, there is a complex, intertwined set of federal and state statutes that governs this area, and many of

them contain criminal prohibitions. Proper analysis of these laws is time consuming, and in many respects the law is not clear. As a result, it can be unnecessarily risky for governmental and private entities to take certain actions to thwart cyber threats. The basic idea here is that when someone in the government or a private company asks, "Can we do this?" it can be very difficult to figure out the correct answer quickly under today's statutory framework.

There are ways to remedy this, however, and the Administration's current cyber proposal does just that when it comes to simplifying the law with respect to allowing private entities to share more easily cyber security information with the government on a voluntary basis. The proposal also includes appropriate privacy safeguards. That proposal is not a panacea, and some have criticized it from a variety of perspectives, but my point is that the statutory issues can be addressed once we decide what we want to do.

Of course, we must also address constitutional issues. There is a good case to be made that reasonable governmental activities directed at enhancing cyber security would pass constitutional muster. I do not have time here today to address fully all of the constitutional issues, but the basic point is that the Supreme Court's special needs doctrine likely would apply in the cyber security context and should provide the government with the flexibility it needs to address the threat so long as its programs are reasonably designed in light of the threat and the level of intrusion into constitutionally protected spheres.

Again, I think that what we need to be focused on right now is deciding what we as a country want to do to respond to the complex and dangerous cyber threat that we face. Lawyers obviously must be involved in that discussion. But we should not conflate tough policy choices with real or imagined legal problems.

Finally, I would like to address some of the Administration's proposals to amend the Computer Fraud and Abuse Act (CFAA) and related provisions. As the Subcommittee is well aware, criminal statutes are only one means that we must use to deter cyber criminals. Standing alone, these provisions will not address fully all of our cyber security requirements. They are an important, however, and likely will assist law enforcement agencies and prosecutors in better ensuring that cyber crime is deterred effectively and punished appropriately. In my view, these proposals will update, simplify, and strengthen the CFAA.

For example, it will strengthen the CFAA to add a provision to prohibit activities that involve knowingly causing or attempting "to cause damage to a critical infrastructure computer, and such damage results in (or, in the case of an attempted offense, would, if completed have resulted in) the substantial impairment – (A) of the operation of [a] critical infrastructure computer; or (B) of the critical infrastructure associated with such computer." In light of the severity of such a crime, the three-year mandatory minimum sentence that the Administration has proposed seems appropriate. I understand that some Members have concerns about mandatory minimum sentences in general, but I believe that such a provision is justified here to ensure that courts will sentence those

convicted of such offenses in line with the severity of the crime. In any event, I urge Congress to work with the Administration to find a set of mutually acceptable provisions to modify the CFAA and related laws that you can enact quickly.

What Congress should not do, however, is to take steps that would weaken, rather than strengthen, the CFAA. I am concerned that some proposals to modify the terms of the existing Act – in particular, those directed at modifying the scope of the term "exceeds authorized access" – would have the unintentional effect of undermining the CFAA in important respects. I understand the concerns that some have raised that the scope of the Act may be ambiguous and that government overreaching could result in individuals being prosecuted for what essentially are innocent or harmless violations of the terms of service of particular websites or services. Notwithstanding one frequently cited example (the prosecution of Lori Drew), I do not believe that the case has been made that federal prosecutors have misused the CFAA. And to the extent that Congress is concerned that such abuses might occur, it strikes me that it may make more sense to use your oversight powers to ensure that enforcement of the CFAA is properly focused on the worst offenders. Indeed, rather than amending the definition of "exceeds authorized access" under the statute, Congress could legislate a reporting requirement to ensure that you are made aware promptly of any prosecutions brought against individuals or entities for exclusively violating the terms of service of a website.

Unnecessarily restricting the scope of the CFAA on the basis of one or two cases will needlessly tie the hands of prosecutors to the advantage of those who use computers to undertake fraudulent activities and abuse their otherwise authorized access to computers to harm others. Do we really want to make it harder for the government to prosecute individuals who abuse their authorized access to immense databases at financial institutions, social networking sites, and email providers to steal money or sensitive personal information? Do we want to give the government fewer tools to combat identity theft and fraud using computers? Bad facts in one case should not make bad law.

In closing, I recommend that the Subcommittee move quickly to enact some version of the Administration's proposal. As the Administration has acknowledged, the current proposal will not address fully all of the cyber security challenges that we face today. But the proposal is a good start that will have to be followed up by further legislative and executive branch action in the future. This is not a problem that is amenable to simple solutions, but we need to start moving in the right direction as quickly as possible. Our adversaries are not waiting for us to act.

Mr. GOHMERT. Thank you, Mr. Baker.
Professor Kerr?

TESTIMONY OF ORIN S. KERR, PROFESSOR OF LAW, GEORGE WASHINGTON UNIVERSITY

Mr. KERR. Thank you, Judge Gohmert, Ranking Member Scott for the invitation to appear here this morning. I am going to begin by doing something that is probably unusual for a witness before you. I am going to admit that I am a criminal, at least according to the United States Department of Justice's interpretation of the Computer Fraud and Abuse Act.

Mr. GOHMERT. Sir, you have the right to remain silent. [Laughter.]

Anything you say may—could be used against you.

Mr. KERR. I will waive that right.

Mr. GOHMERT. You have the right to consult an attorney if you wish.

Mr. KERR. In fact, I would like to speak about this. Why am I——

Mr. GOHMERT. If you can't afford an attorney one will be appointed for you. [Laughter.]

Mr. KERR. Why am I a criminal? Well, I have a Facebook account. Facebook requires its terms of service—in its terms of service that you cannot provide any false information on Facebook.

However, I do so. I say in my profile that I live in Washington, D.C. In fact, that is a blatant lie. I live in Arlington, Virginia. Therefore, I am in blatant violation of the terms of service, and according to the Justice Department I violate Federal criminal law every time I log in.

Those of you may have children or grandchildren who are under the age of 18 who use Google to conduct searches. According to the Justice Department, they are also all criminals. Why?

Well, because Google's terms of service say you have to be of legal age to enter into a contract in order to use Google. The legal age to enter into a contract in most states is 18.

Therefore, anybody under the age of 18 who uses Google is, according to the United States Department of Justice, a criminal.

Tens of millions of Americans have Internet dating profiles. Those Internet dating profiles typically say the terms of service of the Internet dating services say that individuals must give all truthful information and cannot give misleading information.

According to one study, more than 80 percent of Internet dating profiles give misleading information. Somebody might say they are an inch taller than they are, maybe five pounds less. Maybe they might say they go to the gym every week when they don't. According to the United States Department of Justice, that makes them criminals.

In fact, probably most people in this room, most of the witnesses, Members, counsel, members of the audience, most if not all are criminals under the United States Department of Justice's interpretation of the Computer Fraud and Abuse Act.

What is the government's position here in how to amend the statute? My understanding is that the Justice Department wants

to further broaden the statute so that it encompasses more cases and is more punitive than before.

I think the answer is to narrow the scope of this act to ensure that routine computer usage is not criminalized rather than to further broaden and enhance the penalties of the statute.

The reason why this is a problem—the reason how we got into this situation—is that Section 1030 of the Computer Fraud and Abuse Act treats computers differently than it treats the physical world. If you think about you are an employee at a job, your boss says don't go into the personnel files without a good work-related reason, you might—someone might look into those personnel files and might be disciplined for that. The boss might fire them or might not give them a raise but it wouldn't be a crime just to look into the folder.

On the Internet or in the case of computers, it is a different rule. The law says you cannot exceed authorized access, which the Justice Department sees as saying that any term of use or term of service by an employer or an Internet service provider is binding as a matter of law.

If an employer says you can't use the workplace computers for personal reasons and you do so, you are a criminal, again, a different rule in the case of using computers than there is in the case of offline real-world conduct.

I think we need to amend the statute to eliminate those overly broad readings of the Computer Fraud and Abuse Act and that it is actually quite simple to do so.

I have put in my written testimony two different ways of amending the statute which would narrow it and yet also preserve the Justice Department's authority to prosecute the kinds of cases that they mention when they explain why they want existing law to be as it is.

In particular, the Justice Department, when it talks about prosecuting cases under the "exceeds authorized access" prong, always talks about cases in which the data that is obtained is very valuable or very private information.

However, the statute does not contain any such limitation. The statute applies to any act of exceeding authorized access to obtain any information at all. One simple way of fixing the statute would be to limit the Computer Fraud and Abuse Act so that the "exceeding authorized access" prong only applies to efforts to obtain personal information or valuable information. That would preserve the Justice Department's ability to prosecute the kinds of cases it wants to prosecute and yet also preserve civil liberties of every other American who might, for good reasons, violate Internet terms of service of websites which it looks like most Americans who use the Internet and a computer probably do.

Thank you. I look forward to your questions.

[The prepared statement of Mr. Kerr follows:]

Testimony of Orin S. Kerr
Professor, George Washington University Law School

United States House of Representatives
Committee on the Judiciary
Subcommittee on the Crime, Terrorism,
and Homeland Security

"Cyber Security: Protecting America's New Frontier"
Tuesday, November 15, 2011
2141 Rayburn House Office Building, 10 a.m.

WRITTEN STATEMENT OF ORIN S. KERR

The current version of the Computer Fraud and Abuse Act (CFAA) poses a threat to the civil liberties of the millions of Americans who use computers and the Internet. As interpreted by the Justice Department, many if not most computer users violate the CFAA on a regular basis. Any of them could face arrest and criminal prosecution.

In the Justice Department's view, the CFAA criminalizes conduct as innocuous as using a fake name on Facebook or lying about your weight in an online dating profile. That situation is intolerable. Routine computer use should not be a crime. Any cybersecurity legislation that this Congress passes should reject the extraordinarily broad interpretations endorsed by the United States Department of Justice.

In my testimony, I want to explain why the CFAA presents a significant threat to civil liberties. I want to then offer two narrow and simple ways to amend the CFAA to respond to these problems. I will conclude by responding to arguments I anticipate the Justice Department officials might make in defense of the current statute.

I. My Experience With the CFAA

Before I begin, let me briefly explain my experience with the CFAA. I have worked with the CFAA at various times in the capacity of prosecutor, legal scholar, and

defense attorney. I first began studying the Computer Fraud and Abuse Act in 1998, when I joined the Computer Crime and Intellectual Property Section in the Criminal Division of the United States Department of Justice. From 1998 to 2001, I assisted in the investigation and prosecution of many CFAA cases as a Justice Department Trial Attorney and as a Special Assistant U.S. Attorney in the Eastern District of Virginia.

In 2001, I joined the faculty at George Washington University Law School. Since that time, I have authored a chapter of a law school casebook on the CFAA, and I have taught the law of the CFAA in a course on computer crime law. *See* Orin S. Kerr, Computer Crime Law 26-109 (West 2nd ed. 2009). I have also written two law review articles about the Act. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561 (2010); *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes,* 78 NYU L. Rev. 1596 (2003).

Finally, I have also worked as a defense attorney and consulted with defense lawyers in CFAA cases on a *pro bono* basis to try to block the expansive readings of the Act that are the subject of my testimony. In particular, I briefed and argued the successful motion to dismiss in the so-called "MySpace Suicide" case. *See United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009). My written testimony draws from all of these experiences, although of course it is made entirely in my personal capacity.

II. The Extraordinary Scope of 18 U.S.C. §1030, the Computer Fraud and Abuse Act.

When the Computer Fraud and Abuse Act was first enacted in the 1980s, it was a narrow statute that targeted computer hacking and other harmful computer misuse. Over the last 25 years, however, Congress has broadened the statute dramatically four different times: in 1986, 1996, 2001, and 2008. Each of these amendments significantly expanded the reach of the statute. Today's statute is breathtakingly broad, and its key terms are subject to a wide range of interpretation that can make it so broad as to render the statute unconstitutionally vague. *See generally* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561 (2010).

A quick look at the broadest crime in the statute reveals the problem. The broadest provision of the broadest crime, 18 U.S.C. § 1030(a)(2)(C), punishes whoever "intentionally . . . exceeds authorized access, and thereby obtains information from any protected computer." We can break this federal crime into its three elements as follows:

(1) Intentionally exceeds authorized access
(2) Obtains information
(3) From a protected computer

Critically, elements (2) and (3) will be satisfied in most instances of routine computer usage. Element (2), the requirement that a person "obtains information," is satisfied by merely observing information. *See, e.g., United States v. Tolliver*, 2009 WL 2342639 (E.D. Pa. 2009) (citing S. Rep. No. 99-432 at 2484 (1986)). The statute does not require that the information be valuable or private. *Any* information of *any* kind is enough. Routine and entirely innocent conduct such as visiting a website, clicking on a hyperlink, or opening an e-mail generally will suffice.

Element (3) is easily satisfied because almost everything with a microchip counts as a protected computer. The device doesn't need to be what most people think of as a "computer," and it doesn't need to be connected to the Internet. Consider the relevant definitions. Under 18 U.S.C. § 1030(e)(1), a "computer" is defined as:

> an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device[.]

This definition "captures any device that makes use of a electronic data processor." *United States v. Kramer*, 631 F.3d 900, 902 (8th Cir. 2011). Indeed, the Justice Department has argued that any "electronic, magnetic, optical, [and] electrochemical" data processing device is included, whether or not it is "high speed." *Id.* at n.3. Given that many everyday items include electronic data processors, the definition might

plausibly include everything from many children's toys to some of today's toasters and coffeemakers.

The statutory requirement that the computer must be a "protected" computer does not provide an additional limit. In 2008, Congress amended the definition of "protected" computer to include any computer "used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). In federal law, regulation that "affects interstate or foreign commerce" is a term of art: It means that the regulation shall extend as far as the Commerce Clause allows. *See Russell v. United States*, 471 U.S. 858, 849 (1985). Under the aggregation principle of *Gonzales v. Raich*, 545 U.S. 1 (2005), this appears to include all computers, period. As a result, every computer is a "protected" computer.

Because elements (2) and (3) are so extraordinarily broad, liability for federal crimes under 18 U.S.C. § 1030(a)(2)(C) hinges largely on the first element: What conduct "exceeds authorized access"? That phrase is defined in 18 U.S.C. § 1030(e)(6):

> the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.

This provides little guidance, unfortunately, as the definition is largely circular. Under the definition, conduct exceeds authorization if it exceeds entitlement. But what determines entitlement? The statute doesn't say, and that failure to provide guidance has allowed the Justice Department to adopt extremely broad readings of what might exceed authorized access.

As a practical matter, the key question has become whether conduct "exceeds authorized access" merely because it violates a written restriction on computer access such as the Terms of Use of a website. The Justice Department has taken the position that it does. This interpretation has the effect of prohibiting an extraordinary amount of routine computer usage. It is common for computers and computer services to be governed by Terms of Use or Terms of Service that are written extraordinarily broadly. Companies write those conditions broadly in part to avoid civil liability if a user of the computer engages in wrongdoing. If Terms of Use are written to cover everything slightly bad about using a computer, the thinking goes, then the company can't be sued

for wrongful conduct by an individual user. Those terms are not designed to carry the weight of criminal liability. As a result, the Justice Department's view that such written Terms should define criminal liability – thus delegating the scope of criminal law online to the drafting of Terms by computer owners – triggers a remarkable set of consequences. A few examples emphasize the point:

(a) The Terms of Service of the popular Internet search engine Google.com says that "[y]ou may not use" Google if "you are not of legal age to form a binding contract with Google." http://www.google.com/accounts/TOS (last visited November 14, 2011). The legal age of contract formation in most states is 18. As a result, a 17-year-old who conducts a Google search in the course of researching a term paper has likely violated Google's Terms of Service. According to the Justice Department's interpretation of the statute, he or she is a criminal.

(b) The Terms of Use of the popular Internet dating site Match.com says that "You will not provide inaccurate, misleading or false information . . . to any other Member." http://www.match.com/registration/membagr.aspx (last visited November 14, 2011). If a user writes in his profile that he goes to the gym every day – but in truth he goes only once a month – he has violated Match.com's Terms of Use. Similarly, a man who claims to be 5 foot 10 inches tall, but is only 5 foot 9 inches tall, has violated the Terms. So has a woman who claims to 32 years old but really is 33 years old. One study has suggested that about 80% of Internet dating profiles contain false or misleading information about height, weight and age alone. *See* John Hancock, et. al., *The Truth about Lying in Online Dating Profiles* (2007), available at https://www.msu.edu/~nellison/hancock_et_al_2007.pdf. If that estimate is correct, most Americans who have an Internet dating profiles are criminals under the Justice Department's interpretation of the CFAA.

(C) Terms of Use can be arbitrary and even nonsensical. Anyone can set up a website and announce whatever Terms of Use they like. Perhaps the Terms of Use will declare that only registered Democrats can visit the website; or only people who have been to Alaska; or only people named "Frank." Under the Justice Department's interpretation of the statute, all of these Terms of Use can be criminally enforced. It is true that the statute requires that the exceeding of authorized access be "intentional," but

this is a very modest requirement because the element itself is so easily satisfied. Presumably, any user who knows that the Terms of Use exist, and who intends to do the conduct that violated the Term of Use, will have "intentionally" exceeded authorized access.

I do not see any serious argument why such conduct should be criminal. Computer owners and operators are free to place contractual restrictions on the use of their computers. If they believe that users have entered into a binding contract with them, and the users have violated the contract, the owners and operators can sue in state court under a breach of contract theory. But breaching a contract should not be a federal crime. The fact that persons have violated an express term on computer usage simply says nothing about whether their conduct is harmful and culpable enough to justify criminal punishment. There may be cases in which harmful conduct happens to violate Terms of Use, and if so, those individuals should be punished under criminal statutes specifically prohibiting that harmful conduct. But the act of violating Terms of Service alone should not be criminalized.

III. Two Statutory Solutions to the Overbreadth of the CFAA

Fortunately, there are two simple ways to amend the CFAA to cure its overbreadth. The first solution is to amend the statutory definition of "exceeds authorized access" in 18 U.S.C. § 1030(e)(6) to clarify that should not be interpreted to prohibit Terms of Service violations. The Senate Judiciary Committee recently approved an amendment to a pending bill, S.1151, that includes such language limiting the scope of the CFAA. As amended, Section 110 of S.1151 states:

> Section 1030(e)(6) of title 18, United States Code, is amended by striking ''alter;'' and inserting ''alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized;''

This is a very helpful amendment, and I endorse it. To be sure, it is not a model of clarity. It defines "exceeds authorized access" by what it *isn't* rather than by what it *is*, which may lead to confusion. It also leaves unclear when a violation should be deemed

the "sole basis for determining that access to a protected computer is unauthorized," as compared to merely one part of that basis. But I read the amendment as indicating that the Justice Department generally cannot bring prosecutions based on violations of Terms of Service and Terms of Use.

Notably, the language carves out one significant exception. The government can pursue prosecutions for violations of computer use policies used by government employees. This will enable prosecutions when government officials misuse sensitive government databases. *See, e.g., United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (allowing a criminal prosecution of a Social Security Administration employee for accessing Social Security Administration databases for nonbusiness reasons in violation of workplace policies). Many government workplace computer use policies protect important government interests, and violations of such policies can trigger significant societal harms. As a result, it is sensible that the Justice Department's broad theory of the CFAA should be retained in that specific setting. Other uses of the Justice Department's broad theory will be prohibited.

(b) An alternative statutory solution would be to limit § 1030(a)(2) directly by creating significant limits on the kind of information that can trigger liability under 18 U.S.C. § 1030(a)(2)(A)-(C). As explained above, the current version of § 1030(a)(2) is triggered when an individual obtains *any* information. It doesn't matter what the information is, or whether it has any value. This means that the prohibition can apply even to violating arbitrary Terms of Use that protect websites that contain no private or valuable information. To correct this, the statute could be rewritten to limit § 1030(a)(2) to obtaining the specific kinds of information that, when obtained in excess of authorization, are associated with significant harms. For example, § 1030(a)(2) could apply only when an individual obtains:

> (a) information with a value of more than $5,000; or
> (b) sensitive or private information involving an identifiable individual (including such information in the possession of a third party), including medical records, wills, diaries, private correspondence, financial records, or photographs of a sensitive or private nature;

Under this proposal, violating Terms of Service could still violate the CFAA in *some* cases. However, liability only would extend to the rare violations of Terms of Service

in which the violation allowed an individual to obtain very valuable or very private information to which they were not entitled. These will tend to be the rare cases in which the violation of an express term on computer use is associated with a harm that might justify criminal prosecution.

IV. Responses to Anticipated Counterarguments

I anticipate that the Justice Department will defend the current state of the law with three related arguments. The first argument I anticipate is that although the current language of the statute is tremendously broad, the Justice Department can be trusted with this power because it has not often abused its authority under the statute. The second argument is that the Justice Department needs maximum discretion in this area to account for the unpredictability of technological change. The third argument I anticipate is that the broad reading of the statute is helpful to the Justice Department because it may make it easier to punish some individuals who have caused harms using computers.

I'll start with the first argument, that the Justice Department can be trusted with this power because it has exercised its discretion wisely This argument is problematic for two reasons. First, it appears to misunderstand the proper role of Congress and the Executive branch in the enforcement of criminal law. It is the responsibility of the United States Congress to enact criminal laws that only prohibit conduct that is harmful, culpable, and deserving of criminal punishment. It is the responsibility of the Executive to enforce those violations in appropriate cases. This division of duties does not allow Congress to write DOJ a blank check, and for DOJ to be the ultimate arbiter of what is criminal.

This argument is also weak because the Justice Department's broad interpretation of the CFAA has not been clearly endorsed by the courts, meaning that it is not at all clear that the prosecutors actually enjoy the discretion they might claim to have wisely exercised. In the one and only criminal prosecution for violating Internet terms of service, the district court rejected the Justice Department's interpretation as unconstitutional and dismissed the charges. *See United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009). The Justice Department declined to pursue an appeal from that ruling. Just a few weeks ago, the Ninth Circuit granted the defendant's petition for rehearing *en*

banc in the first criminal prosecution based on violations of a private-sector employee computer use policy. *See United States v. Nosal*, 642 F.3d 781 (9th Cir. 2011), *reh'g granted*, -- F.3d --, 2011 WL 5109831 (October 27, 2011). In light of the judicial resistance to the Justice Department's efforts to read the CFAA so broadly, it would be premature for Justice Department officials to commend themselves for how prosecutors have exercised the power that prosecutors may or may not have.

I am also unpersuaded by the second argument I anticipate, that the Justice Department needs maximum discretion in this area to account for the unpredictability of technological change. This argument might have been persuasive in the 1980s, when Congress enacted 18 U.S.C. § 1030. It might have made sense in the 1990s, when most Americans first began to use the Internet regularly. But the argument doesn't work in late 2011, more than a quarter-century after the passage of the CFAA. The basic ways that computers might be misused have been well-known for decades. The concepts and principles are the same today as they were twenty years ago. There is little new under the sun, and therefore no apparent need for maximum discretion to account for technological change.

The third and final argument I anticipate is that the broad reading of the statute is helpful to the Justice Department because it may facilitate punishment of some individuals who have caused harms using computers. If Justice Department officials make this argument, I urge the Committee to ask for specific scenarios and to make sure that the conduct described isn't already criminal under other provisions of the criminal code. Making a threat using a computer already violates the federal threat statute, for example. Stealing trade secrets using a computer already violates the federal theft of trade secrets statute. It is hard to see what value there is in making such conduct also a CFAA violation.

Indeed, it is easy to see the harms of doing so. A broad reading of the CFAA that effectively makes it illegal to do anything harmful using a computer would mean that the carefully-crafted statutory scheme of federal criminal law would be trumped whenever a computer is involved. If computer-related conduct is harmful, prosecutors should charge the preexisting crimes that relate to the harm. They should not use the CFAA as a catch-all.

The pending case of *United States v. Nosal* provides a helpful illustration of the problem. The facts of *Nosal* justify a theft of trade secrets prosecution: Nosal allegedly worked with employees of his old company to help steal secrets from that company so he could set up a competing business. The Justice Department charged the defendants with both theft of trade secrets and violating the CFAA. The trade secrets charge was based on stealing trade secrets, and the CFAA charge was based on the employees' violating a workplace computer policy that banned use for reasons other than official company business. If the Ninth Circuit allows the CFAA charges in *Nosal* to proceed, the CFAA charges will be much easier to prove. Establishing a theft of trade secrets requires proving all the elements of the crime, and that can be a difficult task. In contrast, proving that an employee did *something* for reasons other than official company business is vastly easier. To my mind, allowing this theory would set a dangerous precedent. If the government is really bringing the prosecution because of the alleged theft of trade secrets, the government should have to prove a theft of trade secrets.

Thank you for this opportunity to testify. I look forward to your questions.

Mr. GOHMERT. Thank you.

At this time, we will go to questions and I will reserve mine to allow other Members to go ahead.

So let's see, Mr. Forbes of Virginia?

Mr. FORBES. Thank you, Mr. Chairman.

Gentlemen, thank you all for your expertise and willingness to come here, and I understand Professor Kerr's desire to want to be able to lie on his Facebook account and that is okay. My concern is this.

I realize that we can have death by a thousand cuts with all these small cyber attacks but my big concern from sitting on the Armed Services Committee is the major gaping wounds that can happen to us if we were to have cyber warfare.

And the question I would ask for all of you gentlemen who would like to respond is are our laws in any way hampering the Department of Defense from developing the technologies that we need to defend and protect against that major kind of attack if it was coming, which I believe one day we will see it in some portion or the other.

And secondly, are our laws in any way hampering DOD from developing the kind of strategies we would need to be able to use that same kind of attack if, you know, heaven help us, we would have to do it? And then can you give me a little insight on how we even know when such a war would be launched against us?

How do we know who is doing it and how do we possibly say okay, now this is the time when we can launch a counter action against that? And I will defer to any of you who would like to go first. But I really respect and appreciate your insight on it.

Mr. CHERTOFF. Well, thank you—thank you for the question. It is a broad set of questions.

Mr. FORBES. I know it is.

Mr. CHERTOFF. I will address maybe the last question, which is what is often referred to as the issue of attribution, and it is a complicated issue because the reality is many of the attacks we suffer, if you—if you follow the attack back the point at which you're proximate to, the target may be in the United States but it may be a computer that has been taken over and is being operated remotely from China or someplace else in the world.

And the difficulty is proving that connection is often very difficult. It is compounded by the fact that some of the ways we might prove it make reference to sophisticated and secret sources and methods that we are not going to want to reveal.

So there is a huge challenge unlike what we faced in the Cold War when, if a missile was launched, we could demonstrate where the missile comes from. I think the answer there is a—the laws are really not the issue here.

The issue here is for us to develop a doctrine and to be very clear about, first of all, what we believe our response ought to be to an attack—distinguishing between a theft of property, which is espionage which we have traditionally not viewed as an act of war, and an attack on a system that might destroy the system itself like the electric power grid.

And once we have determined what we want our response to be, we have got to do two things. We have got to, first of all, make sure

the law permits us to respond, and second, I believe we need to have a declared policy of deterrence.

We need to, for example, tell the world that if there is an attack upon our electric grid that results in a loss of life we reserve the right to respond by, A, eliminating the servers that launched the attack, we may reserve the right to do so physically as well as in cyberspace and we need to explain what our red lines are. If we don't do that, then we run the risk of a miscalculation where somebody launches on us without a clear understanding of our response, and experience shows that that is how people get into wars, when there is an unclarity of doctrine.

Mr. BAKER. I would agree with that completely. I think that the key problems are making the tough policy choices first, and once you have the policy, both the policy in terms of what do we want to do as a country to respond to these kinds of attacks. And when I am talking about an attack here in this setting I am talking about something that when it is directed at us would constitute a use of force against the United States if it was done by kinetic means. So that is—so when I talk about an attack that is what I mean, not an exploitation or espionage or something along those lines.

But I think we need to get the policy right in terms of what we want our military to do. We need to get the technology right in terms of what it is that we think we are going to be doing, what are the collateral effects of that kind of activity.

For example, if you launch something will you be able to restrict it narrowly or will it spread more broadly? How confident are we going to be in that? I think those are the tough questions.

Once the policy makers figure out what they want to do, then the lawyers can help figure out how to do this legally either under the existing regimes with the, you know, the laws of war, the laws of armed conflict, the very statute they have to deal with, or that we need to make some kinds of changes and so on.

Just one other quick question to address the last part of what you said, knowing whether we are actually under attack may be difficult in some circumstances because a smart adversary might just degrade our systems in a way that make them difficult for us to use and make us—make it hard for us to respond to a threat somewhere in the physical world but that we can't quite figure out whether it is actually being destroyed or not or whether there is an attack that is underfoot.

Mr. FORBES. Mr. Downing, my time is up but I would love at some point in time to hear your response to that maybe for the record or maybe if you could give it to me in person.

Mr. GOHMERT. Without objection, we will go ahead and extend the time to allow an answer to that question.

Mr. FORBES. Thank you, Mr. Chairman.

Mr. DOWNING. So I guess what I would add to these other comments that have gone before is that I am not aware of any particular laws that are holding the military back at this time, although to be clear I work in the Computer Crime Section of the Department of Justice so perhaps that question is best asked to members of our Department of Defense.

But what I would emphasize here is that unlike other sorts of defenses of the Nation, the victims of these attacks are going to be in the hands of our private infrastructures for the most part and thus it is not possible for the Defense Department to defend in the traditional way.

And so that is very much why we see the comprehensive cyber security package as being very important because it provides the incentives we need to help industry to defend itself, since the Defense Department is not going to be able to put up, you know, ships on the sea and planes in the air to defend that.

Mr. GOHMERT. Okay. Thank you, Mr. Forbes.

At this time, Mr. Scott was going to defer and we will hear from Mr. Deutch.

Mr. DEUTCH. Thank you, Mr. Chairman.

Mr. Downing, the Administration's proposal for information sharing states, if I understand it correctly, that notwithstanding any other provision of law, businesses can share their customers' private information with Department of Homeland Security.

I presume that means Internet and email information. What else are you trying to get at? What else is there that will be shared and could this information potentially include medical records and all sorts of other personal information that would violate the privacy laws?

Mr. DOWNING. So the idea of that is shared for the purpose of securing cyber security. So I think the primary areas would be things like threat and vulnerability information.

A Internet service provider discovers a new exploit that is allowing people to access computers without authority. It is able to report it to the government and also to spread that information to help defend other networks as well.

It is true, though, that sometimes there will be a narrow set of private information that would have to be disclosed. For example, in certain kinds of phishing attacks there is an email that is sent to a particular person in an effort to get them to give up their password.

So there may be some cases where there is a need for that sharing of private information. What the bill does, though, is contain a number of ways that would protect the privacy of that information, so it would have sharing restrictions once it reaches the government.

The attorney general would have a set of rules that would require that it be treated in a protected way. It also requires that the person giving the information to take out all other sorts of private information as well.

Mr. DEUTCH. Just going back to what you just said, though, when you referred to phishing expeditions that we should be concerned then about the possibility, understanding that there are—there are requirements that would be imposed and guidelines that this could include all kinds of information about individuals. The sorts of things that these criminals are looking for are all of the sorts of things that may be turned over to the government including bank account numbers, credit card numbers, passwords for all of those accounts.

Might all of that be included in the information that is going to be turned over?

Mr. DOWNING. I think it is important to make sure that there are appropriate privacy restrictions because there will be some, I think, fairly limited situations where that sort of information may need to be turned over.

So I think attention to the need to protect that information appropriately is proper, and we feel we have done a pretty good job of putting into the bill protections for that. But, of course, if there are other needs here, we are happy to work with Congress to sharpen them as well.

Mr. DEUTCH. All right. I appreciate that.

Mr. Baker, I have a question for you. You said—you said we can't stop theft, and we can't ensure that elements of our infrastructure won't be destroyed. You refer to the technological problems and policy issues.

Can you speak to the extent to which lawmakers, policy makers can partner with the technology community to approach some of these issues? Does that—is that happening? Should that be happening?

Mr. BAKER. Partner—I am sorry.

Mr. DEUTCH. Please.

Mr. BAKER. No. I was just going to say partnering directly on those kinds of issues. I mean, I think the main thing is to be informed and so calling hearings and bringing folks up to explain exactly what the problems are and what is going on—I mean, as Secretary Chertoff explained, the supply chain problem and the insider problem. The zero-day threat is a significant one.

But I think one of the main things to do in terms of lawmakers is to figure out the boxes in terms of what parts of the United States government are going to have the lead or—yeah, I guess the lead in addressing these problems and some of the proposals in the Administration's recommendation try to address that.

They try to give an enhanced role for DHS to do this. Not because DHS is perfect. I think they would not say that they are perfect. But we need to make a decision and move forward.

We need to get going on this legislation and start down this road and then fix the problems as we go. As Secretary Chertoff said, this is just the beginning. We have got a long way to go.

Mr. DEUTCH. And Mr. Baker, you and Secretary Chertoff both spend a lot of time thinking about what these—what these concerns might be. As you—as you play these out, all of the various risks, in terms of critical infrastructure and the risks that we face because of the technology, what is it that worries you most? What do you think—where do you think we are most vulnerable?

Mr. BAKER. Well, I think any of these—any of these systems are vulnerable, any of them, and the electrical one is one of the primary ones. I think if that was shut down or degraded in a significant part of the United States that is a significant problem.

And it is not only a problem of somebody intentionally doing that. I mean, there might be reasons that a nation state is not going to do that in an otherwise—in a situation that is otherwise a time of peace. They may do it in a time of crisis.

But you might have a terrorist group that gets its hands on some kind of a tool that would enable them to do this or somebody is experimenting with something and it leaks out and it gets out into the wilderness, if you will, out into the wild and then it just starts shutting down systems and we don't know what is going on—I mean, that kind of a virus, if you will, in terms of something leaking out.

So I think any one of these systems is vulnerable. The financial system is vulnerable. I mean, any of them. Take your pick.

Mr. DEUTCH. Thank you. Thank you, Mr. Chairman.

Mr. GOHMERT. Okay. Thank you, Mr. Deutch.

At this time, we will hear from Mr. Gowdy from South Carolina.

Mr. GOWDY. Thank you, Mr. Chairman.

I want to thank all the witnesses for lending us your expertise.

Mr. Downing, I think I understood you correctly. One of the Administration's proposals is to raise the statutory maximum.

Mr. DOWNING. That is correct, in certain ways. Different parts of the statute, yes.

Mr. GOWDY. I know that sounds good. I get the politics behind raising the statutory maximum. How many of these cases ever approach the statutory maximum? If you want to do something about it, do something about the guidelines, not the statutory maximums.

Mr. DOWNING. Well, we certainly agree that a lot of the sentencing is driven by the guidelines and there actually was an effort to try to improve the guidelines, by raising the penalties. That occurred the year before last.

But, unfortunately, the Sentencing Commission largely did not do much to raise them. I would say though——

Mr. GOWDY. Would you be gracious enough to send to me your recommendations for the Sentencing Commission? They were kind enough to come visit with us a few weeks ago too and I was shocked at how infrequently even judges who were on the Sentencing Commission bother to follow the sentencing guidelines. So if you would send me those recommendations.

Also, if you know how many motions for upward departure Department of Justice may have filed in cyber security cases that would be helpful to me as well. The——

Mr. DOWNING. I would be happy to take that back.

Mr. GOWDY. The ratio of motions for downward departure versus motions for upward departure is 17 to 1 for downward. So some evidence of the Administration's seriousness about cyber security to me would be requests for upward departures in the cases where there has been a prosecution.

RICO, practically, for the line AUSAs in the districts how is RICO going to help them?

Mr. DOWNING. RICO is particularly useful in those situations where you want to try to take down an entire enterprise and, in particular, where you have leadership of the enterprise that may not be actually committing the offenses or may not be in conspiracy with others who are. So the usual tools of the direct crime and the conspiracy are not available.

We have seen this in terms of cyber security in the area where you have an organized group that will have different pieces of the organization doing different parts of the job.

Some of them are actually hacking. Some of them are using it to commit fraud. Some of them are doing other tasks. And so we think that it is a useful tool to be able to take down the entire organization including the senior leadership, and so that is one important way that it would help.

Mr. GOWDY. What leads you to think the Department of Homeland Security is the best agency to handle this?

Mr. DOWNING. Well, to handle this, I am not quite sure which piece of it you mean. You mean why should they get clarified authorities to be a leader in the area of cyber security?

Mr. GOWDY. Right, as opposed to the Bureau.

Mr. DOWNING. Well, we think the Bureau is an important piece of the puzzle but they have a very different role then that we would proscribe for the Department of Homeland Security. The Bureau does a terrific job on investigating cases and they are a critical piece of creating deterrence.

However, DHS has an important role too. DHS, as the proposal would suggest, would strengthen or clarify the rules that would allow it to be better at outreach with private industry, making clear its role in helping to protect the civilian infrastructure and the government infrastructure.

So it is really a different role that we see for DHS, and that is why we are seeking to have its authorities clearly laid out in legislation.

Mr. GOWDY. Can you tell me the difference between computer trespassing/theft and treason?

Mr. DOWNING. I am sorry. And treason?

Mr. GOWDY. Treason. When does it become treason?

Mr. DOWNING. Well——

Mr. GOWDY. Because the penalty for treason is already pretty high, I think.

Mr. DOWNING. I believe it is, yes. Treason, I would have to probably get back to you on that. I am not sure I know the elements of the offense of treason. But my understanding would be that it would require that it be done in terms of wartime or where it would be a direct——

Mr. GOWDY. So it has to be during a time of war to be treasonous?

Mr. DOWNING. I am sorry. I don't want to guess.

Mr. GOWDY. What about one of our law professors?

Mr. KERR. My understanding is that treason is defined by the Constitution and requires somebody who is loyal to the United States who does an act intentionally against the interests of the United States as an act, intentional act of disloyalty to the United States.

So I don't see how that is implicated in an act of computer trespass, which can be conducted for many different reasons. It might be. You could have an act of computer trespass that is part of an act.

Mr. GOWDY. So if a soldier were to download information and give it to an enemy, would that be treasonous or not?

Mr. KERR. I don't know.

Mr. GOWDY. What do you think?

Mr. KERR. Well, prosecutions for treason, my recollection is that the Constitution has requirements as to the witnesses that have to be available for acts of treason. So it is actually a very rarely prosecuted crime. I don't know if there have been prosecutions for treason in my lifetime.

But it certainly would be a criminal act with severe penalties. Whether it is an act of treason or not, I don't know.

Mr. GOWDY. I yield back, Mr. Chairman, or yield to the gentleman—no, I am out of time.

Mr. GOHMERT. I thank the gentleman.

The Chair now recognizes the distinguished gentleman from Virginia, Congressman Scott.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Chairman, one of the issues we have been working on is ID theft and the statutory maximum is not usually the problem. The problem is that these cases don't even get investigated much less prosecuted.

And so let me ask in that line, Mr. Downing, is unauthorized possession of credit card numbers, passwords, ID information—is unauthorized possession only a crime?

Mr. DOWNING. Under criminal law, it generally has to be with an intent to commit a fraud. So mere possession may not be but in almost all cases we can show that there is a intent to commit a fraud.

Mr. SCOTT. Well, you have—but just—if you just looked in my computer and found all kinds of credit card information you would have to either show that I intended to do something with it or that I obtained it illegally.

Mr. DOWNING. That is right.

Mr. SCOTT. That mere possession is not a crime.

Mr. DOWNING. I believe that is the case.

Mr. SCOTT. Now, child pornography, if you found something on somebody's computer you wouldn't care how they got it, would you?

Mr. DOWNING. We would definitely care how they got it. It would also be a crime for mere possession.

Mr. SCOTT. Well, I mean, in terms—in terms of a crime being committed you could prosecute without being concerned about how they got it.

Mr. DOWNING. That is true. Mere possession of child pornography is a crime.

Mr. SCOTT. Is—do you know if in the Federal Government whether or not there is any requirement that banks try to limit ID theft by doing things like sending a real-time email every time a charge is made?

I mean, there is no technological problem with the bank if somebody uses a credit card instantaneously text messaging that to the user. Is there anything—does anybody have any authority in the Federal Government to require banks to do stuff like that?

Mr. DOWNING. As a technological matter, I assume that it is possible to do that. As far as the regulations——

Mr. SCOTT. But it is technologically possible to do it. Is there anybody in Federal Government that can order the banks to do that?

Mr. DOWNING. I don't know the answer to that question, I am afraid.

Mr. SCOTT. Under RICO, we—Mr. Downing, you want to use RICO for computer crimes. Why is not the underlying crime that you are investigating enough to access RICO rather than the fact that they used a computer?

I mean, if they—if they are doing some operation that is some big organized crime effort that ought to be enough to get RICO. Why do you have to show that they are using a computer? Why is that important?

Mr. DOWNING. There are, certainly, some cases where there is another predicate offense that could be used to prove the RICO. But there are some situations where it might not be. I am going to give you an example.

If an organized crime group were to use a denial of service attack against a gambling website, let's say, to prevent the site from operating right before a critical event, it would be an extortion under Section 1030(a)(7). It is not clear that that sort of extortion falls into traditional extortion statutes since there is no physical property at risk and no risk of harm to human life.

So it is true that there are some areas that could be done through a RICO prosecution, but we feel that this would close some gaps and allow us to make sure that it covers it in all situations.

Mr. SCOTT. You have in your testimony the statement that the Administration has proposed a mandatory minimum sentence of 3 years imprisonment as one appropriate way to achieve the needed deterrence.

Do you have any research that shows that mandatory minimums rather than longer maximum sentences subject to guidelines serves as a deterrence?

Mr. DOWNING. I am not an expert on the research on mandatory minimums, but I can say that this particular one is very narrowly focused.

Mr. SCOTT. Can you point to any—can you point to any research—you can't point to any research that shows that it serves as a deterrence.

Mr. DOWNING. I would be happy to research that issue and get back to you.

Mr. SCOTT. Are you aware of research that shows that mandatory minimums do not reduce crime and serve only to waste the taxpayers' money? Are you familiar with that research?

Mr. DOWNING. I am not aware of that research either. That is not my field of expertise.

Mr. SCOTT. Mr. Chairman, my time is just about up. But before I yield back, I would just like to ask for the record for the witnesses, I guess Mr. Downing and anybody else, on these reports, exactly what—how these reports work, who can ask for it, do you need a subpoena and then what happens to it because in earlier versions of Homeland Security, information sharing was very important.

So if Homeland Security got something the FBI and Department of Defense and everybody else could look at it, how this information is shared and what exactly—what information there can be, and

also we talked a little bit about the international aspects of the Internet and trying to prove who did it is a problem.

But another problem is if you find out who did it does the Department of Justice have jurisdictional problems—if things are going on in France that affect things in the United States how we deal with the jurisdictional problems, if anybody would want to respond to those for the record.

Thank you, Mr. Chairman.

Mr. FORBES [presiding]. Thank you, Congressman Scott. And do each of you have a comfortable understanding of what Congressman Scott needs to supply? Good.

If you have any questions I am sure he will be glad to clarify that for you and if you would respond to the record for him on that we would appreciate it.

Chair recognizes the former Attorney General of California, Mr. Lungren.

Mr. LUNGREN. Thank you very much, Mr. Chairman.

Secretary Chertoff, in the Cyber Security Task Force we had on the Republican side early this year information that we got both public and private was that the best estimate was that perhaps 85 percent of intrusions in the cyber world could be taken care of if we just had good cyber hygiene and that because of that, because we don't have that, the 85 percent clutter that is out there makes it more difficult for to identify the 15 percent of the more serious nature.

When we are asked to perhaps pass new laws with respect to criminal sanctions and so forth, I guess one of the questions our constituents would ask is are we as a government as well as the private sector doing what we need to do to identify and encourage good cyber hygiene, and if not, why not?

Mr. CHERTOFF. Well, Congressman, I think you are dead right about this. I think that, and I can't tell you if 85 percent is exactly the right number, but I think you could take a lot of hay off the haystack with good cyber hygiene. What do I mean by that?

I mean appropriate use of passwords and changing of passwords, appropriate implementation of access controls, appropriate rules about who and what can download off a network and who and what can insert various kind of media into a network.

And you are quite right. A lot of this is in private hands and that is why when I look at the Administration's proposal, in many ways, to me, the more significant element has to do with the requirements as it relates to critical infrastructure and requiring that a nationally significant critical infrastructure have plans and programs in place to make sure they have cyber security and much of that involves internal processes and internal programs.

Now, there are a lot of different ways to skin the cat and I am not prescribing one particular way to do it. But a big challenge is to architect your internal security system so that it is not so cumbersome that people just avoid it altogether but that it is robust enough so that it is not obvious or easy for people to penetrate it.

You know, take a very simple thing like the ability to take a thumb drive and put it into a network and download, as was reported to be the case with Bradley Manning. If you are dealing

with sensitive systems you ought to have restrictions on who has the capability to do that.

So, to me, rolling out a set of processes and having the private sector have to meet certain standards would take a lot of hay off that haystack.

Mr. LUNGREN. I guess it would be my observation that as we are looking at these proposals, and I certainly support us moving forward in the area of cyber security, enhanced awareness of it within our various laws, I would hope that we would have at least as much effort in the public and private sector on raising the awareness of the need for computer hygiene.

I mean, we need a equivalent of a Smokey the Bear campaign to somehow help us. That is not to say we ought not to do these things now.

One thing I would like to address to Professor Kerr and Mr. Chertoff and Mr. Downing is this. There has been a Memorandum of Understanding entered into by the—by DHS and by the Defense Department in terms of proper exchange of information, et cetera. I happen to think that is a good start.

However, if we do not from the beginning ensure that civil liberties are protected here and that we are not in any way acting in a position that does not recognize the traditional and constitutional priority of civilian control of the military, we are buying a real problem.

I guess my question—I will start with you, Professor Kerr, if you have some knowledge of that Memorandum of Understanding. Are you satisfied that that—it has reached an appropriate position of balance such that as we designate DHS as the primary repository of this information and the coordinator of information and—or overview of cyber security throughout the Federal Government that the concern—the legitimate concerns of civil libertarians or anybody, any American concerned about that, have been met?

Mr. KERR. I share, certainly, all of your concerns with the need to protect privacy and civil liberties in this situation and also to balance that with the appropriate exchange of information within the government, which can be tremendously important.

As an outsider, I really can't tell how things are working. So I would love to know the answer just as you would like to know the answer but, unfortunately, I don't have it.

Mr. LUNGREN. Mr. Chertoff or Mr. Downing?

Mr. CHERTOFF. I think I can probably offer some insight into this because I think this in the main reflects an agreement that we had in the prior Administration between DHS and the Department of Defense concerning the proper allocation of responsibility.

With respect to government networks and the commercial domain, I think it was understood that the authorities should be DHS authorities to maintain the principle of civilian control.

On the other hand, there are unique capabilities in the Department of Defense both in terms of access to information and tools and techniques which are important to have available to deploy to protect the United States, and as long as that is undertaken under the authorities of DHS I think you manage to balance between using all of the elements of national power but having a civilian-

controlled and civil-liberty respecting way of actually operationalizing.

You know, I would leave you with this thought. I don't think security and privacy here are in conflict. I think they actually are mutually reinforcing.

You cannot have privacy on the computer if you don't have the security to be able to control who gets into your computer, and I think that it is important not to lose sight of the fact that it would not be a triumph of civil liberties to keep the U.S. government from protecting computers so the Chinese government could get on our computers. [Laughter.]

Mr. DOWNING. If I may, I would add, certainly, the Administration is very concerned about the sharing of information and that there are appropriate civil liberties and privacy protections in place.

One example of that is what I referred to earlier in the legislative proposal where sharing is going to occur under a set of rules that allows the private sector to share with the government. We have really been very careful to think through how that sharing is going to happen once it occurs inside the government, and there would be appropriate limitations to make sure that there isn't going to be any abuse.

Mr. GOHMERT [presiding]. Thank you, Mr. Lungren.

At this time we will hear questions from Ms. Jackson Lee of Texas.

Ms. JACKSON LEE. Let me thank the Chairman and the Ranking Member for this hearing. It is interesting to see our former Secretary of Homeland Security, thanking him for his service and as well the numbers of individuals.

Mr. Baker, I was looking for my friend from Texas but you have a good name and certainly I know that testimony has been productive. Mr. Secretary Chertoff would know that I was in Homeland Security and going back to Homeland Security, still serve on Homeland Security and cyber security has been a enormous issue.

I am going to go right to you, Mr. Secretary, and I think we do have a dilemma between the First Amendment rights, as we have always had a tension, the whole question of the—when we had the discussion on the PATRIOT Act was during your tenure and some of the ramifications of that.

But I am going to go directly to an entity, that preceding 9/11 there were challenges and that is China, and cyber security is not any longer a fly that we swat at. It is annoying. They have just gotten my formula for the—or the formula for how to do a Gucci purse or they have just found out how to make Colgate toothpaste or at least label it and say it is Colgate toothpaste.

How dangerous is it to have a friend that is engaging in the intrusion of one's cyber system and does that friend's accessibility then open it up to individual—to entities that would wish to do us harm?

Mr. CHERTOFF. Well, I think, you know, the National Counterintelligence Executive recently publicized the extent to which our networks and our systems are being penetrated by foreign powers, and I would—I would have to say I think it is now a general consensus that in terms of both our economic well being and poten-

tially our national security and military posture the ability of foreign governments to penetrate into our networks is probably at the very top of the list of threats that we face.

You know, I have heard people debate whether the theft of intellectual property has national significance. If you consider the amount of money and time we spend developing our technological advances, to have somebody come in and steal it and short circuit it is nothing less than giving away our economic competitiveness.

Beyond that, again, just relying on open source public documents like the U.S.-China Security Commission, we know that in China, for example, there is a military doctrine that looks to cyber warfare as one of the domains of warfare.

So, again, we have to be concerned about the possibilities, as Mr. Baker said, either in a tense situation or even in a peacetime situation a foreign adversary taking advantage of their ability to distract us by degrading or disrupting our networks.

So, you know, there are multiple dimensions to this. There are some diplomatic issues that need to be pursued. But most important, I think, we need to have the internal capability to manage our risk in a way that does not leave us hostage to foreign actors.

Ms. JACKSON LEE. I thank you. And Mr. Baker, I don't know if this—thank you very much, Secretary—whether this would fit you but on the Homeland Security side we are completely frightened of this process or prospect of cyber security as it relates to, and I know that the government witness is from Intellectual Property but the extent that cyber security can intrude on water distribution, electrical grids and how much government oversight, intrusion and emergency action should be engaged in as it relates to cyber security or the protection of our cyberspace.

There are a lot of bells going off but how much government activity should we have? How precious is this cyberspace that it could literally shut us down as a Nation?

Mr. BAKER. The cyberspace is precious. It is absolutely precious. We have to be worried about it being degraded and destroyed, disruptive and having a shut down, having significant parts of our economy shut down.

As others have said, I think we are in, you know, based on everything that I have seen, sort of a pre-9/11 mode right now where we see we have got some significant problems. We see we have got significant vulnerability. We have got adversaries out there that are serious about doing us harm and we need to get going and we need to get organized.

Ms. JACKSON LEE. What would you want us to do and——

Mr. BAKER. So we need—we need to figure out one thing, just for example, and was talked about here. One thing we need to figure out is as a society how much government involvement, meaning how much government monitoring of private communications, do we want and are we willing to tolerate.

And if we are going to have government monitoring of private communications in order to obtain information to protect us from cyber security threats, how are we going to monitor that, how do we monitor the monitoring. In other words, what privacy protections do we have in place, what oversight.

We have to pay for that oversight. Everybody talks about oversight. Oversight is expensive so we need to make a commitment that we are going to pay to have the right people in place to do that kind of oversight.

So I think it is inevitable that you are going to have government monitoring of private communications to some degree. The question is how much and then who watches to make sure that we are all comfortable with what is going on.

So I think it is—I think you are going to have—you have to have—I think no entity standing alone, private sector or government, anybody else, military, civilian, has all the tools necessary to address this threat.

We need to bring all of our resources together in a way that we are all comfortable with and then move forward.

Ms. JACKSON LEE. Mr. Chairman, would you allow Mr. Kerr to answer that question?

Mr. GOHMERT. Yes, without objection. Mr. Kerr, you may answer.

Ms. JACKSON LEE. And you might put your influence on the question. Thank you.

Mr. KERR. Yeah.

Ms. JACKSON LEE. And I thank Mr. Baker. Thank you, Professor.

Mr. KERR. Thank you. I think striking the right balance is quite difficult then and Mr. Baker's answer raises, I think, what is the missing half of the puzzle that we are looking at in this hearing, which is the procedural rights, the rights of government investigation.

The problem in cyber security from the standpoint of criminal law is not that the punishments aren't high enough. The punishments are not only as high as they are in non-cyber crime laws. In many ways, they are higher.

The difficulty is it is very difficult to catch people. So what tends to happen is the government wants more investigatory power. That becomes quite controversial. So instead, the government gets broader and broader substantive criminal laws and greater and greater punishments for crimes.

We should not use substantive criminal law and the Computer Fraud and Abuse Act as a substitute for the difficulty of catching the bad guys. We should focus on making sure the government has the power necessary to catch people that are engaging in wrongdoing online.

Ms. JACKSON LEE. I thank the Chairman.

Mr. Chairman, if I could just say to you or say for the record I know that we are in the Crime Subcommittee and the Committee dealing with terrorism but I truly believe I think Secretary Chertoff and I think Professor Baker might answer Mr. Kerr's point.

I think we need to ramp up and get coordination between military, civilian and government resources. We need to get in front of this. If we are pre-9/11 on cyber security we have got some work to do, and I hope this Committee can be part of the solution, Mr. Chairman.

I thank you very much for yielding.

Mr. GOHMERT. Thank you, Ms. Jackson Lee, and you do make a very good point. We do need to get ahead of it and I appreciate you all addressing that. Hopefully, we will get into that a little further.

At this time, I have the Honorable Mr. Goodlatte from Virginia with questions.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Welcome, all of you. I want to direct this first question to Mr. Downing and Mr. Baker.

The Administration proposal includes a so-called "name and shame" provision to coerce industry to beef up cyber security. We certainly understand what that objective is but I wonder if that doesn't paint a target on the backs of vulnerable systems for cyber criminals to exploit or to encourage others to keep their problems as hidden as possible so that they won't be discovered to have been put in that situation.

I wonder if you might comment on that, starting with you, Mr. Downing?

Mr. DOWNING. Certainly. The—it is important to understand that this publicizing the vulnerability of a particular company is done at an extremely high level. It wouldn't reveal any particular threats that would be successful against a network. It would simply provide some information to the public and to the government about how well the company is doing overall.

I think it is also important to think about what sort of incentives we think are appropriate to encourage the kind of better cyber security behavior that we would like to see. One option that the Administration has not proposed is to create a huge regulatory framework that would require lots of fines and auditors and all that sort of thing.

Instead, it is a light-touch regulatory idea that would require but there still has to be some incentive made to cause companies to change their behavior. And so in this way, we think that by publicizing those that need to improve, that will provide a significant but not overreaching type of incentive to get them to change.

Mr. GOODLATTE. Mr. Baker?

Mr. BAKER. Yes, just real quick.

I think you are right to be concerned about that. I think the Administration understood that and tried to come up with a solution where there was a sufficient amount of enhanced incentives for people to—companies to improve their cyber security posture without making them a target, as you suggest.

I think you are right, we need to make sure we get the legislation right on that point. I would say, however, I mean, I think to a certain degree even today companies face risks in this area by not exposing to some extent what their vulnerabilities are because they have obligations to their shareholders and reporting requirements to the SEC to make known a set of risks that may be material in some fashion. The SEC recently put out some guidance on this.

I think that is very significant. I mean, I think there is an incentive already and I just think it is unrecognized.

Mr. GOODLATTE. Thank you.

Mr. Chertoff, how can Congress encourage the kind of innovative solutions we need from the private sector for cyber security and at the same time avoid a one-size-fits-all regulatory scheme?

Mr. CHERTOFF. Well, first, let me say that, as I said in my opening statement regarding the legislation, I think it is a good start but I think there are some pieces that need to be strengthened.

The good start piece is the concept of having the government lay out general standards and requirements but allowing the private sector to meet those standards using a variety of different methods. That is actually pretty similar to what we did in the chemical security area back when I was at DHS.

So the good news is I think that gives you flexibility and allows people to tailor an approach, including one which the private sector can help to develop.

I think on the—on the disappointing side, I would actually like to see some tougher responses to the issue of those elements of critical infrastructure that don't meet those standards or requirements because I think if you have a serious vulnerability in our electric grid or our water or any other important element of national security we are not going to have a lot of time to coax those entities into coming into compliance.

We need to have the ability at some point to compel them to come into compliance. So that is an area where I would, frankly, like to see a little bit of strengthening.

Mr. GOODLATTE. Thank you.

And back to you, Mr. Baker, how would including the CFAA within RICO help protect Americans from cyber criminals?

Mr. BAKER. It is a further tool that prosecutors can use to go after these very aggressive robust organized crime groups, mainly located overseas, and I take Professor Kerr's point. It is difficult.

You have to have two things. You have to have the legal tools in place so that you can investigate and prosecute these crimes if and when you get your hands on somebody.

But then we need to work with our international partners as the FBI does regularly to actually go out and get them and bring them to justice either in the United States or in a separate jurisdiction. But I think RICO is another tool that strikes me as appropriate here because that is what is going on. Organized crime groups are using the Internet to steal a vast amount of funds.

Mr. GOODLATTE. Thank you very much.

Thank you, Mr. Chairman.

Mr. GOHMERT. Thank you, Mr. Goodlatte. And having been a judge for a decade and at times sat on the bench and thought does this lawyer not know that he's wasting his time asking those silly questions, it is a real honor to listen to such insightful questions that I think we have heard on both sides of the aisle here, and it points to the understanding people here have of the risks and problems inherent in what we are talking about.

One of the things that—I don't know, it may be the only thing that the Heritage Foundation, the ACLU, Mr. Scott and I have agreed on and that is that we have over criminalized so many things, 5,000 or so crimes.

We don't even know how many because they are not required to come through the Judiciary Committee in order to slap a prison

sentence on, and there are so many things that have been made a crime. And people say oh, well gee, the Justice Department would never pursue anything like that.

But it turns out it is not just up to the Justice Department. You know, we had a hearing previously where a guy just didn't stick the little sticker on his package that had an airplane with a line through it and he went to prison. You know, a guy received an orchid from a South American company without properly filling out their material. He went to prison for 18 months.

So some things do get prosecuted. The poor guy that sent the package without the sticker with the airplane with the line through it was run off the road with what sounds like what amounted to an EPA SWAT team, ran him off the road, threw him to the ground, handcuffed him and hauled him in.

So we are rather sensitive to over criminalizing and if I understand correctly we are talking about the potential for the Federal Government to run somebody off the road like they did the gentleman from Washington State and put him in handcuffs because he checked that he had scrolled down and read and agreed to the end user agreement and he didn't actually do that, and then as a result now he has committed a Federal crime.

Is that a possibility, Mr. Kerr?

Mr. KERR. It is certainly my understanding of the Justice Department's interpretation of the law but I don't know if the Justice Department here would agree.

Mr. GOHMERT. Well, and then a good question was asked, Mr. Baker. How much government monitoring of private communications are we going to allow, and that has been a concern of a lot of us on both sides of the aisle.

Have any of you read the President's American Jobs Act? Not my American Jobs Act. It was two pages. But the President's that was 155 pages.

Were you aware that he set up a—the Public Safety Broadband Corporation in that that will help take care of our use of broadband? I mean, had you all heard that?

Well, it won't do anything to create jobs but it will give more government control of our broadband, and you couple that with a potential push for more control of the Internet here it causes me some concerns.

But on the same—at the same time, I know the question was asked who would have ever dreamed that planes would be flown into a building and some of us said well, that was Tom Clancy back several years ago had a hijacker fly one into the Capitol. Well, Clancy, if you—he has also written about this Net problem and Net security.

So I mean, it is clearly an issue that we have got to deal with. Let me ask what—Mr. Chertoff, I will start with you. You said the value of damage for our intrusion may exceed the value of the asset. How do you think it would be damaged, if you could be more specific?

Mr. CHERTOFF. I mean, here is the challenge you have, I think, in the case of some of the critical infrastructure. You might own a power plant and it might be worth a certain amount of money,

and no rational person is going to invest more in securing the power plant than it is worth.

Mr. GOHMERT. Right.

Mr. CHERTOFF. I mean, that is common sense. The problem is, and we have seen this both in terms of cyber and in the physical world, that power plant may be critical in terms of the whole surrounding community, even a state, involving public health, involving public safety, involving public communication.

If that power plant goes down, there could be an enormous loss of life and economic damage that exceeds the value of the asset.

So the challenge is how do you make the people who operate the asset and own the asset invest enough to protect against a cyber attack, and I think that is where it is appropriate to have the government play a role in laying out a set of general metrics and a set of general standards and then allowing the private sector to figure out the precise way in order to meet those standards and metrics.

Mr. GOHMERT. Anybody else care to comment on that aspect? If not——

Mr. SCOTT. Can I make another comment, a quick comment?

Mr. GOHMERT. Well, sure. It is your turn.

Mr. SCOTT. No. I have already asked questions.

Mr. GOHMERT. Oh, okay. All right. Yes. Then we will go to Mr. Scott.

Mr. SCOTT. Mr. Chairman, Mr. Baker and Professor Kerr have talked about the problems in defining "exceeds unauthorized access." You kind of know it when you see it but, obviously, that term can cover a lot more than we want covered and, for the record, they can—if they have any suggestions as how we can define "exceeds unauthorized access" in a way that covers what we want covered without being over expansive that would be helpful.

Thank you, Mr. Chairman.

Mr. GOHMERT. Well, thank you, Mr. Scott. Do you have any further questions? I mean, we could mount to a second round if you wish. Pardon?

Mr. SCOTT. If you want a second round.

Mr. GOHMERT. Okay. Go ahead. I will allow Mr. Scott to complete—you can see the two of us are here and this is such an important issue. If you don't mind, let's—go ahead, Mr. Scott, if you would.

Mr. SCOTT. Well, if—do you want to—do you want to—do you have any recommendations on "exceeds unauthorized access?"

Mr. KERR. I do. I think there are two basic strategies that could be used to limit "exceeds authorized access."

One would be to just amend the current definition. Unfortunately, the current definition of "exceeds authorized access" is entirely circular. It says that you exceed authorized access when you do that to which you are not entitled, which doesn't really answer the question.

It just makes the issue entitlement rather than authorization, just substitute a word. So one method of limiting the statute would be to clarify that that definition does not apply to mere terms of service violations and computer use policies, essentially just defining by exclusion that which the definition does not apply.

And another approach would be to limit the substantive statute rather than limiting "exceeds authorized access" by saying that Section 1030, the Computer Fraud and Abuse Act, only applies to obtaining personal information or valuable information rather than any information.

So under that approach, violating a terms of service or violating a terms of use could in fact lead to criminality but only in the kind of cases that the Justice Department focuses on, namely those cases where there's access to a sensitive database by a government employee or particularly valuable information that is taken in violation of an employer's computer use policy.

Both of those strategies, I think, are two different ways of getting to the same conclusion and either is acceptable.

Mr. BAKER. I think the main thing that I am concerned about is making sure that we have the tools necessary to prosecute insiders who have access to vast amounts of data whether they are at a government employer or whether they are with a private-sector employer.

I mean, if you think about how much data employees at Facebook or Google have access to, it is amazing, about—access to information about Americans and what Americans are doing. And so I think that is the kind of thing that I want to make sure that we don't change the statute to somehow inhibit or cripple, in some ways, the ability of the government to prosecute those kinds of cases.

So if you were to somehow take—I mean, I have seen some of the suggestions with respect to amending the definition of "exceeds authorized access."

As long as they still allow for prosecution of in the employment context I think that would be the key thing and it would avoid some of the things that Professor Kerr was talking about in terms of what—you know, misrepresentations that people make on Facebook or website and so on.

The other—I think his suggestion with respect to amending the specific provision of 1030(a)(2)(C) I think shows—I think there is more promise there. It is a more narrowly-focused provision. It doesn't deal with this definition. It applies to the whole statute, and I think it does get at the kinds of cases where somebody does something, accesses information in order to steal something or do something fraudulent or cause some harm. I think that shows much more promise, at least in my mind.

Mr. SCOTT. Mr. Downing, this is limited to—this entire code section is limited to computers—government computers, financial institutions and protected computers. What about my computer? Is that—is that a Federal jurisdictional problem?

Mr. DOWNING. The computer in your office? Yes, it would certainly be covered. A protected computer——

Mr. SCOTT. What about my personal computer?

Mr. DOWNING. Protected computer is actually a fairly broad term. So it would include——

Mr. SCOTT. What is—what is not included?

Mr. DOWNING. Not included would be certain stand-alone computers that aren't connected to the Internet, for example. Relatively

rare these days. Most computers are covered by the term "protected computer."

Mr. KERR. If I could add—if I could add a brief comment, actually computers—stand-alone computers are also protected computers. Every computer in the United States is a protected computer because the definition of protected computer includes any computer that affects interstate commerce, a term of art which included anything that the Commerce Clause can include, and under the court's—Supreme Court's—Commerce Clause jurisprudence that would include every computer.

So basically everything with a microchip except for a handheld calculator—there's an old 1980's era exclusion in there—is included.

Mr. SCOTT. Thank you.

Mr. Downing, under civil forfeiture, who gets the proceeds of the forfeiture?

Mr. DOWNING. Generally, the proceeds are kept by the government. In part, they are used to further enforce the laws and part of it is put back to the general Treasury.

Mr. SCOTT. Does the local—one of the problems I have with some of these civil forfeitures are is there is an incentive to do law enforcement based on how you can make money and fund your local operation, which kind of distorts the criminal justice system.

When you say the law, does the FBI get to keep the money generally or does the local FBI office get to keep the money and avoid cutbacks in employment that may be coming with this budget deal?

Mr. DOWNING. I am afraid I don't know all the ins and outs of the forfeiture rules. But my understanding is that it doesn't go to the local office at all, no. This is an important tool for getting at certain kinds of actors where criminal law is not sufficient.

Mr. SCOTT. Well, yeah. And I know why we have civil forfeiture. My question is whether it is distorting. You have got Eighth Amendment problems of proportionality. Two people commit the same crime and one loses a house and a car. Another one doesn't lose anything.

Who gets the money and whether or not you want civil forfeiture rather than criminal forfeiture means that you don't have to prove that somebody is guilty. They got to prove their innocence to get their money back, and so even if they are innocent they are out of attorneys' fees and a lot. So civil forfeiture, if not done properly, can be problematic.

Thank you, Mr. Chairman.

Mr. GOHMERT. Okay. Thank you, Mr. Scott, and I just want to follow up. Now, of course, we have had a Federal court say you can't prosecute, as has been done before, a cheerleader mom that violates an end user agreement. But it brings to question in my mind is there anybody that polices the end user agreements, just what people are required to agree to before they utilize a service.

Mr. DOWNING. Well, I am not sure what you mean by polices but, certainly, there are a couple of forces that would control what gets put into an end user agreement by a big website.

Certainly, these things are made public because, obviously, people are signing them, and when Facebook recently or perhaps it was last year changed their user agreement in a way that was real-

ly egregious in the eyes of many of the customers, they protested and moved away from that—using that service. So there's a real vote-with-your-feet kind of possibility here.

The importance of end user agreements is also important in the context of the Federal Trade Commission. So companies have to live up to their—what they say in their agreements, and if they fail to do that then they can be sanctioned for unfair trade practices.

Mr. GOHMERT. And we know here on the Hill—it hadn't been disclosed publicly—we have had government, our congressional computers hacked from foreign countries, at least one, and it is a threat and it is—can be international terrorism of a sort when you, as you all have discussed, realize what could be done by destroying our Internet usage.

But by the same token, you don't want to create a problem for the greatest freedoms any country has ever experienced, as we do here.

I know there are some that say well, gee, the Justice Department would never pursue that because that would just be too much. But we have heard example after example of when prosecutions have occurred that people can't believe. It just sounds like a Kafka novel or something.

But I would hope that on both sides we are ready to be as tough as possible on espionage, whether it is domestic or foreign, so that the Homeland Security, our Justice Department intelligence has the ability to pursue those that want to hurt us but at the same time not pursue somebody just because they made some minor mistake or even negligently made a mistake.

And one of the things we pushed is, and we haven't done it yet, defining what things are really just clerical administrative mistakes individually where maybe you should have somebody subject to a fine and what requires prison sentences, forfeiture, all of those kind of things so that we don't keep—just so that we can show how tough we are for the next election criminalize some conduct where it is more appropriate to just make it a fine or decide does it justify somebody being thrown down in front of their wife and kids and handcuffed and hauled in.

So I think that is the issue and a lot of us on both sides of the aisle want to make sure that we don't do that.

Before we conclude the hearing, you have given your opening statements. You have answered questions and been very gracious in doing so. But I would just like any final comments based on the questions that have been asked, things that may have been triggered in your mind, things that we ought to consider because this is all be part of the congressional record here.

So if you would, starting with Mr. Downing.

Mr. DOWNING. Thank you for that opportunity.

There have been a lot of characterizations of what the Department of Justice position is on the 1030(a)(2) question of "exceeds authorized access." Let me be very clear that DOJ is in no way interested in bringing cases against people who lie about their age on a dating site or anything of the sort. We don't have time or resources to do that.

And, in fact, no court has in fact ruled that that is an appropriate use of the statute and, quite to the contrary, the one case

that has addressed it ruled that it is not an appropriate use, and the government has not brought any further cases. So we are a little bit concerned whether this is truly a problem.

Given all that, however, we recognize that this is an issue, and we are very much interested in working with the Committee to resolve this question in a way that is proper for all.

What we do need to be careful about is to make sure that as we do that, we don't harm the ability to bring cases that everyone in the room would agree are proper and appropriate ones.

And so, as we think about what sort of solution might be available here, that we do it in a way that isn't going to cause other harm and actually harm our ability to create deterrence in this area, which is so important.

Mr. GOHMERT. Mr. Chertoff?

Mr. CHERTOFF. Well, I guess I would just conclude by saying I do think it is worth giving serious consideration to Professor Kerr's point about maybe some narrowing of the—of the statute.

I agree with Mr. Baker that I think we are probably more concerned about insiders and employees who exploit their privileged position than we are people getting on Facebook.

But the other point I would make, which I think is important, is there is a little bit of a tendency over—observed over the years to deal with the issue of criminalizing by simply piling on additional penalties and jail time rather than recognizing the real challenges and being more efficient and more effective in enforcing the law against a broader number of law breakers. And here the problem is a lot of the activity is overseas, and we are not going to find the people who do this stuff because they are never coming over to the United States.

And, frankly, in some countries there is not a lot of interest in cooperating with us.

So an area which I think is worth exploring is what we can do to leverage, again, all of our economic and other powers to really induce countries in the world that have tolerated open and notorious criminal activity on the Internet into coming into compliance with what ought to be any reasonable international norm about preventing this kind of cyber criminality.

Mr. GOHMERT. Do you have any last suggestions about how we do that, how we deal with foreign individuals?

Mr. CHERTOFF. Well, you know, I mean, one of the, of course, is a topic for a whole separate hearing probably. You know, we have entered into conventions with other countries and, certainly, the Europeans have been—have been cooperative.

But there are countries in the world where, although there is lip service to wanting to play by the rules, they will tolerate the existence of these servers which are nothing more than marketplaces for criminal activity.

Now, we do have a lot of economic power. We have trade power and the ability to use that, to say to some of these countries you not only have to sign up to doing the right thing but you have got to then walk the walk, I think is worth taking a serious look at.

Mr. GOHMERT. Yeah. Those sanctions work so well. I mean, basically we brought Iran to their knees.

Oh, wait. No, that hasn't worked. Never mind.

Mr. Baker?

Mr. BAKER. Yes, Mr. Chairman, just two quick points.

One, I agree with Mr. Downing. I don't foresee the Justice Department prosecuting the kinds of cases that folks are concerned about. I understand the concern. It is a legitimate——

Mr. GOHMERT. But you understand, we just want to get the law right so it is not even an option. We give them the power to go after the bad guys as completely as necessary without even risking some runaway prosecutor.

Mr. BAKER. I agree, but, you know, my experience is with any statute that you write there is this huge amount of ambiguity in any of these statutes.

I mean, if you look at the mail fraud and wire fraud statutes, they don't even define fraud and so the government and courts have figured out how to—how to prosecute cases and how to adjudicate those kinds of cases over the years. But I—it is difficult to write a statute that is so tightly focused to only get at the problem you are trying to get at without having some kind of collateral effect as well.

I just—I would just be cautious about that and I would say then that it is a matter then of oversight for this Subcommittee to make sure that you stay on top of the Justice Department, to make sure you know what they are doing in terms of these prosecutions and bring them up here and have them explain why they did X, Y or Z in a particular case. That would be my suggestion on that.

To go back just to close a loop, I think on a question that Mr. Forbes had raised earlier, just briefly, I think in terms of the legal problems that we are facing versus other kinds of questions, again, I think it is a policy problem more than a legal problem.

But I think folks should be comfortable, I think, that the President has the authority, in the event of an imminent or actual attack on the United States, he has the authority under the Constitution and laws of the United States to take whatever actions are necessary to protect the country today. He has that authority today.

The difficult question is figuring out how he would implement that authority, how that would be done and exactly what would the military do and under what circumstances or what other elements the United States government would do.

That is what we need to figure out, as opposed to worrying about whether we have, you know, enough legal authority and whether he is going to be hamstrung in the event of a crisis.

I think—I think he does have that authority. We need to figure out technically, strategically, doctrinally what we want to do to protect us.

Mr. GOHMERT. Thank you, and——

Mr. SCOTT. Mr. Chairman?

Mr. GOHMERT. Yeah.

Mr. SCOTT. I would hope if the President concludes that we are in a imminent threat that he wouldn't have to fool around and try to figure out how this fits under a computer law where he can take——

Mr. BAKER. I don't think he would have to do that. That is what I am saying. I think he has the authority to take whatever steps he deems appropriate in a crisis of that nature.

Mr. SCOTT. Without having to worry about whether it technically fits under some computer—whether they are using computers as they do it or a protected computer or something like that. If he makes that——

Mr. BAKER. That would not be top on his list.

Mr. SCOTT. If he makes that conclusion then we would expect action to be taken.

Mr. BAKER. I think—well, I am suggesting this would be the situation in a cyber event and he could take whatever action are necessary whether it is a cyber action or some kind of physical kinetic action.

Mr. GOHMERT. Okay. Thank you, Mr. Scott.

And you had said we need to figure that out and so I would ask you have recommendations in that regard if you would submit them to the Committee that would be extremely helpful.

It is helpful to point out we need to figure this out and what we should do but it is even more helpful when you have a suggestion as to the best way to proceed in figuring it out.

Mr. BAKER. Yes, sir.

Mr. GOHMERT. But Mr. Kerr, final comment?

Mr. KERR. Thank you, Judge Gohmert. Just two quick points.

First, I think the concern of the Justice Department's overbroad reading of the Computer Fraud and Abuse Act is a real one.

Just a few weeks ago, the Ninth Circuit granted rehearing in a case in which the earlier panel of the Ninth Circuit Court of Appeals had held that private-sector employee computer use policies do in fact—are in fact—criminally enforceable. The employer had a policy that said you can't use the computer for non-business reasons.

The Justice Department prosecuted the employee for using the computer for a non-business reason. The Ninth Circuit granted rehearing. We don't know what the court's interpretation will be but this is a very real current question.

And then, second, on the question of civil RICO and mandatory minimums under the Computer Fraud and Abuse Act, I think it is really important to be specific as to where are the cases where this is necessary.

In my experience, the actual penalties in Computer Fraud and Abuse Act cases tend to be relatively low because the damage tends to be low in the kinds of cases where the Justice Department actually catches the bad guy.

So I don't think there is a lot of—there aren't any demonstrated cases of which I am aware of where, for example, there is the need for a mandatory minimum where under current law there wouldn't be and there is an actual case where the law would have applied.

So some of the Justice Department's concerns strike me as very abstract, kind of, "well, if we ever catch someone like this it would be nice to be able to give them a higher sentence." I think we should be responding to real problems, not abstract hypothetical ones.

Mr. GOHMERT. Okay. Thank you.

We appreciate the witnesses being here. We know you are not here because of the money witnesses get paid since you don't get paid at all but—and Mr. Chertoff, nice to see you again. I was a little bit surprised you were willing to come in voluntarily after some of the hearings you have had here but——

Mr. CHERTOFF. Yeah, I was a little surprised too, actually. [Laughter.]

Mr. GOHMERT. Well, we do appreciate all of you being here on such a serious topic that has to do with our national security.

Thank you all very much. This hearing now is adjourned.

[Whereupon, at 11:45 a.m., the Subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

Response to Post-Hearing Questions from Richard W. Downing, Deputy Chief, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice

Questions for the Record

The Honorable Robert C. "Bobby" Scott, Ranking Member
U.S. House of Representatives Judiciary Committee
Subcommittee on Crime, Terrorism and Homeland Security
"Cyber Security: Protecting America's New Frontier"
November 15, 2011

1. ***Would the Administration's bill apply the same mandatory minimum sentences proposed in the bill to conspiracies to commit the offenses for which these sentences apply?***

The only mandatory sentence proposed in the Administration's legislative proposal is for the proposed new offense for aggravated damage to a critical infrastructure computer. An individual would have to be charged with a substantive count of this offense to be subject to a mandatory minimum sentence, as proposed 18 U.S.C. § 1030A does not include conspiracy language (e.g., "or conspires to commit").

2. ***Do you have any research that shows that mandatory minimum sentences rather than longer maximum sentences, subject to the Sentencing Guidelines, serves as a deterrence to crime.***

There is ample research showing that swift and certain punishment does have a strong deterrent effect on criminal behavior. *See, e.g.,* Cook, Ludgwig, and McCrary, *Controlling Crime: Strategies and Tradeoffs,* National Bureau of Economic Research (2011). This research supports our belief that our proposal will send a clear deterrent message to criminals and terrorists that any attempt to damage a vital national resource will result in serious consequences.

We would of course welcome discussion about this and other parts of our proposal. The mandatory minimum proposal was intended to add an element of deterrence to our overall efforts to protect critical infrastructure. However, there may be other ways to achieve this effect, and the proposal we put forward is not the only way to achieve adequate deterrence.

3. ***Please explain the bill's proposed process for information sharing with the government, including any requirements for subpoenas for the information, the standards by which the information is to be shared, the type of information which may be shared, and with whom it would be shared.***

Section 245(a)(1) of the Administration's cybersecurity proposal would govern private sector sharing with the Government. It would permit companies and other non-governmental entities to share information that is lawfully intercepted, acquired, obtained, or possessed. Such information would be reported to the DHS cybersecurity center, and sharing would have to comply with the privacy and civil liberties requirements of section 248. Such sharing must be for the purpose of protecting an information system from cybersecurity threats or mitigating such threats, and it may occur only if reasonable efforts are made to remove information that can be used to identify specific persons unrelated to the cybersecurity threat. Under section 245(b)(1), the DHS cybersecurity center would be permitted to further disclose shared information to appropriate governmental and private

entities, (such as, for example, the National Counterterrorism Center), consistent with section 248(a)'s privacy and civil liberties requirements, for the limited purpose of protecting information systems from cybersecurity threats, mitigating cybersecurity threats, or, with the approval of the Attorney General, to law enforcement entities when the information is evidence of a crime that has been, is being, or is about to be committed.

Thus, the statute expressly provides standards for the type of information that may be shared (lawfully obtained information from which reasonable efforts have been made to remove identifying information), the purpose for which such sharing may occur (to protect against or mitigate cybersecurity threats), the manner in which sharing should occur (consistent with requirements of section 248 that protect privacy and civil liberties), and the conditions under which any further sharing may occur (with other entities for purposes of protecting against or mitigating cybersecurity threats or with law enforcement if it is evidence of a crime and the Attorney General approves it). These sections cover only voluntary disclosures; no provision would create new subpoena authority or subpoena requirements. DHS would be in the best position to provide further information about implementation of this provision if you have additional questions.

4. ***With respect to the proposed extension of civil forfeiture provisions in the Administration's bill, is the 8th Amendment's requirement of proportionality of punishment a meaningful restriction on the amount which must be forfeited? Who receives the proceeds of civil forfeiture? Are attorneys' fees awarded to individuals who have had their funds or property forfeited but who are later found innocent of wrongdoing?***

In assessing Eighth Amendment challenges to forfeiture, courts have held that a forfeiture violates the Excessive Fines Clause when it is grossly disproportional to the convicted offense, based upon the four factors laid out in *United States v. Bajakajian,* 524 U.S. 321 (1998): (1) the essence of the crime of conviction and its relationship to other criminal activity; (2) whether defendant fits into the class of persons for whom the statute was principally designed; (3) the maximum sentence and fine that could have been imposed; and (4) the nature of the harm caused by defendant's conduct.

Although *Bajakajian* was a criminal case, courts have held that civil forfeitures are also subject to the Excessive Fines Clause. In addition, the Civil Asset Forfeiture Reform Act (CAFRA) of 2000 codified the application of the gross disproportionality test of the Eighth Amendment to civil forfeitures in 18 U.S.C. § 983(g). Section 983(g) provides that *all* civil forfeitures, regardless of the nature of the relationship between the property and the offense, are subject to challenge on the ground that the forfeiture would be "grossly disproportional to the gravity of the offense."

Consequently, an Eighth Amendment inquiry is focused on whether the forfeiture of a given category of property, such as the proceeds of the offense, unreported currency, instrumentalities and facilitating property, is "grossly disproportional" to the crime. As a result, the courts appear to be unanimous in holding that the forfeiture of the proceeds of the offense can *never* be considered disproportional because the forfeiture of proceeds is precisely calibrated to the gravity of the offense giving rise to the forfeiture.

However, most Excessive Fines Clause challenges have occurred with the forfeiture of instrumentalities and other property used to facilitate the offense. For such property to be subject to forfeiture at all, it must be "substantially connected" to the offense giving rise to the forfeiture. Once this hurdle is met, an Eighth Amendment analysis of the forfeiture can occur.

In the Comprehensive Crime Control Act of 1984, Congress established the Department of Justice Assets Forfeiture Fund (AFF) to receive the proceeds of forfeitures brought by the United States, such as those in the Administration's proposal. As codified at 28 U.S.C. § 524(c), AFF funds may be used to pay necessary expenses associated with such forfeitures, including the costs of managing and disposing of forfeited property. Congress also established a similar fund for seizures made by the law enforcement agencies of the Departments of the Treasury and Homeland Security. The Treasury Forfeiture Fund is codified at 31 U.S.C. § 9703. In appropriate cases, victims of crimes giving rise to forfeiture may also receive compensation for pecuniary losses resulting from the crime through the processes of remission and restoration.

Under 28 U.S.C. § 2465, amended as part of CAFRA, the United States is liable for reasonable attorneys' fees, other litigation costs reasonably incurred by the claimant, and post-judgment interest in any civil forfeiture case in which a claimant substantially prevails. Section 2465 does not apply to criminal forfeiture cases, in which the forfeiture attaches to the crime of conviction. As a result, if a defendant is not convicted of an offense, the property alleged for forfeiture based solely on that offense cannot be forfeited.

5. ***With respect to the proposal to extend RICO to certain offenses under the Computer Fraud and Abuse Act, why is it not sufficient that offenders be charged with the underlying computer crime offenses? And, for instance, if someone is using a computer to facilitate extortion, why isn't it sufficient to charge the offender with extortion?***

RICO should be extended because the fight against organized crime is far from over; rather, much of the battlefield has moved online. RICO has been used for over forty years to prosecute members and associates of racketeering enterprises ranging from mob bosses to Hells Angels to insider traders, and its legality has been consistently upheld by the courts. Members and associates of racketeering enterprises now commit computer hacking offenses in order to steal money, extort companies, and commit other crimes. The Administration's proposal simply makes clear that attacks on the confidentiality, integrity, and availability of computers should be considered criminal activities under the RICO statute – nothing more.

Congress passed the RICO statute to punish those who are members and associates of a criminal enterprise and who engage in racketeering activity. In order to qualify as a racketeering enterprise, the group at issue must have an ongoing organization with some sort of framework for carrying out its objective and the various members and associates must function as a continuing unit to achieve a common purpose. Further, the defendant must have either committed two acts of racketeering activity or agreed that a conspirator would commit two acts of racketeering activity.

Use of the RICO statute permits the full scope of the criminal racketeering activity to be tried before one jury. In cases involving computer hacking crimes, the members of the enterprise

may play different roles within the overall criminal scheme. For example, some enterprise members may steal databases of credit cards while other enterprise members contact the victims to extort them; some enterprise members may manufacture false credit cards which are used by yet another set of enterprise members to fraudulently obtain money or merchandise. While these individual crimes may seem unrelated or the evidence may be insufficient to charge each enterprise member in every racketeering act, the use of the RICO statute permits the racketeering activity tied to the racketeering enterprise to be tried in one case. Merely charging substantive offenses, such as extortion or fraud, may not be sufficient to charge all of the enterprise members who participated in the various parts of the criminal scheme.

One important example of a circumstance in which it is insufficient to charge offenders with the underlying crime is the case of the organization's leader – whether it is a traditional mob boss or the head or a computer organized crime group. In such cases, that leader may not directly commit the underlying crime. His role is to direct and operate the criminal enterprise, and he obtains the lion's share of the money, power, and influence generated by the enterprise. Thus, prosecutors have for years used RICO effectively to dismantle entire criminal enterprises, and the law must be updated to take into account the changing nature of criminality.

It should be noted that the Department of Justice has a thorough screening process for all RICO prosecutions. No RICO criminal indictment or information or civil complaint can be filed without the prior approval of the Organized Crime and Gang Section ("OCGS") of the Criminal Division. In order to pass OCGS review, prosecutors must demonstrate the existence of an aggravating characteristic of the case that makes RICO prosecution appropriate, such as that RICO is necessary "to ensure that the indictment adequately reflects the nature and extent of the criminal conduct involved in a way that prosecution only on the underlying charges would not," or "for a successful prosecution of the government's case against the defendant or a codefendant." *See* USAM § 9-110.310.

6. ***Please describe the any unique international challenges to investigating and prosecuting cyber crime, including any jurisdictional issues and obstacles.***

We face, on a daily basis, a variety of unique international challenges to investigating and prosecuting cybercrime. In many instances, we receive excellent cooperation from our foreign law enforcement partners. For example, the worldwide, and growing, network of 24/7 points of contact for urgent matters allows our investigators to preserve digital evidence located in foreign countries. The process works well and efficiently in helping to preserve evidence in many locations abroad. We in the Department work very hard to develop close relationships with our law enforcement colleagues in other countries and can report that in many places we have achieved outstanding levels of cooperation that have led to successful prosecutions in the United States.

Despite close relationships and good cooperative efforts, the time involved in the process of obtaining evidence from a foreign entity does make the investigation of such cases difficult. For example, IP addresses can be changed very quickly at a pace that exceeds our ability to obtain evidence. We have also experienced some difficulty obtaining subpoenaed information

from foreign corporations, including those that maintain a corporate presence in the United States.

We have also had significant problems with certain countries that have prevented us from successfully bringing cyber-criminals to justice. For example, we have seen (a) the targets of an investigation tipped off prior to the execution of a foreign computer search; (b) a lack of technical training causing foreign law enforcement to seize evidence in a manner that makes it difficult for us to use it for evidentiary purposes; and (c) foreign law enforcement authorities unable to respond to requests for assistance because their laws do not give them the authority to do so.

The Department has had some success in extraditing fugitives charged with cybercrimes in the United States to face U.S. charges. However, in some cases individuals who have committed computer related crimes in violation of U.S. law are located in countries with whom the United States currently has no extradition treaty or whose laws prohibit the extradition of their nationals. Since these criminals cannot be extradited to the United States, we are often left to rely on the prosecutors and judicial systems in these countries. The results in such situations have been mixed. Many times, offenders tried in foreign jurisdictions are given appropriate and fair sentences. However, we have seen more than a few defendants receive proverbial "slaps on the wrist" for extremely serious crimes, including little or no jail time and meager, if any, restitution to victims.

Because of these difficulties, it is vital that the Department have strong overseas representation to ensure that we can work more quickly and effectively with our international partners when investigating and prosecuting international computer crimes that target American citizens. Thus, the Department has requested funding to establish six Department of Justice Attaché positions at embassies around the world that would emphasize the investigation and prosecution of laws prohibiting international computer hacking and protecting intellectual property rights. The program would establish Department representatives in regions with a high incidence of computer and intellectual property crime and would help ensure that we can continue to protect American citizens' privacy, both at home and abroad.

7. ***Is someone who is found to be in possession of a Social Security Number (SSN) belonging to someone else guilty of a federal crime - assuming the owner of the SSN did not voluntarily give the number to the possessor or consent to it being given to that person? If not, would you support a bill to criminalize mere unauthorized possession of SSN's of others? Similarly, would you support legislation to criminalize mere unauthorized possession of passwords and other unique information necessary to log in to private accounts, credit card numbers, personal identification numbers, and other sensitive personally identifying information?***

Current federal offenses such as 18 U.S.C. §§ 1028(a)(3), (4), and (7), § 1028A(a), and § 1029(a)(3) address the possession of identifying documents, access devices, and means of identification, but include one or more additional essential elements, typically a specific intent to defraud (or, in the case of sections 1028(a)(7) and 1028A(a), a requirement that the possession be "without lawful authority"). For example, a person violates 18 U.S.C. § 1028(a)(7) if he or she knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another

person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law. A Social Security Number (SSN) can be such a means of identification, as defined in 18 U.S.C. § 1028(d)(7). So long as we could show that the individual who possessed the social security number had the requisite criminal intent, he or she could be prosecuted under this statute.

In general, we have not found proving criminal intent to be an insurmountable burden. Identity thieves generally possess hundreds or thousands of pieces of stolen identity information, and this fact alone is strong evidence of their criminal intent.

Without the criminal intent, such a statute might be too broad. For example, suppose a person left her social security card in her wallet at a convenience store check-out counter. Suppose further that the clerk picks it up and runs out of the store to return it. He would be in possession of her card, even though she did not voluntarily give it to him, nor did she consent to it being given to him. We would have to carefully consider how to draft such a statute to make sure that it would have an appropriate scope. Of course, we are always happy to work with members of the Committee on proposals to enhance our ability to bring identity thieves to justice.

8. ***Would you support a requirement that issuers of credit cards send an immediate email or text message to credit card holders each time their account is charged in order to notify them and better enable them to protect against financial loss and identity theft?***

We are always happy to work with members of the Committee on proposals to help consumers protect themselves against identity theft. In general, issuers have strong incentives to alert cardholders of fraud because the Fair Credit Billing Act limits cardholder loss to $50.00 for unauthorized charges if the cardholder notifies the issuer within sixty days of receipt of the transaction statement. As a result, many issuers have a practice of promptly contacting the cardholder by telephone or e-mail if a suspicious transaction appears on the cardholder's account. In addition, some financial institutions enable customers to sign up to receive notifications of every transaction. The benefits of these current practices should be balanced against the concern that automatic notification could cause consumers to ignore or "tune out" all notifications, including ones that might alert them to suspicious activity.

Response to Post-Hearing Questions from the Honorable Michael Chertoff, Co-Founder and Managing Principal, The Chertoff Group

Michael Chertoff's Responses to Questions for the Record
from Congressman Robert C. "Bobby" Scott, Ranking Member
Cyber Security Hearing
December 6, 2011

1. **Please describe any unique international challenges to investigating and prosecuting cybercrime, including any jurisdictional issues and obstacles.**

   In my opinion, there is a particular challenge to investigating and prosecuting cybercrime involving those countries that tacitly tolerate or encourage cyber misbehavior. Getting those countries to cooperate and actually arrest and prosecute cyber criminals is important to overcome this challenge. A second, lesser problem is that some companies simply lack the forensic capabilities to identify the cyber criminals who have performed these crimes.

2. **Is someone who is found to be in possession of a Social Security Number (SSN) belonging to someone else guilty of a federal crime - assuming the owner of the SSN did not voluntarily give the number to the possessor or consent to it being given to that person? If not, would you support a bill to criminalize mere unauthorized possession of SSN's of others? Similarily, would you support legislation to criminalize mere unauthorized possession of passwords and other unique information to log in to private accounts, credit card numbers, personal identification numbers, and other sensitive personally identifiable information?**

   I believe a bill to criminalize the unauthorized possession of Social Security Numbers (SSN), passwords or other similar sensitive information should, at minimum, have a requirement of knowledge and willfulness by the person in unauthorized possession of the sensitive information. I do not think, however, that it should be necessary to show an actual intent to take further action or steps to defraud.

3. **Would you support a requirement that issuers of credit cards send an immediate email or text message to credit card holders each time their account is charged in order to notify them and better enable them to protect against financial loss and ID theft?**

   I cannot provide a definitive answer to this question as I am not aware of how expensive it would be or how burdensome to the recipient it would be if this action were required. Moreover, conveying this type of information over e-mail or text message could create its own security and privacy vulnerabilities.

Response to Post-Hearing Questions from Orin S. Kerr, Professor of Law, George Washington University

Orin Kerr
Questions for the Record for Ranking Member Scott

Question 1: International Challenges

International issues pose a serious challenge in many computer crime investigations and prosecutions. To investigate and prosecute crime successfully, investigators must have the power to collect evidence and to arrest suspects and bring them into court. When a crime and investigation all occurs inside a single jurisdiction, this can be relatively straightforward: Investigators will have the power to collect evidence there and to arrest suspects and bring them into court.

In computer crime cases, however, international issues often pose a serious obstacle. The Internet is global and borderless, and that means evidence can be anywhere and wrongdoers can be anywhere. Investigators in one country do not have the inherent power to investigate cases in another country or to arrest suspects there. Instead, investigators generally must rely on the cooperation of law enforcement in the other country where the evidence or suspect may be located. The need for cooperation with any foreign country where the evidence or a suspect may be located greatly increases the complexity and difficulty of many computer crime investigations.

Question 2: Possession of SSNs

Someone who is merely found in possession of a Social Security Number (SSN) of another person without consent, without more, is not guilty of a crime. Further, I would not support creating a new crime of mere unauthorized possession of SSNs or login information of others.

There are two major problems with such a proposed offense. First, it is difficult to define what "unauthorized" possession actually means. For example, if I consent to giving my SSN to B, and B gives that number to C, is C in unauthorized possession? What if B work at the same company, or in a related company? It is difficult to know what possession is "authorized" and what is "unauthorized," making such a law very unclear.

Second, and relatedly, it is very easy and very common for a person to innocently possess numbers or information that just so happen to be the passwords or login information of another person. For example, imagine you decide that your new password will be my first name, "Orin." Because I have many documents in my possession that contain the name "Orin," your choice of password would mean that I am in possession of your password without your first voluntarily giving me your password. In such a case, I would not have acted culpably, and my conduct would not merit criminal punishment.

Question 3: Sending Messages to Credit Card Holders

No, I do not support such a requirement. The free market can best resolve this problem. If credit card holders want to be notified when their credit card has been charged, they can sign up for such a notification voluntarily. If credit card holders do not want to be so notified, however, the United States government should not force credit card issuers to provide notice that holders do not want and therefore that users will simply ignore.

○