S. HRG. 112–126

CYBER CRIME: UPDATING THE COMPUTER FRAUD AND ABUSE ACT TO PROTECT CYBER SPACE AND COMBAT EMERGING THREATS

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

SEPTEMBER 7, 2011

Serial No. J–112–38

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

70–751 PDF WASHINGTON : 2011

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

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin	CHUCK GRASSLEY, Iowa
DIANNE FEINSTEIN, California	ORRIN G. HATCH, Utah
CHUCK SCHUMER, New York	JON KYL, Arizona
DICK DURBIN, Illinois	JEFF SESSIONS, Alabama
SHELDON WHITEHOUSE, Rhode Island	LINDSEY GRAHAM, South Carolina
AMY KLOBUCHAR, Minnesota	JOHN CORNYN, Texas
AL FRANKEN, Minnesota	MICHAEL S. LEE, Utah
CHRISTOPHER A. COONS, Delaware	TOM COBURN, Oklahoma
RICHARD BLUMENTHAL, Connecticut	

BRUCE A. COHEN, *Chief Counsel and Staff Director*
KOLAN DAVIS, *Republican Chief Counsel and Staff Director*

VerDate Nov 24 2008 14:48 Oct 27, 2011 Jkt 070751 PO 00000 Frm 00002 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\70751.TXT SJUD1 PsN: CMORC

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

SUBMISSIONS FOR THE RECORD

CYBER CRIME: UPDATING THE COMPUTER FRAUD AND ABUSE ACT TO PROTECT CYBER SPACE AND COMBAT EMERGING THREATS

WEDNESDAY, SEPTEMBER 7, 2011

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 10:09 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Whitehouse, Klobuchar, Franken, Coons, Blumenthal, and Grassley.

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Chairman LEAHY. Good morning. Today the Committee is holding an important hearing on cyber crime. Protecting American consumers and businesses from cyber crime and other threats in cyber space has been a priority of this Committee for many years—I might say a bipartisan priority—and we continue that tradition today. Before we start, I want to thank Senator Grassley who has worked closely with me on this hearing in a bipartisan way. I think cyber crime impacts all of us, regardless of political party or ideology, so I look forward to our continued partnership, Chuck, in this Congress and as we continue.

Developing a comprehensive strategy for cyber security is one of the most pressing challenges facing our Nation today. I think of the days not many years ago when you worried about somebody going into a bank and robbing a bank and maybe getting $20,000—they were usually caught—or looting a warehouse. Now it is a lot different. A study released today by Symantec Corporation estimates the cost of cyber crime globally is $114 billion a year. In just the last few months, we have witnessed major data breaches at Sony, Epsilon, RSA, the International Monetary Fund, and Lockheed Martin—just to name a few. It is not the masked person with the gun walking into a bank. It is somebody maybe sitting thousands of miles, even another country away and committing the crime.

Our Government computer networks have not been spared. We saw the hacking incidents involving the United State Senate, and also the Central Intelligence Agency websites. We cannot ignore these threats. We cannot ignore the impact on our privacy and security. That is why the Committee will carefully examine the

Obama administration's proposals for new legal tools to help law enforcement investigate and prosecute cyber crime today.

I do want to thank and commend the dedicated men and women at the Departments of Justice and Homeland Security, and elsewhere across our Government, who are on the frontlines of the battle against cyber crime. Every day they are successfully investigating and disrupting the growing threats to our cyber security.

In July, the FBI announced that it had arrested more than a dozen individuals associated with a group of computer hackers called, obviously, "Anonymous" after the group launched a series of cyber attacks on Government and private networks, according to the charges made. The Secret Service recently announced a successful cyber crime investigation that led to the Federal indictment of an individual alleged to have hacked into the computer system at the Massachusetts Institute of Technology, MIT, resulting in the theft of more than 4 million scientific and academic articles. These are just two examples of the many accomplishments of our law enforcement community in this area.

But with every new victory, we are challenged by even greater threats and even more cunning cyber thieves. A recent report by the computer security firm Symantec found that on any given day, an average of 6,797 websites harbor malware, or other unwanted programs. That is an increase of slightly over 25 percent since June 2011. I am pleased that representatives from the Department of Justice and the Secret Service are here to share their views on this, and later this week the Committee will consider these proposals and other privacy measures in my comprehensive data privacy and security legislation. I hope that the Committee will promptly report this legislation on a bipartisan basis, as it has done three times before.

We are talking about the security of our Nation and our people in cyber space, so we have to work together. Again, this is not a Democratic or Republican issue. This is something that should unite us all. It is a national issue that we have to address, so I am hoping that all Members of Congress will join in that.

Again, I thank the distinguished Senator from Iowa for his help, and I yield to him.

STATEMENT OF HON. CHUCK GRASSLEY, A U.S. SENATOR FROM THE STATE OF IOWA

Senator GRASSLEY. Before I go to my statement, there are a couple things I would say.

I think the fact that Majority Leader Harry Reid had a meeting several months ago on various committees that were involved in this—and you and I were involved in that—plus the fact that in our party Senator McConnell has had hearings, I think that highlights the bipartisanship as well as the national security reasons for these pieces of legislation.

Also, the second thing I would say is that I think you have correctly stated that you and I are very, very close on this legislation, and I can say from the standpoint of this Committee's work, very close with the administration's legislation. I may have some ideas that vary a little bit, and I will refer to a couple of those in my remarks.

VerDate Nov 24 2008 14:48 Oct 27, 2011 Jkt 070751 PO 00000 Frm 00006 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\70751.TXT SJUD1 PsN: CMORC

I thank you very much for today's hearing. Given the growth of the Internet and our society's increased dependence on computer systems, this is a very important topic. Cyber criminals are no longer confined by the borders of their community, their State, or even their country. Cyber space has allowed criminals to steal money, steal personal identities, and commit espionage without even leaving their home. Cyber criminals are now using the Internet to conspire with other cyber criminals. They collaborate to install malicious software, commit network intrusions, and affect account takeovers.

Cyber criminals also target the point-of-sale computers at restaurants and retailers in order to steal millions of credit card numbers, as they did at companies such as TJX, BJ's Wholesale Club, Office Max, Boston Market, Sports Authority, and I suppose many others.

Moreover, there are online criminal forums that traffic in stolen credit card numbers, such as the notorious CarderPlanet forum that traffic in stolen credit card numbers. Cyber criminals also continue to engage in phishing attacks, denial-of-service attacks, and web application attacks.

Cyber criminals are smart, and they learn from their mistakes. They learn from evaluating other cyber attacks, and they learn from successful prosecution of their peers. Cyber criminals design relentless new computer viruses and malware as they attempt to stay one step ahead of the anti—virus programs.

All of these attacks are serious and dangerous to our Nation. However, I fear that the threats we have not heard about or even thought about are likely to be even more dangerous and devastating. So we must take these cyber attacks seriously and ensure that our critical system infrastructure is well protected from cyber criminals.

Accordingly, the Federal Government must take every single breach of a computer system or potential vulnerability seriously. For example, I have asked the Department of Defense Inspector General to properly investigate serious allegations that Department of Defense employees purchased child pornography online and were never adequately investigated by the Defense Criminal Investigative Service. These allegations include DOD employees possibly purchasing child pornography from their own work computers. I remain deeply concerned that DOD employees who purchased child pornography continue to work in key positions and retain high-level security clearances, putting the Federal Government and our military computer systems at risk for intrusion. I want to know what the Defense Department is doing to stop this sort of behavior, whether these individuals will be brought to justice, and whether Government systems could be compromised because of criminal behavior.

Aside from this example, I generally support the efforts that the administration is undertaking to work toward a bipartisan solution on cyber security. However, I have some concerns with part of the administration's proposal. I also have reservations about how these sweeping policies will be implemented and how much they add to an already large Government bureaucracy.

On top of these concerns, I also question the wisdom of the administration in some of the personnel appointments that they have made to critical positions. Example: The administration recently hired an individual at U.S. Cyber Command, an agency charged with securing our military capability network. I am concerned that the Obama administration seemingly failed to conduct an adequate background investigation of the individual's qualifications. If they had, I am confident they would have easily seen that she played a role in the Clinton administration's alleged loss of subpoenaed e-mail during the investigation of the 1996 Presidential campaign or that she allegedly paid a diploma mill thousands of dollars for a bachelor's, master's, and doctorate degree in computer science. Ensuring that our Nation's most sensitive networks are safe from international cyber espionage should not be assigned to someone who obtained their degrees from a diploma mill.

These types of personnel decisions weaken our ability to protect our Nation from cyber attack, essentially putting us at risk. Further, they raise questions about whether the administration is truly serious about protecting our Nation's critical infrastructure and military computer systems.

External threats continue to target our infrastructure, whether that is the financial services industry or retail. According to a recent data breach study conducted by the U.S. Secret Service and Verizon, 92 percent of the breaches were from "external agents." I appreciate that the Secret Service continues to aggressively combat worldwide financial and computer cyber crimes. In 2010, the Secret Service arrested more than 1,200 suspects for cyber crime violations involving over $500 million in actual fraud and prevented another $7 billion in potential loss. I plan to ask the Secret Service and the Department of Justice witnesses how we can improve our protection of cyber space. I am eager to understand how they are proactively engaging in emerging threats of cyber criminals, and I also want to know more about why they feel they need new criminal laws, new bureaucracies, and thousands of pages of regulations that could hamper virtually all businesses, large and small, across the country.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you very much.

Our first witness is James Baker. He is an Associate Deputy Attorney General at the U.S. Department of Justice. I know he was planning to be here once before for this hearing, and we had to cancel, and everybody's schedule changed. I told him earlier this morning that I am glad he is here, and the same with you, Mr. Martinez. He has worked extensively on all aspects of national security policy and investigations. As an official at the U.S. Department of Justice for nearly two decades, he has provided the United States intelligence community with legal and policy advice for many years. In 2006, he received the George H.W. Bush Award for Excellence in Counterterrorism. I would note that that is the CIA's highest award for counterterrorism achievement. He also taught at Harvard Law School and served as a resident fellow at Harvard University's Institute of Politics.

Mr. Baker, as always, it is good to have you here. Please go ahead, sir.

VerDate Nov 24 2008 14:48 Oct 27, 2011 Jkt 070751 PO 00000 Frm 00008 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\70751.TXT SJUD1 PsN: CMORC

STATEMENT OF JAMES A. BAKER, ASSOCIATE DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC

Mr. BAKER. Thank you, Senator. Chairman Leahy, Ranking Member Grassley, and members of the Committee, thank you for the opportunity to testify today on behalf of the Department of Justice regarding the administration's cyber legislation proposal.

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 potentially put lives at risk. Intruders have also stolen confidential information and 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. Even more alarming, these intrusions might be creating future access points through which criminal actors and others can compromise critical systems during times of crisis or for other nefarious purposes.

That is why the administration has developed what we believe is a pragmatic and focused legislative proposal for Congress to consider as it moves forward on cyber security legislation. We think that the proposal will make important contributions toward improving cyber security in a number of respects. Today I would like to take a moment to highlight the parts of the administration's proposal aimed at improving the tools that we have to fight computer crimes.

The administration's proposal includes a handful of changes to criminal laws aimed at better ensuring that computer crimes and cyber intrusions can be investigated and punished to the same extent as other similar criminal activity. Of particular note, the administration's proposal would clearly make it unlawful to damage or shut down a computer system that manages or controls a critical infrastructure, such as electricity distribution or the water supply.

This narrow, focused approach is intended to provide deterrence to this class of very serious, potentially life—threatening crimes. Moreover, because cyber crime has become 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. Also, the proposal would harmonize the sentences and penalties in the Computer Fraud and Abuse Act, or CFAA, with other similar laws.

For example, acts of wire fraud in the United States carry a maximum penalty of 20 years in prison, but violations of the CFAA involving very similar conduct carry a maximum of only 5 years. Such disparities make no sense.

In addition, the administration proposal would expand the scope of the CFAA's offense for trafficking in passwords to 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. Such language should also cover log-in credentials used to access any protected computer, not just Government systems or computers at financial institutions. The means to access computers at hospitals, nuclear power plants, and air traffic control towers are no less worthy of protection. 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.

The administration also proposes several amendments to the CFAA related to forfeiture, including adding a civil forfeiture provision. The lack of a civil forfeiture authority in the CFAA currently forces Federal prosecutors to use criminal forfeiture authorities in instances where civil forfeiture would be more appropriate or efficient. Our proposed civil forfeiture provision is consistent with similar provisions in Federal law that have existed for many decades.

Finally, 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 a service provider. We appreciate this view, but we are concerned that restricting the statute in this way would make it difficult or impossible to deter and address serious insider threats through prosecution. My written statement goes into this issue in more depth.

I would note that we have been working with Chairman Leahy, Ranking Member Grassley, and their staffs on a common solution to address this issue.

Mr. Chairman and members of the Committee, this is an important topic, as you all know. The country is at risk, and there is much work to be done to better protect critical infrastructure and improve our ability to stop computer crime. I look forward to answering your questions today, and I would ask that my full written statement be made part of the record of the hearing.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Baker appears as a submission for the record.]

Chairman LEAHY. Thank you, and your full statement will be part of the record. I appreciate the statement.

Next we will hear from Mr. Martinez. He serves as Deputy Special Agent in Charge of Cyber Operations for the Criminal Investigative Division of the United States Secret Service. In nearly two decades at the Secret Service, he oversaw the agency's first major cyber operation, Operation Firewall, in which over 30 online criminals from across the globe were apprehended. Incidentally, very impressive. He is currently responsible for the oversight of all cyber training and criminal intelligence operations conducted by the Criminal Investigative Division. Prior to that assignment, he supervised the New York Electronic Crimes Task Force, oversaw multiple transnational cyber fraud cases, again, pointing out that none of these things happen just in the locality where you are. He is a 1990 graduate of the Virginia Military Institute, where he received a Bachelor of Arts in economics, then a commission in the U.S. Army Reserves.

Please go ahead.

VerDate Nov 24 2008 14:48 Oct 27, 2011 Jkt 070751 PO 00000 Frm 00010 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\70751.TXT SJUD1 PsN: CMORC

STATEMENT OF PABLO A. MARTINEZ, DEPUTY SPECIAL AGENT IN CHARGE, CRIMINAL INVESTIGATIVE DIVISION, U.S. SECRET SERVICE, WASHINGTON, DC

Mr. MARTINEZ. Good morning, Chairman Leahy, Ranking Member Grassley, and distinguished members of the Committee. Thank you for the opportunity to participate in this morning's hearing.

One of the significant challenges in producing an analysis of the cyber criminal underground lies in the diversity of the online criminal community. For example, criminals may choose to cluster around a particular set of Internet relay chat channels, Internet-based chat rooms, or web-based forums. In some instances, a group of online criminals may come from a particular geographic area and may know each other in real life. In other instances, a group may be dispersed across the globe and know one another only through their online interaction.

Many venues are populated by those whose capabilities are unsophisticated; however, other more exclusive groups are comprised of members who have a decade or more of experience and extensive contacts in diverse criminal worlds. This diversity is reflected in the group's interests and aims. One group may see the researching of vulnerabilities and development of new exploits as a technical challenge fundamentally related to the basics of computer security. Another group may have little or no interest in underlying technological issues but will happily use exploits developed by others in order to intrude into third-party computer systems and harvest data of commercial value. Still other online criminal communities show even less interest in coding and exploits but use the Internet as an operating base, taking advantage of the anonymity and instantaneous communication the Internet affords them.

Two of the hallmarks that distinguish effective online criminal groups are organizational structure and access to a well-developed criminal infrastructure. One striking manifestation of these trends in online criminality is found in the web-based online forums that first began to emerge approximately a decade ago. In the early days, these online forums were established by hacking groups or by groups of carders, criminals who traffic in or exploit stolen financial data. Many of these forums have a strong representation of members from Eastern Europe. Although membership often spans the globe and includes members from multiple continents, by utilizing the built-in capabilities of the forum software, the people behind the organization are able to set up a system of foreign administrators and moderators who form the core of the organization and who maintain order at the site.

Some of these online forums developed into marketplaces for criminal goods and services. By 2004, forums such as DumpsMarket, CarderPortal, Shadowcrew, and CarderPlanet were already well-developed criminal marketplaces overseen by an experienced group of administrators who were often established criminals. In reality, these sites serve as a business platform for a fusion of criminal communities, each of which provides its own contribution to the development of the organization's capabilities by making a greater variety of reliable criminal services available to all members.

Some of the major classes of participants in these forums include the following broad categories: Carders, hackers, spammers, malware developers, and specialized hardware developers, to name just a few.

As evident from the array of criminal service providers I have just listed, the development of diverse online criminal organizations has greatly enhanced the criminal infrastructure available to pursue large-scale criminal activity. The far-reaching availability of a reliable criminal infrastructure in combination with other developments on the Internet presents a global challenge to law enforcement, which has found itself forced to adapt in order to apprehend and prosecute online criminals.

The administration is aware that in order to fully protect American citizens from cyber threats, certain sections of our current cyber security laws must be updated. This past spring, the administration released its proposal to address the cyber security needs of our country. The legislative package proposed by the administration addresses key improvements for law enforcement. Secret Service investigations have shown that complex and sophisticated electronic crimes are perpetrated by online criminals who organize in networks, often with defined roles in order to manage and perpetuate ongoing criminal enterprises dedicated to stealing commercial data and selling it for profit. The administration's proposal will better equip law enforcement agencies with additional tools to combat transnational cyber crime by enhancing penalties against criminals that attack critical infrastructure and by adding computer fraud as a predicate offense under the Racketeering Influenced Corrupt Organizations Act.

Chairman Leahy, Ranking Member Grassley, and distinguished members of the Committee, the Secret Service is committed to our mission of safeguarding the Nation's financial infrastructure and will continue to aggressively investigate cyber and computer-related crimes to protect American consumers and institutions from harm. This concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the Secret Service.

[The prepared statement of Mr. Martinez appears as a submission for the record.]

Chairman LEAHY. Well, thank you. And I assume you have no doubt in your mind these attacks are going to continue, no matter how many you have been able to stop in the past. Is that correct?

Mr. MARTINEZ. Yes.

Chairman LEAHY. Mr. Baker, like most Americans, I am concerned about the growing threat of cyber crime. If you have a business, you worry about that. If you are just an average citizen, you worry about somebody stealing your identity. I understand the FBI National White Collar Crime Center's Internet Crime Complaint Center received more than 300,000 complaints about cyber crime last year. That is an astounding number.

You discussed in your testimony the need to keep the Computer Fraud and Abuse Act up to date. How would the administration's proposals to update the Computer Fraud and Abuse Act ensure that the statute keeps us with the changes in technology?

Mr. BAKER. Well, in particular, on the question of keeping up with changes in technology, I would focus on the provision regard-

ing trafficking in passwords and other identifying information. Right now we think the language is broad enough to enable us to do what we need to do, but we think that expanding it to include other means of access to computers will clarify in the future, as hopefully security systems advance and other new technologies are developed to protect access, that this would be an easy way to make sure that we can actually get at defendants who we are able to bring to court and not have them escape on some technicality because a court thinks that the definition is not precise enough with respect to this new type of technology. So that is one example, Senator.

Chairman LEAHY. Well, I can imagine decades ago any predecessor of mine being in here talking about 'how do we get these bank robbers; how do we get these train robbers'. That is pretty simple. I have to assume that no matter how good a defense any one of the major companies have somebody is constantly trying to figure out a way to get around it. Is that not true?

Mr. BAKER. Yes, they are under constant assault. Yes, that is why I think you have the large number that you cited.

Chairman LEAHY. Now, one criticism of the Computer Fraud and Abuse Act is that the statute has been—this leads from your answer, it is interpreted so broadly that it could treat relatively innocuous behavior, violating terms of a service agreement, for example, as a Federal criminal offense.

What kind of assurances do we have if we pass this statute that either this administration or a future administration might abuse the authorities under the law?

Mr. BAKER. Well, certainly one thing is that we are accountable to this Committee and to the Congress in terms of how we enforce the Act, and we have to come up here and explain what it is that we have been doing. I think that if you look at our whole record with respect to how we have enforced the Act over time, I think we have done it in a responsible way.

I think we would be happy to work with the Committee under your leadership to try to find a way to address those concerns. There are perhaps a variety of different things, increased reporting requirements, for example, that might be effective, but we are certainly willing to work with you to make sure that this Committee believes that you have the right information to enable you to assess how it is that we are enforcing the Act.

Chairman LEAHY. You know what I am saying. In the normal criminal code, you could have some kid who takes a car joyriding and leaves it. You can charge him with some minor offense, or you can charge him with grand larceny. And most prosecutors would not charge him with grand larceny—we want you to concentrate on the real cyber crimes and not the minor things.

Mr. BAKER. Of course, we agree with that. We have limited resources. As you expressed, the threat is large, and we have resources but they are limited in terms of the number of people we are trying to——

Chairman LEAHY. Let us talk about that. How many investigators and prosecutors are there at the Department of Justice investigating and prosecuting cyber crime?

Mr. BAKER. In terms of prosecutors dedicated to cyber intrusions, if you will, there are approximately 230. Now, if you expand that to include other types of fraud, child exploitation-type crimes, it is going to be a larger number than that. I do not have that exact figure.

Chairman LEAHY. What about investigators?

Mr. BAKER. In terms of that, the difficulty is that the exact number of investigators that the FBI has in particular dedicated to this, because of the national security aspect of it, is classified. We would be happy to share that information with you in a different setting.

Chairman LEAHY. Perhaps in a different setting, if you could let both Senator Grassley and myself know.

Mr. BAKER. Absolutely.

Chairman LEAHY. Thank you. And do you have sufficient resources?

Mr. BAKER. I think we can always use more resources. We, the administration, put forward a proposal for fiscal year 2011 that included a request for some, I think, 160, approximately, additional personnel and some $45 million to go along with it. And the key is, I think, we want to make sure that we have the right resources. This is not something you just throw bodies at and solve it. You need to have trained people. You need to develop them over a period of time. So what we need to do is have sort of a long-term goal and objective in terms of bringing people in, training them, and then having them be able to work on these issues.

Chairman LEAHY. Well, the same question to you, Mr. Martinez. How many people do you have dedicated to this? And do you have adequate resources?

Mr. MARTINEZ. Chairman Leahy, we have put over 1,400 of our special agents through some type of computer training. We take cyber crime as a serious offense. We have been doing this for a while, so much so that part of the training that we now provide all of our special agents when they become agents is a specific 2- to 3-week block of cyber training. So it has now become part of our basic training for every special agent that goes through the academy.

In addition to that, with the assistance of the Committee, we now have 31 Electronic Crime Task Forces throughout the country, 29 of them domestically and 2 overseas. And what we have done with that, in addition to the special agents that we have that have cyber training, we have also partnered with our State and local law enforcement officers throughout these task forces and provided them with this training. We do that training through the National Computer Forensic Institute down in Hoover, Alabama, where we only train State and local law enforcement on computer forensics, network intrusion, and in basic skills of computers.

Those individuals, when they leave the NCFI, are then either members of our Electronic Crime Task Forces throughout the country or are providing assistance and support to State and local municipalities throughout the country. We are proud to say that we have had State and local law enforcement from all 50 States of the Union and 2 of its territories. And in addition to having the State and locals train there, we also train State judges and State prosecutors because we feel as important as it is to train our investiga-

tors, it is that important to also train prosecutors and judges so that these cases get prosecuted and so that judges know how to prosecute these cases.

The other thing we have taken with the Electronic Crime Task Force model is that we have partnered with academic institutions, because a good amount of the research and development that goes on in this country is done by universities. So for the last 12 years, we have been at Carnegie Mellon University and have been a member of the Software Engineering Institute where we work with Carnegie Mellon NCI, which is a federally funded research and development center, to develop software and hardware that helps our investigators.

In addition to that facility, we have also partnered with the University of Tulsa where we have a cell phone/PDA forensic facility to also boost the capabilities of our agents and our State and local partners.

Chairman LEAHY. Thank you very much. I know my little State of Vermont has had people down there, so I appreciate that.

Senator Grassley.

Senator GRASSLEY. I want to zero in on cyber attacks on our infrastructure, like power grids, traffic control. These things, where they can be interfered with, control most of our important day-to-day operations. As such, our criminal laws should reflect the need to protect critical infrastructure by sending a signal to would-be criminals that these attacks, including even attempted attacks, will not be tolerated. That means not only criminalizing the conduct but including tough sentences that Federal judges cannot play games with. So, Mr. Baker, I would like to ask you questions along this line.

The administration's cyber security proposal includes a new crime for aggravated damage to a critical infrastructure computer. This proposal includes a 3-year mandatory minimum prison sentence for those who knowingly cause or attempt to cause damage to a critical infrastructure computer. Why did the administration include this mandatory minimum for this crime but not other crimes?

Mr. BAKER. Because we understand the concerns that some Members of Congress have with respect to the use of mandatory minimums, we believe that it was appropriate in this circumstance, given, as you just recited, that it is involving damage to critical infrastructure systems that result in the substantial impairment of the system, so we thought that under those circumstances, given the gravity of the offense, that a mandatory minimum of 3 years was appropriate in this circumstance, and we thought it was a judicious use of the mandatory minimum concept, which is why we attached it to this particular offense.

Senator GRASSLEY. We are scheduled to mark up a Senate bill that does not currently include a crime for aggravated damages to a critical infrastructure computer. It is my understanding that may be added at markup. However, I understand it may not include a mandatory minimum. Would the Department support including a mandatory minimum, as the President's proposal does, as part of the Committee process?

Mr. BAKER. The administration's proposal is to include a mandatory minimum. Obviously, we want to work with Congress in this area. We understand the concerns, and so we are happy to work with the Committee. But we do think that this prohibition, this new criminal offense, is something that we do need to address and try to include.

Senator GRASSLEY. Okay. This would be for Mr. Martinez. As I stated in my opening remarks, I believe that we must take cyber attacks seriously and ensure that our critical systems' infrastructure is well protected from cyber criminals. However, I am concerned that we provide too broad of a definition for things like "sensitive personal identifiable information," that we may desensitize that information and create complacency within the public. Individuals that constantly receive data breach notifications from their banks will begin to maybe ignore them. A broad definition of "sensitive personal identifiable information" could also overburden businesses by requiring them to make unnecessary notification for what amounts to public information that is easily obtainable through Internet searches.

So how does the Secret Service define "sensitive personally identifiable information"?

Mr. MARTINEZ. Senator Grassley, we identify it the same way that it is laid out in the administration's bill and also as it appears on the 1028(d)(7). I think what we also need to take into account is when we look at what constitutes a data breach, it includes the information you are referring to, but it also includes Section (b) which states, "which present a significant risk of harm or fraud to any individual." So that is taken into account along with the definition of "personally sensitive identifiable information" in order to make notification.

The other way I think we address it also is through triggers. I think there are triggers in the bill that define when notification needs to be made and when it does not.

In reference to the broad definition of "personally sensitive identifiable information," I will tell you that there are individuals in the online criminal community that can take that general information and put it together with additional information that they have already compromised to give you a better idea as to the information involving your victim target. So, for example, I could take the first initial and last name of an individual, his home address, and provide it to one of these online criminal data brokers and say, "Can you run a credit report on an individual at this address with this first initial and last name"? So that combined information can then really cause harm to the victim.

Senator GRASSLEY. Well, if banks send their customers breach notification that involves nothing more than their name address, or their mother's maiden name, do you agree that this broad definition of "sensitive personally identifiable information" could potentially desensitize the public perception and maybe create a "boy who cried wolf" situation?

Mr. MARTINEZ. There is a possibility that something like that could happen, and that is why, again, I go back to the administration's proposal that talks about significant risk of harm or fraud. I think the organization, the company, needs to take that into ac-

count, you know, before we start desensitizing these intrusions by sending too many of these notices.

Senator GRASSLEY. Well, if you would support narrowing the definition of that term to cover information that leads to a significant risk of identity theft, how would you narrow the definition?

Mr. MARTINEZ. I believe in the definition or in that area, as it is submitted as part of the administration's proposal, it talks about combining the PSII information with the second part of it, which is, "which presents a significant risk of harm or fraud to that individual." I would add that section to the bill as it is laid out in the administration's proposal.

Senator GRASSLEY. And, last, if Congress were to give rulemaking authority to modify the definition in the future, what agency or combination of agencies would you suggest be given that authority?

Mr. MARTINEZ. I believe the FTC and I think also in consultation with the Department of Justice, because the Department of Justice is responsible for prosecuting these cases, so I definitely think that the FTC has the expertise in this area, and I think consultation with the Department of Justice would also be good.

Senator GRASSLEY. Thank you, Mr. Chairman.

Chairman LEAHY. Well, thank you. And, incidentally, Mr. Baker, I think the House of Representatives would find it very difficult to accept the mandatory minimum, and certainly I do not intend to include it in the bill that I will put forward. Just in passing, I want strong penalties, but the mandatory minimum is something that I worry can be abused.

Senator Coons.

Senator COONS. Thank you, Mr. Chairman.

I want to start by thanking the Chairman and the Ranking Minority for convening this hearing. I think we have heard from the Chairman, from the President, and from many leaders in the private sector and public sector that this is one of the most grave threats facing our Nation, that the number and complexity of cyber crimes continues to grow year after year and the cost and the impact on victims large and small continues to grow. So I am glad we are continuing to press on this. I hope that the Senate will, indeed, take the opportunity to move in a bipartisan and responsible way to reconsider the CFAA, to amend it in ways that deal with overbreadth or last of clarity but to, frankly, also strengthen the tools available to law enforcement.

I want to focus on just a few simple points, if I could. One is about training and the skill set that is available, both in the Department of Justice and in the Secret Service. Mr. Martinez, Special Agent Martinez, I was struck in your written report about the scope of training available, the 1,400 agents having gone through ECSAP training, the 31 ECTFs you referred to, the institute in Alabama that I know Delaware law enforcement has benefited from as well as many other States, I think all States. But I am concerned about the depth of training and the breadth of it.

There was an Inspector General report from the Department of Justice just in April of this year that suggested that the National Cyber Investigative Joint Task Force, actually a third of the agents engaged lacked the necessary expertise in networking and counter-

VerDate Nov 24 2008 14:48 Oct 27, 2011 Jkt 070751 PO 00000 Frm 00017 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\70751.TXT SJUD1 PsN: CMORC

intelligence to be able to effectively participate in intrusion cases, and that many of the field offices also lacked the forensic and analytical capability. I am clear that training is expense, that we have lots of other things on our needs list for the country, but this is not a want that strikes me as a critical need. I would be interested in comments from both of you, if I might, about what more we can and should be doing to strengthen the training, the depth and breadth of training by law enforcement.

And then as a follow-on to that, if I might, Special Agent Martinez, you have, I think, a reserve commission. In Delaware we have a National Guard unit that takes advantage of a lot of the private sector strength and skills in our financial services community to also bring them into training and make them available as a resource. I wondered if both of you might comment on the possibilities or the risks of engaging the National Guard and the Reserve as a way to get some of the most skilled private sector folks also engaged in some of the national security-relevant pieces of ongoing forensic and network defense and investigations. If you might, please, first.

Mr. MARTINEZ. Thank you, Senator. Yes, it is an expensive undertaking to get these folks trained, and that is why we have tried to force multiply, working with our partners. Cyber crime is not something that can be solved by any one organization. We all have to work in a collaborative way to do that. And we think we are—that is what we have been trying to do with our task forces, and not only partnering with State and local law enforcement and other Federal partners, but also bringing the private sector in.

There is a section of the administration's proposal which actually talks about having folks from the private sector come in to assist Government and so forth. So there is probably some mechanism that is already been used in other parts of the Government that can be used to help here.

One of the other issues that we see from cyber crime is that we have a lot of involvement from Eurasian cyber criminal organizations or some of the most robust organizations. In speaking about the National Guard, there is potentially something we should probably look into that is similar to some of the activities that other Department of Justice organizations, law enforcement organizations have done in the past with the assistance of some National Guard entities in other parts of the country, and specifically in the area of linguistic capabilities. You know, that is one of our biggest challenges, is the fact that a lot of these criminals are Eastern European and speak Russian or a Russian dialect. There is probably a way to get that same model that we set up in narcotics enforcement for language translations and have that sort of supplement what we do in cyber crime because these individuals primarily communicate through some type of online method, whether it is instant message, e-mail, or peer-to-peer, and so there probably would be a good venue to get that type of linguistic capability up to speed and utilize it in furtherance of cyber crime investigations.

Senator COONS. Thank you. I would be happy to work with you, if I can, in furthering that. And if you might, Associate Deputy Attorney General Baker, please.

Mr. BAKER. Sure, just a couple quick comments to amplify on that.

I think with respect to the use of the National Guard, I agree. We need to use all of our available resources. The key there is to make sure we understand what hat they are wearing when they are engaged in that role and to make sure that what they are doing is consistent with the law and executive branch policy, and then to make sure that we have appropriate privacy protections in place and appropriate oversight to make sure when any element of DOD, assuming they are acting in that capacity and in that way, is engaged in these kinds of activities. But I agree with your general point that we need to make sure that we have the resources—that we use all the resources that are available, especially if these people are coming with particular skill sets that they have developed in the private sector. That is absolutely critical.

Just real quickly on the IG report with respect to the FBI, I would just note that the FBI, it was my understanding, accepted all the recommendations from the IG, so they understand it. They place a huge amount of importance on this, and they get it as well.

Senator COONS. Great. Thank you. As we try to move responsibly to strengthen law enforcement's toolkit, I also want to make sure that we are striking the right balance, as you mentioned, between privacy and continuing to be certain that there are robust divisions between DOD authority and domestic law enforcement, and that we are respecting the rights of Americans and protecting individual liberties.

Thank you for your answers.

Senator WHITEHOUSE [presiding]. I will be chairing the remainder of the hearing, so that means I will be here until the end. So to expedite my colleagues, let me defer my questioning until the end, and so unless a Republican colleague arrives, we will have Senator Klobuchar, then Senator Franken, then Senator Blumenthal. Senator Klobuchar.

Senator KLOBUCHAR. Thank you very much, Mr. Chair, and thank you to both of you for working on this very difficult and important area. I am glad that we are holding this hearing, obviously, but also that we are moving ahead on legislation, because I have heard time and time again, whether it is confidential briefings with our Defense Secretary and others about the concern of the cyber attack issue—and I certainly have seen in a much smaller way in my previous job a prosecutor for 8 years just the growing, escalating number of cases that we had involving just individuals being hacked or data stolen. And I have introduced a number of bills in this area, and I wanted to talk through some of those and how they could work with the larger bill that we are working on.

Senator Hatch and I introduced a bill aimed at child pornography that would require Internet service providers to retain information on the IP addresses they assign to customers for a minimum amount of time. This is information that the providers already have and already retain, but some providers, we have learned, keep it for longer periods than others, and the bill would simply set a minimum retention period. The providers would not be required to retain any content of a person's online activity. It simply mean that if law enforcement sees illegal activity online,

then they can tell that it is emanating from a certain computer or device. They would then be able to go to the Internet service provider and get information on who owned that computer or device, and, of course, they would need a subpoena to do that.

It seems to me that this could be an important reform not just for child pornography cases but also for many of the types of crimes that we have been talking about today. I do not know if either of you would like to comment on that. Mr. Baker.

Mr. BAKER. Yes, thank you, Senator. Just briefly, we agree completely that this is a significant issue and it potentially impacts a whole range of cases, including child exploitation, gangs, other types of—you know, terrorism potentially, national security crime. So we think it is a significant problem.

We do not, unfortunately, have a cleared administration position on how long and what types of data to retain and so on, but I agree with your characterization of the basic idea with respect to the proposals that we have seen. It is certainly something we would like to work with you on because it is a very, very important issue.

Senator KLOBUCHAR. Agent Martinez.

Mr. MARTINEZ. Yes, Senator. Digital crime scenes tend to evaporate more quickly than traditional crime scenes, so preserving data is an important part of any type of cyber investigation. So we concur with Mr. Baker's comments that, you know, some type of retention would be good to cyber investigations.

Senator KLOBUCHAR. Then another area is cloud computing, and I think we are seeing more and more of that, for good reasons: bringing down the cost of data storage, computing for businesses, consumers, and government alike. However, we need to also ensure that our laws are keeping up with the new technology. Cloud computing represents a unique challenge. The way the data is stored and accessed in the cloud makes it sometimes hard to prove the damages that are currently required by the Computer Fraud and Abuse Act. And so we are looking at how we can make sure that those damages can be proved when you are dealing with the cloud, and I do not know if you want to comment at all about that and what is happening with hacking.

Mr. MARTINEZ. Again, I go back to the crime scene. A cloud crime scene is much more difficult to solve than to try to get evidence from a traditional crime scene. So it is going to be a challenge to make sure that when we respond to an organization that is storing information in the cloud, that that organization knows exactly where that information is at and, you know, make sure that law enforcement can access that information in a quick manner.

I go back to, you know, the fact that digital evidence evaporates a lot quicker, so it is going to be incumbent on organizations that establish some type of cloud computing environment that they know the layout or the topography of their information. And the other challenge that we also face is, you know, if the information is stored in the cloud and that cloud is out of the jurisdiction of the United States, what challenges might that pose to us?

Senator KLOBUCHAR. And that is why we are trying to put in here some structure for other countries to work together on these things, because that is going to be key as we move forward.

Shifting to another topic, do you think the jail terms and the fines in the current law are severe enough to have a substantial effect in deterring or reducing cyber attacks? And how about in the proposal before us?

Mr. MARTINEZ. I think the administration's proposal does a very good job of addressing that. And, in fact, I used some examples where we have charged cyber criminals with other offenses as identified by Mr. Baker, where these individuals were charged with either wire fraud or credit card fraud or bank fraud that received significant jail terms, in excess of 10, 15, 20 years. That is definitely a deterrent to criminals that conduct this type of activity.

If you look at our Verizon data breach investigative report, we see a larger number of intrusions occurring right now, but we do not see as many of the large-scale intrusions that we have seen in the past. We think part of the reason for that is the deterrent factor that these stiff sentences have had on these criminal organizations. So to get a statute like 1030, the Computer Fraud and Abuse Act, up to par with some of these other ones we believe will make a deterrent against criminals that are undertaking these types of intrusions.

Senator KLOBUCHAR. Okay. Then just one last question, Mr. Chair, if I could. Economic espionage is clearly a drain on the American investment in our country, our talent, whether it is blueprints to the way a manufacturing facility is set up or a design of a dress. Does, do you believe, the Computer Fraud and Abuse Act adequately combat the problem of economic espionage? And do you think the administration proposals helps with this? Are there more things that we should be doing as we look even away from the cyber attacks on Government and look into what has been going on in the private sector?

Mr. MARTINEZ. I think Mr. Baker could better answer that than I.

Senator KLOBUCHAR. Mr. Baker.

Mr. BAKER. Absolutely. I mean, the focus of the Computer Fraud and Abuse Act is sort of on the means that are used to perpetrate the crime that I think you are talking about. We would fully support efforts to try to make sure that we can address the type of crime that you are concerned about because we are very concerned about it as well. I think that our proposals in the administration's legislation would be effective in addressing the type of crime. But if there were particular things that we should focus on, we would be happy to work with you on that because it is a huge problem, and the theft of our intellectual property is a very, very significant problem for the country.

Senator KLOBUCHAR. Have you seen instances of retaliatory hacking where groups actually go after people that are working on this, these issues?

Mr. BAKER. Groups go after a lot of different people working on a whole range of issues, and, you know, I guess I would defer to Special Agent Martinez on the cases because—well.

Mr. MARTINEZ. Yes, I think no one is immune from these types of intrusions and attacks. I think we have seen a lot of these types of attacks have been reported in the media, and there is a lot that

happen. So I do not think anybody is immune from this type of cyber attack.

Senator KLOBUCHAR. Thank you very much.

Senator WHITEHOUSE. Senator Franken.

Senator FRANKEN. Thank you, Mr. Chairman.

Mr. Baker, I want to ask you a question to follow up on a question from Chairman Leahy. In recent cases the Department of Justice has actually argued that the violation of a website's term of service or an employer's computer use policy can constitute a Federal crime under the Computer Fraud and Abuse Act. In other words, under this interpretation of the statute, people could conceivably be guilty of a Federal crime for checking their gmail or the weather if their employer's computer policy prohibits them from using their computers for personal reasons. Two Federal judges have found this reading of the statute to be unconstitutional because people do not read those policies, and when they do, they can be, as you know, long and complex and full of fine print.

Don't you think it would be worthwhile to somehow address the concerns of those Federal judges in updating this statute?

Mr. BAKER. Thank you for that question. As I said earlier, Senator, we would be happy to work with folks to address these kinds of concerns. I think that the challenge is to address those concerns and at the same time not create a significant loophole that would allow somebody, for example, who worked at the Social Security Administration, the IRS, the U.S. passport office, or a bank to take information in violation of their employer's policies and misuse it for some purpose, either to spy on somebody that they know or to take information and pass it others to actually steal money. So I think this insider case where somebody violates the rules of their employer using a computer is a very challenging thing to address and at the same time address the types of concerns that you suggest.

The difficulty is that, you know, we have to think about how and whether we should have a regime that is parallel to the actual physical world. So if an employer says, "Well, you can use the petty cash for certain purposes but not for other purposes," and somebody takes the cash and spends it on something that they are not supposed to, we would prosecute them, potentially, depending upon the amount, for fraud. And so the question is or the issue is employers all the time set rules about what can be done with their resources. Do we want to make a difference—or how do we want to differentiate the cyber world from the physical world? So I think these are real challenges, but we understand what you are saying, and obviously we have read those opinions, and we have heard loud and clear what the judges were saying, and in the Drew case, in particular, we decided not to appeal in that case.

Senator FRANKEN. Okay. Thank you.

Again, Mr. Baker, I know that this is not technically the subject of the hearing, but since you are here, I want to ask you about the administration's data breach proposal. The administration's proposal would require certain companies holding "sensitive personally identifiable information" to notify their customers if that information is breached. I was surprised to see that the administration's definition of "sensitive personally identifiable information" did not

include an individual's geolocation. Today many companies literally have minute-to-minute records of everywhere a smartphone user has been over a period of months. In my mind, that information can be just as sensitive, if not more sensitive, than one's home address, which is covered under the definition.

Would you consider amending your proposal to include geolocation in the definition of "sensitive personally identifiable information"?

Mr. BAKER. I think certainly, Senator, we would be open to looking at that issue. I would have to look at it again. There may be parts of this that would cover that type of information, depending on how it was stored in an account or something already. But in terms of focusing on it directly, I think we would be open to that.

I would just note that, because we looked at the geolocation question in a variety of different contexts, defining geolocation information is tricky, and so we would have to make sure that we got that right in order to include the kinds of things that you are concerned about but not sweep in a bunch of other stuff. But I would be happy to work with you on that, or the Department would be happy to work with you on that.

Senator FRANKEN. Good. Thank you.

I also noticed that this proposal gives companies up to 60 days to notify their customers of a breach of their sensitive personally identifiable information. That period seems long to me. A criminal can do a lot of damage with someone's Social Security number in 2 months. Why can't we have a quicker deadline or shorter deadline for notification?

Mr. BAKER. I think on that as well, Senator, we would be happy to work with you on that, because the one thing to think about, though, is there is invariably some lag time, because there will be a breach and it might take a short period of time for the company to become aware of it. And then I think you want some period of time where the company is required to go to law enforcement and law enforcement can make some assessment about whether we want them to report. We may have an undercover operation ongoing, let us say, to try to target these people. They have been doing a variety of different breaches, and so we have an operation. We do not want them to know that we are on to them. So we may in a particular circumstance ask the company to hold off on the notification because it might harm——

Senator FRANKEN. Okay.

Mr. BAKER. So we want some period of lag time. The trick is to find out what that is, and so I think we would be happy to work with you on that. I do not think there is any magic with respect to the 60-day number.

Senator FRANKEN. Okay. It looks like we have got a lot of little things to work on.

Mr. BAKER. Sure.

Senator FRANKEN. Okay. Thank you, Mr. Baker.

Mr. BAKER. Okay.

Senator FRANKEN. Thank you, Mr. Chairman.

Senator WHITEHOUSE. Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Mr. Chairman, and thank you both for being here today. I want to second the concerns just raised

by Senator Franken about the 60-day period, which I think is way too long in the majority of instances. I recognize there may be some law enforcement activity that requires some lag time, but it seems to me that an exception can be carved out for that kind of specific—and I do mean explicit and specific—law enforcement activity that justifies a delay rather than having a blanket 60-day period, which seems excessively long.

I want to focus—and I was very interested and impressed by your comments on infrastructure vulnerability and potential assaults on that aspect of our economic and security activity. We hear a lot of talk about potential cyber assaults on our information, whether it is electric or gas. Should there be a stronger requirement for those facilities or companies themselves to take proactive and preventive measures? Right now it seems to me if there are any provisions, they are egregiously weak in light of the public responsibility of those private institutions. And so I wonder whether you would care to comment on that.

Mr. BAKER. Yes, Senator, thank you. I think that is addressed in other parts of the bill where the role of the Department of Homeland Security with respect to helping to set standards and then monitoring compliance with standards, I think that is more directed at the kind of concern, very legitimate and absolutely correct concern that you have with respect to that. I am not sure—I would have to think about it for a minute, but I am not sure that the specific proposal we are talking about with respect to the CFAA, for example, would address that. But I think that the larger concern about the critical infrastructure—and, you know, again, the whole point of all this is to prevent anything from happening. It is one thing to prosecute after the fact, but we want to prevent things from happening. We want to deter activity, and we want to make sure that entities have in place the appropriate means to protect themselves and the incentives to do that.

I think we would be happy to work with you on any way that is reasonable that would further those goals.

Senator BLUMENTHAL. And I agree, deterrence is one way to prevent criminal activity, but not always an effective way in light of the interests and stakes. And you mentioned extortion. A potential penalty of 3 years, even if it is a minimum, may not be enough to deter someone from this kind of——

Mr. BAKER. That is right.

Senator BLUMENTHAL. Do other parts of your—meaning the Federal Government's—proposals include penalties, whether civil or criminal, for the failure of these infrastructure institutions to take preventive measures?

Mr. BAKER. They do not include criminal prohibitions or penalties for failing to take these types of measures. I think the idea was to have a lighter touch with respect to building incentives into the system to try to get entities to enhance their cyber security. So I do not think that that is part of the proposal.

Senator BLUMENTHAL. What about civil penalties?

Mr. BAKER. The same thing. I think the idea is not to incur civil penalties, but to provide appropriate information and disclosures with respect to the state of affairs with respect to particular entities.

Senator BLUMENTHAL. Because that really is the thrust of my question to you, whether there should be—taking a broader view, I recognize it is Homeland Security, not the Department of Justice, but if there is no effective remedy for the failure to take such measures, I wonder how effective the standards and advice and counseling will really be, given the economic pressures that these companies may have and given their relative lack of sophistication in this area. Financial institutions are much more likely to be deep into this subject because of the nature of what they do. Their entire business is conducted with computers, and so they are familiar with making those computers less—and more so the other infrastructure every day where smart energy use involves this kind of work. But I guess my point to you is that I think that we do need to consider some kind of stick as well as carrot in this area.

Mr. BAKER. I agree, Senator, and I think there are existing incentives that some folks have just not focused on, I think. For example, there is a loss of good will with your customers when you face a serious breach. That is one thing. You are losing money. You are losing your intellectual property. You have obligations to your shareholders to inform them about the state of affairs with respect to your company. That may be something that the SEC is looking at—or should look at, I guess. Others have suggested that. Senator Whitehouse, in fact, I think suggested that with perhaps Senator Rockefeller.

And so there are a whole range of different incentives built into the system today that I guess you would have to say do not seem to be effective because we still have a very significant problem that we need to address, as you have suggested.

Senator BLUMENTHAL. And my time has expired, but again I want to thank you, and I would just suggest that if we are that concerned about the information vulnerability, maybe those incentives are not working as well as they should.

Thank you.

Senator WHITEHOUSE. Mr. Baker, welcome back.

Mr. BAKER. Thank you, Senator.

Senator WHITEHOUSE. A quick question. Is it clear that the cloud is a computer within the meaning of the statute?

Mr. BAKER. The current statute? Well, I think that the elements of the cloud are. I would have to look at it. I can pull out the definition of a "protected computer." But I would think that because it generally includes any computer connected to the Internet, the cloud itself at a particular cloud provider is going to be included within the definition of a "protected computer."

Senator WHITEHOUSE. When was the statute, 2008?

Mr. BAKER. Yes, I think that is right.

Senator WHITEHOUSE. So that is, believe it or not, in cyber time a generation or so, and it kind of dates back to when it was presumed that data was actually in a computer. And since that is no longer the way this works, I just wonder that you may find that you run into definitional problems, particularly if criminal statutes are intended to be narrowly construed. Anyway——

Mr. BAKER. I agree with that, and as I think I suggested, if we expand anything with respect to something called "the cloud," we need to make sure that we define that appropriately.

Senator WHITEHOUSE. Where do you think your defendants are most likely to be under this provision of law?

Mr. BAKER. We face substantial threats—and I will defer to Special Agent Martinez on this as well, but we face substantial threats from domestic actors, domestic malicious actors, as well as international. So, as you know very well, there is a very substantial threat that we face from actors based overseas.

Senator WHITEHOUSE. Yes, and it worries me to go back to Chairman Leahy's question. You said that there are 230 prosecutors who are working in this area. Where do you get the 230 number? Does that include the people assigned to the United States Attorney's Offices who are the designated cyber prosecutors?

Mr. BAKER. Yes. That includes those people plus folks at Main Justice who are dedicated to this type of activity. Again, it does not include necessarily the fraud prosecutors, the child exploitation prosecutors, because they are dealing with criminal activity on the Net as well.

Senator WHITEHOUSE. So you and I both know that out in the United States Attorney's Offices the designated cyber prosecutors are doing other stuff.

Mr. BAKER. Absolutely.

Senator WHITEHOUSE. So the number in terms of FTE, or whatever you would want to call it, is actually considerably less than 230. Because these cases very often involve overseas activity, you have added a RICO predicate here, which I think is great. But RICO cases are complicated. I do not know to what extent the Department requires departmental oversight of this. If you do, for instance, a public corruption case and you are a U.S. Attorney, you have to check in with the Department all the time on that, and it adds a lot of work and effort and burden to the case, probably with good reason. How closely does the Department supervise and require engagement with a U.S. Attorney's Office that is prosecuting a cyber case? If you are doing a Hobbs Act case, you are kind of on your own. The Department really barely ever checks in if you are doing a—where on the spectrum is this in terms of the Department requiring a lot of back-and-forth with the U.S. Attorney's Office?

Mr. BAKER. Just a quick comment on the RICO case. If adopted by the Congress, the RICO provision would be subject to the same type of oversight by the Department, so just to make sure that is clear.

With respect to existing criminal activities with respect to cyber crimes, there is a range. Some U.S. Attorney's Offices have a significant number of trained prosecutors who know how to do this. You know, they are in large offices, and so they consult with Main Justice as needed. Other districts where they do not encounter this type of activity as much or do not prosecute the cases as much, they are going to rely more extensively on our computer fraud——

Senator WHITEHOUSE. So if a U.S. Attorney's Office has the internal capability to handle a significant cyber case, they can run with it on their own without a lot of supervision by Main Justice?

Mr. BAKER. That is essentially correct, I think, yes.

Senator WHITEHOUSE. Well, that lifts at least one burden off of this, but still, when you divide the 230 down for the extent to

which those are people who are actually doing something different, and when you look at the complexity of RICO cases of chasing people down internationally, probably having to coordinate with our intelligence services to get information about the foreign bad actors, I just continue to worry that we are sorely, sorely understaffed for this.

How would you evaluate, how does the Department evaluate the risk of a cyber attack on the country and the constant regular day-to-day onslaught of cyber attacks in the Nation's priorities?

Mr. BAKER. In the Nation's priorities, I mean, I think that the threat of a cyber attack or addressing the threat of a cyber attack is very high on the list of priorities for the Nation, not only for the Department of Justice but for the entire Defense Department, the intelligence community, and all elements of Government. We are very, very concerned about that kind of thing. So it is very high on the list of priorities.

Senator WHITEHOUSE. And just day to day, there are tens of thousands of attacks. We are having a hemorrhage of our intellectual property, mostly over to China, but to other places. There is an immense amount of crime and fraud that takes place, and that is kind of the baseline. If you put the baseline together with the risk of a really significant knock-down cyber attack on the country, doesn't that equate in terms of risk to national security of, for instance, our exposure to drug crime or our exposure to the hazard of alcohol, tobacco, firearms, and explosives?

Mr. BAKER. As you know, there is a huge problem with many elements to it. We have to address all of them basically simultaneously because there is an onslaught of attacks, as you have described, every day. "Attacks"? Let me back up. There is an onslaught and intrusions and computer activity, malicious activity all the time. Whether something is an attack or not, let us put that aside for a second.

Senator WHITEHOUSE. Yes, understood.

Mr. BAKER. Let me back up 1 second. It is important to make sure that we have adequate resources to deal with these crimes and these activities. It is also important that we make sure we have in place, when we catch someone, the appropriate penalties, the appropriate language in various statutes to make sure that somebody does not get out on a technicality and things like that. So what I think we are focused on today, at least in my comments, on the CFAA is to make sure that we have the statutory structure to address the crime. What we need to do then is go after the criminals, and we need to have all the kinds of resources that we have been talking about today, the Secret Service, the FBI, and that other elements of the Government have.

Senator WHITEHOUSE. I understand that. I am just worried that we are going to pass this bill as it ends up being amended, that it will go into effect, and we are going to pat ourselves on the back for having done something good about protecting America from cyber crime and from cyber attack, and, in fact, what we have done is overlooked the resource disadvantage that we have put ourselves at.

Mr. BAKER. Well, I agree completely. When you look at how the Nation has faced the threat from counterterrorism since 9/11, we

have not just done one piece. We have done a whole range of things since then, and we need to dedicate ourselves to that kind of effort for a prolonged period of time in terms of dealing with this cyber threat. It is going to evolve over time. The adversaries have significant resources themselves devoted to it, and we face substantial risks if they are successful.

Senator WHITEHOUSE. When DNI Clapper had his confirmation hearing in the Intelligence Committee, he listed the threats to America's national security. The No. 1 was cyber.

I wanted to just follow up quickly on the question that I think Senator Franken asked, and I think Chairman Leahy did also, about violating the terms of a service agreement and criminalizing basically contracts with—violations of contracts with your provider. When you were asked that question, you responded with an example of somebody who was stealing large amounts of petty cash. I would just suggest to you that there is a difference between stealing petty cash, which I think every American understands that stealing cash is a bad thing to do, with violating the terms of fine print in contracts. I do not think there has ever been a society more bedeviled by fine print in contracts than America is right now. The average American has so much fine print in all of the computer programs they download, in all of their service agreements, in the cell phone contract. I mean, wherever you look, everything you do with the bank has pages, your credit card agreement is probably 20 pages long of fine print. Americans are absolutely tormented with fine print. And I do think that it would be very salutary for the Department of Justice to put out a proper, solid prosecution policy that would reassure Americans that it is not the Department of Justice's intention in pursuing these criminal offenses to go after somebody who comes in under the wrong name on Facebook or who, you know, one way or another is out of compliance with a private contract that they have entered into that is probably a contract of adhesion more or less in the sense that they did not really negotiate it and it is multiple pages long and the average person does not even read it.

I think you want to be out of that business, and I think the cases that raise that question really throw the Department's prosecution in this area, its activities in this area in a pretty bad light. They have had a lot of attention today. It is attention that I do not think you need, and I think there is a clear difference between going after somebody who goes into the petty cash drawer and takes money out, which everybody knows is wrong, and somebody who sends an unauthorized e-mail or accesses a program that they are not supposed to. I just think you need to be a lot more careful about that and make sure you are going after who you should be, and that I think will calm down a lot of the concern about this, because it really does lend itself to abuse if it becomes a Federal crime to violate the fine print of all the innumerable contracts that Americans are now subjected to.

Mr. BAKER. I do not think that we have actually done that. I think that our performance with respect to enforcing the CFAA has been better than that. And so I would submit that, you know, consistent and pursuant to oversight of this Committee in particular, we have not done that. I think the case that people are concerned

about, the Drew case, did not involve—it was not just some random case of somebody who happened to violate some terms of a service agreement. It was a case involving individuals essentially goading a 13-year-old girl into committing suicide, and I think it is understandable that law enforcement would take a dim view of that and try to address that kind of situation to the fullest extent of the law. In that particular situation, as I noted, the judge disagreed strongly with our interpretation of the statute. We reviewed his decision, and we decided not to appeal. And I do not think it is accurate for those who—I mean, we understand why people are concerned about the kinds of issues that you have raised with respect to terms of a service agreements and all these different contracts and so on. We get that. We understand that completely.

What we are trying to do is find a way to address those concerns and at the same time not let people off the hook who are insiders in particular companies.

Let me back up. The key thing is this term "exceeds authorized access" in the statute.

Senator WHITEHOUSE. Yes.

Mr. BAKER. As you well know. And so the key is: How do you avoid the kind of cases that you are very concerned about and yet at the same time not let off the hook somebody who works, again, at the IRS, the Social Security Administration, you name it, or some bank, to go in, take information, and misuse it for some particular purpose.

So we are happy to work with people to address these kinds of concerns. I will definitely take back your suggestion about issuing some clear policy statement. Maybe that would be helpful in this area.

Senator WHITEHOUSE. I think you are better off doing it yourself than counting on Congress to try to draw that fine line and that moving line. So I would recommend that.

Well, I have gone well beyond my time, which I was able to do since nobody else is here, so it was no prejudice to any colleague. And I want to express my appreciation, Special Agent Martinez, to you for the work that you and the Secret Service are doing in this area, and to you, Mr. Baker, for the work the Department of Justice is doing and for your long and very meritorious service to our country in these areas of national security.

As you know, I continue to believe that we are sorely underresourced in this area and that if you put the 230 prosecutors, many of whom are part-time—or no-time, depending on the nature of the district's caseload—up against, say, the Drug Enforcement Administration and ATF and major organizations like that that are working diligently and properly on threats to our National security and to our National well-being that are probably no greater than the threat we have from cyber crime and cyber attack, there is a huge disconnect. And I would urge that you and the administration ramp up a more energized proposal about how we can go after these folks, particularly bearing in mind how immensely complicated each one of these cases is going to be as you have to track down people in foreign countries and work through all of the complexities of engaging with foreign law enforcement authorities and dealing with the RICO statute. These are not easy cases, and

they take an immense amount of work just to do the forensic preparation of the case.

So as I said, my message is good job on the statute. Obviously, we are not going to agree with everything you have put in, but I think we do need to improve it. But the rhinoceros in the living room is the resource question, and it is fine to improve the statute, but we have really got, I think, to be much more aggressive about this in terms of—I know that individually everybody is doing a wonderful job. It is not your fault that there are not more of you to do this. But I think it is important for Congress to act in this area.

Thank you very much. We will keep the record open for 1 week, if anybody cares to add anything to it, and the hearing is adjourned. Thank you.

[Whereupon, at 11:30 a.m., the Committee was adjourned.]

[Submissions for the record follow.]

SUBMISSIONS FOR THE RECORD

August 3, 2011

The Honorable Patrick Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

The Honorable Charles Grassley
Ranking Member
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Senators Leahy and Grassley:

The undersigned individuals and organizations from across the philosophical spectrum share a commitment to ensuring our nation's cybersecurity in a manner consistent with the Bill of Rights and the rule of law. We write today regarding the Computer Fraud and Abuse Act, the subject of a planned Senate Judiciary Committee hearing. While the CFAA is an important tool in the fight against cybercrime, its language is also both overbroad and vague. The law can be read to encompass not only the malicious hackers and identity thieves the law was intended to cover, but also users who have not engaged in any activity that can or should be considered a "computer crime." Any attempt to update this increasingly outdated 1986 law should start with revisions addressing this structural problem before considering any increase in the penalties for violations.

The CFAA imposes civil and criminal liability for accessing a protected computer "without" or "in excess of" authorization, but fails to define "authorization." This makes the definition of the precise activities that are punishable unavoidably vague. As a result of this lack of clarity, several courts have used companies' network terms of use, which lay out *contractual* constraints on users' use of those networks, to also define what constitutes *criminal* behavior on those networks. The consequence is that private corporations can in effect establish what conduct violates federal criminal law when they draft such policies.

Our primary concern – that this will lead to overbroad application of the law – is far from hypothetical. Three federal circuit courts have agreed that an employee who exceeds an employer's network acceptable use policies can be prosecuted under the CFAA. At least one federal prosecutor has brought criminal charges against a user of a social network who signed up under a pseudonym in violation of terms of service.

These activities should not be "computer crimes," any more than they are crimes in the physical world. If, for example, an employee photocopies an employer's document to give to a friend without that employer's permission, there is no federal crime (though there may be, for example, a contractual violation). However, if an employee emails that document, there may be a CFAA violation. If a person assumes a fictitious identity at a party, there is no federal crime. Yet if they assume that same identity on a social network that prohibits pseudonyms, there may again be a CFAA violation. This is a gross misuse of the law. The CFAA should focus on malicious hacking and identity theft and not on criminalizing any behavior that happens to take place online in violation of terms of service or an acceptable use policy.

We believe any Judiciary Committee action to reform the CFAA should first attempt to correct this glaring vagueness and overbreadth. We are eager to assist the Committee in addressing problems in the existing statutory language and in ensuring that critical Justice Department resources are focused where they are most needed: on the malicious hackers and online criminals who invade others' computers and networks to steal sensitive information and undermine the privacy of those whose information is stolen.

Sincerely,

Laura W. Murphy, Director, Washington Legislative Office
American Civil Liberties Union

Kelly William Cobb, Executive Director
Americans for Tax Reform's Digital Liberty

Leslie Harris, President and CEO
Center for Democracy & Technology

Fred L. Smith, President
Competitive Enterprise Institute

Marcia Hofman, Senior Staff Attorney
Electronic Frontier Foundation

Charles H. Kennedy, Partner
Wilkinson, Barker, Knauer, LLP*

Wayne T. Brough, Ph.D., Chief Economist and Vice President, Research
FreedomWorks Foundation

Orin S. Kerr, Professor of Law
George Washington University*

Paul Rosenzweig
Visiting Fellow, The Heritage Foundation*

Berin Szoka, President
TechFreedom

*(Affiliation listed for identification purposes only)

cc: Members of the Judiciary Committee
James A. Baker, Associate Deputy Attorney General, USDOJ

Department of Justice

STATEMENT OF

JAMES A. BAKER
ASSOCIATE DEPUTY ATTORNEY GENERAL

BEFORE THE

COMMITTEE ON JUDICIARY
UNITED STATES SENATE

ENTITLED

"CYBERCRIME: UPDATING THE COMPUTER FRAUD AND ABUSE ACT TO PROTECT CYBERSPACE AND COMBAT EMERGING THREATS"

PRESENTED

September 7, 2011

TESTIMONY OF ASSOCIATE DEPUTY ATTORNEY GENERAL JAMES A. BAKER

Good afternoon, Chairman Leahy, Ranking Member Grassley, 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").

Senate Majority Leader Reid and six Senate committee chairs wrote to the President and asked for his input on cybersecurity legislation, and Members from both sides of the aisle have remained steadfast in their resolve to act. I want to particularly acknowledge your leadership, Chairman Leahy, in the effort to address these important threats. The Administration welcomed 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.

The penalty for the theft of information under section 1030(a)(2), for example, should be increased. Conduct that falls within this statute includes stealing trade secrets by corporate insiders, obtaining bank logon identification and passwords by domestic and foreign hackers, and

intruding into victim's personal information by stalkers. In order to enhance deterrence, we recommend that the maximum penalties for such conduct be increased.

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. Similarly, suppose a politician hired a hacker to break into the email account of his opponent and steal strategy documents. Under current law, that offense carries a maximum penalty of one year. 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 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.

Mandatory minimum 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 actual imprisonment of a term not less than three years – not probation, intermittent confinement, community confinement, or home detention. The Administration believes that a mandatory minimum sentence of three years imprisonment in addition to any other appropriate penalty provided for by existing criminal statutes will 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. 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 two 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 defendant, while employed as an account manager at a major bank, used her access to the bank's computerized customer account system to print out information for numerous customers and then provided that information to her half-brother so that he and his confederates could engage in identity theft. (United States v. John, 597 F.3d 263 (5th Cir. 2010)).

- A police officer obtained criminal history information from the National Crime Information Center database, 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)).

These are just two cases, but this tool is used routinely. Another example would be the prosecution of State Department employees for improperly accessing passport records of President Obama, Senator McCain, and others, in violation of State Department access rules. 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 a 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.

Statement Of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Committee On The Judiciary,
Senate Committee on the Judiciary Hearing on "Cybercrime: Updating the Computer Fraud and Abuse Act to Protect Cyberspace and Combat Emerging Threats"

September 7, 2011

Today, the Committee holds an important hearing on cybercrime. Protecting American consumers and businesses from cybercrime and other threats in cyberspace has been a priority of this Committee for many years. We continue that bipartisan tradition today.

I thank Senator Grassley for working closely with me on this hearing. Cybercrime impacts all of us, regardless of political party or ideology. I look forward to our continued partnership as the Committee, and the Congress, considers cybersecurity legislation.

Developing a comprehensive strategy for cybersecurity is one of the most pressing challenges facing our Nation today. In just the last few months, we have witnessed major data breaches at Sony, Epsilon, RSA, the International Monetary Fund, and Lockheed Martin -- just to name a few. Our Government computer networks have not been spared -- as evidenced by the hacking incidents involving the Senate and Central Intelligence Agency websites.

We cannot afford to ignore these threats, or their impact on our privacy and security. That is why the Committee will carefully examine the Obama administration's proposals for new legal tools to help law enforcement investigate and prosecute cybercrime today.

I thank and commend the dedicated men and women at the Departments of Justice and Homeland Security, and elsewhere across our Government, who are on the frontlines of the battle against cybercrime. Every day, they are successfully investigating and disrupting the growing threats to our cybersecurity.

In July, the FBI announced that it had arrested more than a dozen individuals associated with a group of computer hackers called Anonymous, after the group allegedly launched a series of cyberattacks on Government and private networks. The Secret Service recently announced a successful cybercrime investigation that led to the Federal indictment of an individual alleged to have hacked into the computer system at the Massachusetts Institute of Technology, resulting in the theft of more than four million scientific and academic articles.

These are just two examples of the many accomplishments of our law enforcement community in this area. But with each new victory, we are challenged by even greater threats and even more cunning cyber thieves. A recent report by the computer security firm Symantec found that on any given day, an average of 6,797 websites harbor malware, or other unwanted programs -- an increase of 25.5 percent since June 2011.

I am pleased that representatives from the Department of Justice and the Secret Service are here to share their views on how the new criminal tools in the Obama administration's cybersecurity proposal will help us to confront this challenge. Later this week, the Committee will consider these proposals and other privacy measures in my comprehensive data privacy and security legislation. I hope that the Committee will promptly report this legislation on a bipartisan basis, as it has done three times before.

To build a secure future for our Nation and its citizens in cyberspace, Congress must work together -- across party lines and ideology -- to address the dangers of cybercrime and other cyber threats. This is a national issue that we must address. I hope that all Members of the Committee will join me in bringing this bipartisan spirit to this hearing and to our work on cybersecurity legislation. I thank both of our witnesses for appearing today, and look forward to a good discussion.

#####

Statement of Mr. Pablo A. Martinez
Deputy Special Agent in Charge
Criminal Investigative Division
U.S. Secret Service

Hearing before the
Senate Committee on the Judiciary

"Cybercrime: Updating the Computer Fraud and Abuse Act to Protect Cyberspace and Combat Emerging Threats"

September 07, 2011

Good morning, Chairman Leahy, Ranking Member Grassley and distinguished members of the Committee. Thank you for the opportunity to testify on U.S. Secret Service's (Secret Service) investigative role in combating cyber crime.

As the original guardian of the Nation's financial payment systems, the Secret Service has a long history of protecting American consumers, industries and financial institutions. Over the last two decades, the Secret Service's statutory authorities have been reinforced to include access device fraud (18 USC §1029), which includes credit and debit card fraud. The Secret Service also has concurrent jurisdiction with other law enforcement agencies for identity theft (18 USC §1028), computer fraud (18 USC §1030), and bank fraud (18 USC §1344).

In 2010, the Secret Service's unique multifaceted approach to combating cyber crime led to the arrest of over 1,200 suspects for cyber crime related violations and the examination of 867 terabytes of data, which is roughly the equivalent of 867,000 copies of the Encyclopedia Britannica. These investigations involved over $500 million in actual fraud loss and prevented approximately $7 billion in additional losses. As a result of our efforts, the Secret Service is recognized worldwide for our innovative approaches to detecting, investigating and preventing cyber crimes. Furthermore, in alignment with the President's Comprehensive National Cyber Security Initiative, the Secret Service will continue to raise our overall capabilities in combating cyber crime and related forms of illegal computer activity.

The Administration is aware that in order to fully protect American citizens from cyber threats, certain sections of our current cyber security laws must be updated. Last spring, the Administration released its proposal to address the cybersecurity needs of our country. The legislative package proposed by the Administration addresses key improvements for law

enforcement. Secret Service investigations have shown that complex and sophisticated electronic crimes are rarely perpetrated by a lone individual. Online criminals organize in networks, often with defined roles for participants, in order to manage and perpetuate ongoing criminal enterprises dedicated to stealing commercial data and selling it for profit. The Administration's proposal will better equip law enforcement agencies, such as the Secret Service, with additional tools to combat transnational cyber crime by enhancing penalties against criminals that attack critical infrastructure and by adding computer fraud as a predicate offense under the Racketeering Influenced Corrupt Organizations Act (RICO).

The proposal also includes additional measures to protect consumers against identity theft by standardizing and simplifying the current patchwork of state laws that govern reporting of breaches of personally identifiable information and requiring businesses to notify affected individuals and the government if the business suffers a breach.

Trends in Cyber Crimes

Advances in computer technology and greater access to personal information via the Internet have created a virtual marketplace for transnational cyber criminals to share stolen information and criminal methodologies. As a result, the Secret Service has observed a marked increase in the quality, quantity and complexity of cyber crimes targeting private industry and critical infrastructure. These crimes include network intrusions, hacking attacks, development and use of malicious software, and account takeovers leading to significant data breaches affecting every sector of the world economy. As large companies have adopted more sophisticated protections against cyber-crime, criminals have adapted as well by increasing their attacks against small and medium-sized businesses, banks, and data processors. Unfortunately, many smaller businesses do not have the resources to adopt and continuously upgrade the sophisticated protections needed to safeguard data from being compromised.

The Secret Service has continued its collaboration with Verizon on the 2011 Data Breach Investigations Report (DBIR) to identify emerging threats, educate Internet users, and evaluate new technologies that work to prevent and mitigate attacks against critical computer networks. Researchers from law enforcement and the private sector examined roughly 800 new data breaches. The results from the Verizon study show that two of the noticeable trends in cybercrime over the past couple of years involve the ongoing targeting of Point of Sale (POS) systems as well as the compromise of online financial accounts, often through malware written explicitly for that purpose, with subsequent transaction fraud involving those accounts.

Compared to recent history, it appears that while there were more data breaches in 2010, the amount of compromised data decreased due to the size of the compromised companies' databases. This change demonstrates the willingness of organized cybercriminals to go after the smaller, easier targets that provide a smaller, yet steady, stream of potentially available data. In light of recent arrests and prosecutions following large-scale intrusions into financial services firms, criminals may be weighing the reward versus the risk, and opting to "play it safe".

The report also indicates that there has been noticeable increase in account takeovers that result in fraudulent transfers from the victim's account to an account under the control of the

perpetrator. This increase can be directly tied to the continued rise of malware variants created to capture login credentials to financial websites. The Secret Service and the financial services community are working together to combat this growing trend. The Financial Services Information Sharing and Analysis Center (FS-ISAC) has teamed up with the Secret Service, Department of the Treasury, Department of Justice and many other agencies to create the Account Takeover Task Force (ATOTF), which focuses on prevention, detection and response to account takeovers.

The increasing level of collaboration among cyber-criminals raises both the complexity of investigating these cases and the level of potential harm to companies and individuals. For example, illicit Internet carding portals allow criminals to traffic stolen information in bulk quantities globally. These portals, or "carding forums," operate like online bazaars where criminals converge to trade personal financial data and cyber-tools of the trade. The websites vary in size; some of these criminal forums are limited to a few hundred members while others boast memberships of tens of thousands of users. Within these portals, there are separate forums moderated by senior and experienced members of the carding community who discuss tactics and techniques for overcoming security controls and pursuing complex fraud schemes. Criminal purveyors on these forums buy, sell, and trade malicious software, spamming services, credit and debit card data, personal identification data, bank account information, brokerage account information, hacking services, counterfeit identity documents and other forms of contraband.

The effects of the criminal acts extend well beyond the companies compromised, affecting millions of individual card holders in one of the incidents. Although swift investigation, arrest, and prosecution prevented many consumers from direct financial harm, all potential victims were at risk for misuse of their credit cards, overall identity theft, or both. Further, business costs associated with the need for enhanced security measures, reputational damage and direct financial losses are ultimately passed on to consumers.

Collaboration with Other Federal Agencies and International Law Enforcement

While cyber-criminals operate in a world without borders, the law enforcement community does not. The increasingly multi-national, multi-jurisdictional nature of cyber crime cases has increased the time and resources needed for successful investigation and adjudication. The partnerships developed with other law enforcement entities, the private sector and academia through our Electronic Crimes Task Forces, the support provided by our Cyber Intelligence Section, the liaison established by our overseas offices, and the training provided to our special agents via Electronic Crimes Special Agent Program were all instrumental to the Secret Service's successful investigation into the network intrusion of Heartland Payment Systems – the largest and most complex data breach investigation ever prosecuted in the United States.

Recognizing these complexities, several federal agencies are collaborating to investigate cases and identify proactive strategies. Greater collaboration within the federal, state and local law enforcement community enhances information sharing, promotes efficiency in investigations, and facilitates efforts to de-conflict in cases of concurrent jurisdiction. For example, the Secret Service has collaborated extensively with the Department of Justice's Computer Crimes and Intellectual Property Section (CCIPS), a key partner in preventing, investigating and prosecuting

computer crimes. The Secret Service's Electronic Crimes Task Forces are a natural complement to CCIPS, and have resulted in an excellent partnership over the years. In the last decade, nearly every major cyber investigation conducted by the Secret Service has benefited from CCIPS contributions. Successful investigations such as the prosecution of the Shadowcrew criminal organization, E-Gold prosecution, and TJX and Heartland investigations, were a result of this valued partnership.

One of the main obstacles that agents investigating transnational crimes encounter are jurisdictional limitations. The Secret Service believes that to fundamentally address this issue, appropriate levels of liaison and partnerships must be established with our international law enforcement counterparts. Currently, the Secret Service operates 23 offices abroad, each having regional responsibilities to provide global coverage. The personal relationships that have been established in those countries are often the crucial element to the successful investigation and prosecution of suspects abroad.

Mitigation and prevention are keys to reducing the threat from cyber criminals. Recognizing this reality, the Secret Service has strengthened its partnership and collaboration with the National Protection and Programs Directorate's (NPPD) United States Computer Emergency Readiness Team (US-CERT), which provides response support and defense against cyber intrusions or incidents for the Federal Civil Executive Branch (.gov) domain, as well as information sharing and collaboration with state and local government, industry and international partners. As the Secret Service identifies malware, suspicious IPs and other information through its criminal investigations, it shares this information with US-CERT. To support such collaboration, US CERT recently published Early Warning Indicator Notices (EWINs) on information gathered through Secret Service investigations. The Secret Service looks forward to building on its full-time presence at US-CERT, and broadening this and other partnerships within the Department.

As a part of these efforts and to ensure that information is shared in a timely and effective manner, the Secret Service has personnel detailed to the following DHS and non-DHS entities:

- NPPD's Office of the Under Secretary;
- NPPD's National Cyber Security Division (US-CERT);
- NPPD's Office of Infrastructure Protection;
- National Cybersecurity and Communications Integration Center (NCCIC)
- DHS's Science and Technology Directorate (S&T);
- FBI National Cyber Investigative Joint Task Force (NCIJTF);
- Each FBI Joint Terrorism Task Force (JTTF), including the National JTTF;
- Department of the Treasury - Terrorist Finance and Financial Crimes Section
- Department of the Treasury - Financial Crimes Enforcement Network (FinCEN);
- Central Intelligence Agency;
- Department of Justice, International Organized Crime and Intelligence Operations Center;
- Drug Enforcement Administration's Special Operations Division
- EUROPOL; and
- INTERPOL

Secret Service Framework

In line with the Department's focus of creating a safer cyber environment and in order to protect our financial infrastructure, industry, and the American public, the Secret Service has adopted a multi-faceted approach to aggressively combat cyber and computer-related crimes. The Secret Service has dismantled some of the largest known transnational cyber-criminal organizations by:

- providing computer-based training to enhance the investigative skills of special agents through our **Electronic Crimes Special Agent Program**, and to our state and local law enforcement partners through the **National Computer Forensics Institute**;
- collaborating with our partners in law enforcement, the private sector and academia through our 31 **Electronic Crimes Task Forces**;
- identifying and locating international cyber-criminals involved in network intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes through the analysis provided by our **Cyber Intelligence Section**;
- maximizing partnerships with international law enforcement counterparts through our 23 **international field offices**; and
- maximizing technical support, research and development, and public outreach through the **Software Engineering Institute/CERT Liaison Program** at Carnegie Mellon University and the **Cell Phone/PDA Forensic Facility** at University of Tulsa.

Electronic Crimes Special Agent Program

A central component of the Secret Service's cyber-crime investigations is its Electronic Crimes Special Agent Program (ECSAP), which is comprised of nearly 1,400 Secret Service special agents who have received at least one of three levels of computer crimes-related training. These agents are deployed in more than 98 Secret Service offices throughout the world and have received training in forensic identification, preservation and retrieval of electronically stored evidence. ECSAP-trained agents are computer investigative specialists, qualified to conduct examinations on all types of electronic evidence. These special agents are equipped to investigate the continually evolving arena of electronic crimes and have proven invaluable in the successful prosecution of criminal groups involved in computer fraud, bank fraud, identity theft, access device fraud and various other electronic crimes targeting our financial institutions and private sector.

The ECSAP program is divided into three levels of training:

Level I – Basic Investigation of Computers and Electronic Crimes (BICEP) The BICEP training program focuses on the investigation of electronic crimes and provides a brief overview of several aspects involved with electronic crimes investigations. This program provides Secret Service agents and our state and local law enforcement partners with a basic understanding of computers and electronic crime investigations and is now part of our core curriculum for newly hired special agents.

Level II – Network Intrusion Responder (ECSAP-NI) ECSAP-NI training provides special agents with specialized training and equipment that allows them to respond to and investigate

network intrusions. These may include intrusions into financial sector computer systems, corporate storage servers or various other targeted platforms. The Level II trained agent will be able to identify critical artifacts that will allow effective investigation of identity theft, malicious hacking, unauthorized access, and various other related electronic crimes.

Level III – Computer Forensics (ECSAP-CF) ECSAP-CF training provides special agents with specialized training and equipment that allows them to investigate and forensically obtain legally admissible digital evidence to be utilized in the prosecution of various electronic crimes cases, as well as criminally focused protective intelligence cases.

Electronic Crimes Task Forces

In 1995, the Secret Service established the New York Electronic Crimes Task Force (ECTF) to combine the resources of academia, the private sector, and local, state and federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructures. Congress further directed the Secret Service in Public Law 107-56 to establish a nationwide network of ECTFs to "prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."

The Secret Service currently operates 31 ECTFs, including two based overseas in Rome, Italy and London, England. Membership in our ECTFs includes: 4,093 private sector partners; 2,495 international, federal, state and local law enforcement partners; and 366 academic partners. By joining our ECTFs, all of our partners benefit from the resources, information, expertise and advanced research provided by our international network of members while focusing on issues with significant regional impact.

Cyber Intelligence Section

Another example of our partnership approach with private industry is our Cyber Intelligence Section (CIS) which collects, analyzes, and disseminates data in support of Secret Service investigations worldwide and generates new investigative leads based upon its findings. CIS leverages technology and information obtained through private sector partnerships as well as evidence obtained from Secret Service investigations and undercover operations to monitor developing technologies and trends in the financial payments industry for information that may be used to enhance the Secret Service's capabilities to prevent and mitigate attacks against the financial and critical infrastructures.

CIS has an operational unit that investigates international cyber-criminals involved in cyber-intrusions, identity theft, credit card fraud, bank fraud, and other computer-related crimes. The information and coordination provided by CIS is a crucial element to successfully investigating, prosecuting, and dismantling international criminal organizations.

National Computer Forensics Institute

The National Computer Forensics Institute (NCFI) initiative is the result of a partnership between the Secret Service, NPPD, the State of Alabama and the Alabama District Attorney's

Association. The goal of this facility is to provide a national standard of training for a variety of electronic crimes investigations. The program offers state and local law enforcement officers, prosecutors, and judges the training necessary to conduct computer forensics examinations. Investigators are trained to respond to network intrusion incidents and conduct electronic crimes investigations.

Since the establishment of NCFI on May 19, 2008, the Secret Service has provided critical training to 932 state and local law enforcement officials representing over 300 agencies from all 50 states and two U.S. territories.

Computer Emergency Response Team/Software Engineering Institute (CERT-SEI)

In August 2000, the Secret Service and Carnegie Mellon University Software Engineering Institute (SEI) established the Secret Service CERT Liaison Program to provide technical support, opportunities for research and development and public outreach and education to more than 150 scientists and researchers in the fields of computer and network security, malware analysis, forensic development, training and education. Supplementing this effort is research into emerging technologies being used by cyber-criminals and development of technologies and techniques to combat them.

The primary goals of the program are: to broaden the Secret Service's knowledge of software engineering and networked systems security; to expand and strengthen partnerships and relationships with the technical and academic communities; to provide an opportunity to work closely with CERT-SEI and Carnegie Mellon University; and to present the results of this partnership at the quarterly meetings of our ECTFs.

In August 2004, the Secret Service partnered with CERT-SEI and the Department of Homeland Security's Science and Technology Directorate to publish the first ever "Insider Threat Study" examining the illicit cyber activity in the banking and finance sector. Due to the overwhelming response to this initial study, the Secret Service and CERT-SEI, in partnership with DHS S&T, are working to update the study. An updated study, expected to be released in late 2011, will analyze actual incidents of insider crimes from inception to prosecution. The research team will share its findings with federal, state, and local law enforcement, private industry, academia and other government agencies.

Cell Phone/Forensic Facility

The U.S. Secret Service Cell Phone Forensic Facility at the University of Tulsa conducts training, examinations, and research in the field of mobile device forensics to include skimmers, cell phones, and GPS units. The facility's mobile device forensic capabilities are among the best in the world. Agents trained at the facility complete examinations in the field with the more problematic devices submitted to the facility for examination. University of Tulsa students, who are a part of the national Cyber Corps Scholarship for Service Program, work in collaboration with special agents on mobile device research projects year round.

To date, 49 special agents have been trained in Basic Mobile Device Forensics; 48 special agents have been trained in Advanced Mobile Device Forensics; 31 special agents have been trained in Mobile Device Forensics Refresher; and 45 special agents have been trained in Advanced Android Forensics. The success of this program is clear, with over 5,000 mobile device examinations conducted since 2008.

Conclusion

As more information is stored in cyberspace, target-rich environments are created for sophisticated cyber criminals. With proper network security, businesses can provide a first line of defense by safeguarding the information they collect. Such efforts can significantly limit the opportunities for these criminal organizations. Furthermore, the prompt reporting of major data breaches involving sensitive personally identifiable information to the proper authorities will help ensure a thorough investigation is conducted.

The Secret Service is committed to safeguarding the Nation's financial payment systems by investigating and dismantling criminal organizations involved in cyber crime. Responding to the growth in these types of crimes and the level of sophistication these criminals employ requires significant resources and greater collaboration among law enforcement and its public and private sector partners. Accordingly, the Secret Service dedicates significant resources to improving investigative techniques, providing training for law enforcement partners and raising public awareness. The Secret Service will continue to be innovative in its approach to cyber crime and cyber security and is pleased that the Committee recognizes the magnitude of these issues and the evolving nature of these crimes.

Chairman Leahy, Ranking Member Grassley, and distinguished members of the Committee, this concludes my prepared statement. Thank you again for this opportunity to testify on behalf of the Secret Service. I will be pleased to answer any questions at this time.

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement for the Record of Gregory T. Nojeim
Director, Project on Freedom, Security & Technology
Center for Democracy & Technology

Before the Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism

CYBERSECURITY: EVALUATING THE ADMINISTRATION'S PROPOSALS

June 21, 2011

Chairman Whitehouse, Ranking Member Kyl, and Members of the Subcommittee:

Thank you for the opportunity to submit this statement for the record on behalf of the Center for Democracy & Technology[1] about the Administration's proposed cybersecurity legislation.[2] We applaud the Subcommittee for examining these proposals, critical parts of which implicate matters that are within the jurisdiction of the Judiciary Committee, including:

- Data breach notification;
- Amendments to the Computer Fraud and Abuse Act; and
- Cybersecurity information sharing provisions.

Today, I will briefly outline existing threats to our cybersecurity. I will then discuss some of the key distinctions that must be drawn in order to chart a path forward that provides for meaningful improvements in security while ensuring protection for America's cherished rights of privacy and free expression and encouraging continued innovation. I will examine the Administration's cybersecurity proposals in broad strokes, then focus on the three proposals that fit within the Judiciary Committee's jurisdiction. I will suggest an approach to information sharing more likely to protect civil liberties and promote security, explain why the Administration's data breach notification proposal is a good start but needs some modifications, and encourage you to address longstanding concerns with

---

[1] The Center for Democracy & Technology is a non-profit public interest organization dedicated to keeping the Internet open, innovative and free. Among our priorities is preserving the balance between security and freedom. CDT coordinates a number of working groups, including the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies, and trade associations interested in information privacy and security issues.

[2] Text of the White House cybersecurity legislative proposal: http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf (hereinafter, "White House proposal") Section-by-section analysis of the proposal, prepared by the White House: http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill-Section-by-Section-Analysis.pdf.

the ambiguity and breadth of the CFAA before considering the penalty enhancements the Administration has proposed.

An overarching theme of our statement for record is that Congress should take a careful, nuanced approach when crafting cybersecurity authorities, avoiding overbroad legislation and the attendant unintended consequences to individual rights and technological innovation. In particular, CDT urges the Subcommittee to think carefully about the role of government in enhancing national cybersecurity. Government action is surely required in some areas, but in others government intervention would raise significant civil liberties concerns, could impede innovation, and might be counterproductive from a security standpoint.

The Cybersecurity Threat

The United States faces significant cybersecurity threats from state actors, from private actors motivated by financial greed, and from terrorists. Earlier this month, the International Monetary Fund (IMF) released news of a major attack on its network that may have given hackers access to the organization's collection of sensitive market data about struggling state economies worldwide.[3] The IMF's announcement came just weeks after one of the nation's largest defense contractors, Lockheed Martin, suffered a "significant and tenacious" cyber attack on May 21.[4] In 2010, the Stuxnet worm, allegedly designed with the involvement of the U.S. government, penetrated the control systems of centrifuges Iran was using to refine uranium, causing hundreds of the centrifuges to spin out of control and damage themselves.[5]

The GAO, among others, has repeatedly criticized the federal government for failing to respond adequately to this threat.[6] The scope of the federal response should not be dictated by the need to react to such criticisms, however, but instead by the actual problems that lie behind them.

---

[3] Sudeep Reddy and Siobhan Gorman, IMF Hit by Cyber Attack, *The Wall Street Journal* (June 11, 2011), http://online.wsj.com/article/SB10001424052702304259304576380034225081432.html.

[4] Gopal Ratnam, U.S. Offers Lockheed Help After 'Tenacious' Cyber Attack, *Bloomberg News* (May 29, 2011), http://www.bloomberg.com/news/2011-05-29/lockheed-offered-help-after-cyber-incident-u-s-government-says.html.

[5] William Broad, et al., Israeli Test on Worm Called Crucial in Iran Nuclear Delay, *New York Times* (January 15, 2011), http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

[6] *See, e.g.*, Testimony of David A. Powner, Director, Information Technology Management Issues, Government Accountability Office, before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity of the House Committee on Homeland Security, *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity* (September 13, 2006), *http://www.gao.gov/new.items/d061087t.pdf*. In 2008, GAO reported that the Department of Homeland Security's U.S. Computer Emergency Readiness Team, which has significant responsibilities for protecting private and governmental computer networks, was failing to establish a "truly national capability" to resist cyber attacks. Government Accountability Office, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability* (July 2008), http://www.gao.gov/products/GAO-08-588. In 2009, GAO testified that DHS had yet to comprehensively satisfy its cybersecurity responsibilities. Testimony of Gregory C. Wilshusen, Director, Information Security Issues, before the Subcommittee on Technology and Innovation of the House Committee on Science and Technology, Government Accountability Office, *Cybersecurity, Continued Federal Efforts Are Needed to Protected Critical Systems and Information* (June 25, 2009), http://democrats.science.house.gov/Media/file/Commdocs/hearings/2009/Tech/25jun/Wilshusen_Testimony.pdf. In 2010, GAO found continued shortcomings. *Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed*, GAO-11-24 (October 6, 2010), http://www.gao.gov/products/GAO-11-24.

A Careful and Nuanced Approach Is Required for Securing the Internet

In developing a national policy response to cybersecurity challenges, a nuanced approach is critical. One size does not fit all. There are four important sets of distinctions to be drawn in any attempt to tackle the cybersecurity problem:

- First, a distinction must be drawn between those systems that are government-owned and those that are owned by the private sector.
- Second, distinctions must be drawn based on the degree to which the operation of particular systems is vital to the national well-being.
- Third, systems that support free speech and democratic discourse must be distinguished from those that do not.
- Fourth, threats to systems must be distinguished based on the capabilities and intentions of the originators of those threats.

Keeping these distinctions in mind when tailoring a cybersecurity policy to the needs of various systems is vital.

First, it is absolutely essential to draw appropriate distinctions between military government systems, civilian government systems, and systems owned and operated by the private sector. Policy towards government systems, both those in the military domain and those under .gov, can, of course, be much more "top down" and much more prescriptive than policy towards private systems.

Second, particularly with respect to private systems, it is important to remember that most networks are not critical infrastructure and should not be treated as such. While the Internet is a "network of networks" encompassing at its edges everything from personal computers in the home to servers controlling the operation of nuclear power plants, cybersecurity policy should not sweep all entities that connect to the Internet into the same regulatory basket. For example, while it is appropriate to require strong authentication of a user of an information system that contains classified information or controls a critical element of the electric power grid, it would not be appropriate to require authentication of ordinary Americans surfing the Internet on their home computers.

Third, when developing policy responses, appropriate distinctions should be made between the elements of critical infrastructure that primarily support free speech and democratic participation – most prominently the Internet – and those that do not. The characteristics that have made the Internet such a success – its open, decentralized, and user-controlled nature and its support for innovation and free expression – may be put at risk if heavy-handed cybersecurity policies are enacted that apply uniformly to all critical infrastructure. Policies that may be appropriate for the power grid or the banking system may not be appropriate for components of the Internet used for exercising First Amendment rights to speak, associate, and petition the government.

Fourth, any cybersecurity policy must recognize that networked system security is aimed at countering a broad range of threats, from national-level actors engaging in the theft of state secrets to organized criminals engaged in financial fraud to teenage hackers testing their skills. As one cybersecurity expert has noted, it is important to "break down attacks by attribution and

category."[7] Only then can the cybersecurity policy be appropriately tailored to a particular set of threats and not attempt to fit these diverse activities into the same policy framework.

For all these reasons, a sectoral, threat-specific approach is called for. Very careful distinctions – too often lacking in cybersecurity discourse – are needed to ensure that the elements of the Internet critical to new economic models, human development, and civic engagement are not regulated in ways that could stifle innovation, chill free speech, or violate privacy.

Top Line View of the Administration's Cybersecurity Proposals

The White House's legislative package of cybersecurity reforms is largely balanced and contains some appropriate nuance, but includes some troubling provisions.

As compared to the leading Senate cybersecurity bill (the Cybersecurity and Internet Freedom Act (CIFA), S. 413), the Administration's bill could subject more entities and assets to regulation as "critical infrastructure" but that regulation would have a lighter touch. The White House proposal defines critical infrastructure as those entities and assets whose incapacity or disruption would cause "a debilitating impact."[8] This vague language could encompass a broad swath of industry. CIFA does a better job, defining critical infrastructures as those systems whose disruption would cause "a mass casualty event which includes an extraordinary number of fatalities," "severe economic consequences," "mass evacuations with a prolonged absence," or "severe degradation of national security capabilities, including intelligence and defense functions."[9] On the other hand, CIFA would impose heavier regulatory burdens on those critical infrastructure owners and operators. CIFA would impose fines for non-compliance with key requirements, while the Administration bill would instead use transparency to encourage compliance, by requiring companies to report publicly their compliance failures. CDT favors the tighter definition of "critical infrastructure" in CIFA (though we would tighten it more) and the lighter regulatory hand of the Administration's bill.

Like CIFA, the White House bill properly makes the Department of Homeland Security (DHS) rather than the Department of Defense (DOD) responsible for securing civilian government systems and for working with the private sector to secure privately held critical infrastructure. The Department of Defense would continue to secure classified systems and the .mil domain. This is the best allocation of responsibilities. There is serious concern that if the National Security Agency or another DOD entity were to take the lead role in cybersecurity for civilian unclassified systems or private sector systems, it would almost certainly mean less transparency, less trust, and less corporate and public participation, thereby increasing the likelihood of failure and decreasing the effectiveness of the effort. The White House legislation draws the lines of authority appropriately.

The White House bill also wisely omits any provision that would give the President or DHS the

[7] Scott Charney, Rethinking the Cyber Threat: A Framework and a Path Forward 7 (2009) http://download.microsoft.com/download/F/1/3/F139E667-8922-48C0-8F6A-B3632FF86CFA/rethinking-cyber-threat.pdf.

[8] White House proposal, proposed Section 3(b)(1)(A) of the Cybersecurity Regulatory Framework for Critical Infrastructure Act.

[9] S.413, Cybersecurity and Internet Freedom Act of 2011, proposed Section 254 of the Homeland Security Act and amendments to Section 210E of the Homeland Security Act.

authority to limit or shut down Internet traffic to a compromised critical infrastructure information system in an emergency or to disconnect such systems from other networks for reasons of national security.[10] This is good policy for many reasons. To our knowledge, no circumstance has yet arisen that could justify a governmental order to limit or cut off Internet traffic to a particular privately owned and controlled critical infrastructure system. Operators know better than do government officials whether their systems need to be shut down or isolated. In contrast, a new Presidential "shut down" power comes with a myriad of unexamined risks. Even if such power over private networks were exercised only rarely, its mere existence could enable a President to coerce costly, questionable – even illegal – conduct by threatening to shut down a system. It would make private sector operators reluctant to share information because it could be used to order them to shut down. Conversely, when private operators do determine that shutting down a system would be advisable, they might hesitate to do so without a government order, and could lose precious time waiting to be ordered by the government to shut down so as to avoid liability for the damage a shutdown could cause others. Finally, the grant of "shut down" authority to the President for cybersecurity purposes would set a precedent other repressive countries would cite when shutting down Internet services for other purposes, including the stifling of dissent. For all of these reasons, we believe it was wise for the Administration to leave this issue out of its bill.

Finally, the White House legislation honors the President's pledge, made in connection with the 2009 release of the Cyberspace Policy Review, that the federal government would not monitor private networks as part of its cybersecurity program.[11] Monitoring private communications networks is the job of the private sector communications service providers themselves, not of the government. Private sector operators already monitor their networks on a routine basis to detect and respond to attacks as necessary to protect their networks.

Nevertheless, caution must be exercised to ensure that government monitoring of private-to-private communications does not occur as an indirect result of information sharing between the private and public sectors or as an unintended by-product of programs put in place to monitor communications to or from the government.

I will now turn to the Administration's information sharing proposal and its other proposals that fall with the Judiciary Committee's jurisdiction.

White House Information Sharing Proposal Is Overbroad, Raising Privacy Concerns

There is widespread agreement that the current level of cybersecurity information sharing – sharing that is essential to a robust cybersecurity program – is inadequate. Private sector network operators and government agencies monitoring their own networks could better respond to threats if they had more information about what other network operators are seeing. How to encourage more robust information sharing without putting privacy at risk is a central policy challenge that falls to the Judiciary Committee to resolve, because many of the statutes

[10] The Cybersecurity and Internet Freedom Act includes such a provision. For an analysis, see http://www.cdt.org/blogs/greg-nojeim/does-senate-cyber-bill-include-internet-kill-switch.

[11] When the White House released the Cyberspace Policy Review on May 29, 2009, President Obama pledged that: *"Our pursuit of cybersecurity will not – I repeat, will not – include monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans."*

that would have to be amended or overridden are within the Committee's jurisdiction.

a. Information Sharing Between the Private Sector and DHS Under the White House Proposal

As a solution to this problem, the White House has proposed a sweeping information sharing regime that would permit any entity to share with DHS any information the entity may have, including communications traffic, no matter how it was acquired, no matter whether it is thought to include information about an attack or not, and *no matter how use and disclosure of that information would otherwise be restricted by law*, so long as the entity shares it for the purpose of protecting a system against a cybersecurity threat, makes reasonable efforts to remove irrelevant identifying information, and complies with as-yet-unwritten privacy protections.[12] The provision would permit a vast amount of personal information to flow to and from DHS and would effectively override protections in the Wiretap Act, the Electronic Communications Privacy Act, the Communications Assistance for Law Enforcement Act, the Foreign Intelligence Surveillance Act, the Freedom of Information Act, the Privacy Act of 1974, and the Sherman Antitrust Act – statutes within the jurisdiction of the Judiciary Committee.[13] In contrast, the leading Senate cybersecurity bill explicitly requires information sharing relating to cybersecurity to adhere to the statutory schemes governing electronic surveillance.[14]

In other words, this "hub and spoke" model of information sharing in the White House bill puts the Department of Homeland Security at the center. DHS would receive information, analyze it, and could share what it receives as well as the results of its analysis with other entities.

On the plus side, information sharing under the Administration proposal would be voluntary, not mandatory. This is commendable because giving a governmental entity mandatory authority to access private sector data that is relevant to cybersecurity[15] would completely eviscerate the electronic surveillance laws and would undermine the public-private partnership that needs to develop around cybersecurity. In addition, it is good to see that the proposal indicates that DHS's policies and procedures must require destruction of communications intercepted or disclosed for cybersecurity purposes that do not appear to be related to cybersecurity threats.

In other regards, however, the White House proposal raises serious concerns. Most fundamentally, the White House information sharing proposal is based on an unsupported premise: the bill assumes that the government is in the best position to identify threats to private sector networks. Therefore, the proposal would permit the sharing of much Internet traffic with the DHS for analysis. We believe that there is no evidence that the government has either the expertise or the ability to act quickly enough to protect private sector networks better than the private sector can. A better approach is to build on and improve the current network security activities of the private sector. As we explain below in our discussion of an alternative approach to information sharing, much more narrowly targeted changes can be made to the privacy laws. Such changes would promote private sector cooperation for cybersecurity without the risks

---

[12] White House proposal, "Department of Homeland Security Cybersecurity Authority and Information Sharing, proposed Section 245 of the Homeland Security Act.

[13] It also supersedes any state statute that regulates interception, collection, use, and disclosure of communications.

[14] S. 413, Cybersecurity and Internet Freedom Act of 2011, proposed Section 246(c) of the Homeland Security Act.

[15] For an example of such a proposal, see Section 14 of S. 773, the Cybersecurity Act of 2009, as introduced in the 111th Congress.

associated with feeding large amounts of traffic to the government.

Under the White House proposal, DHS could use and retain the communications traffic and other information it receives from service providers, could further disclose that information to private entities and to state and local governmental entities for cybersecurity purposes, and could disclose it to law enforcement entities when it is evidence of a crime. Agencies receiving communications, records, and other disclosures from DHS could use them for cybersecurity and law enforcement purposes and could further disclose them to other entities that have agreed in writing to use them for cybersecurity and law enforcement purposes and to abide by the as-yet-unwritten privacy protections.

The privacy and civil liberties protections in the proposal are weak, difficult to enforce, and principally center on the purpose limitation: limiting information sharing to cybersecurity and law enforcement purposes. Sharing a vast amount of communications traffic could, however, fall within those broadly defined purposes. The legislation would draw no distinctions between sharing content and non-content. While DHS would issue policies and procedures designed to protect privacy and civil liberties, it would have substantial discretion about what to include and little legislative guidance. The proposed legislation does not require that those policies and procedures be subject to notice and comment rulemaking under the Administrative Procedure Act. Moreover, there is no effective way for an aggrieved party to enforce compliance with the policies and procedures because there is no private right of action for violations. Knowing and willful violations are misdemeanors that the Department of Justice has discretion to prosecute; they bring no prison time and fines can be no more than $5,000/incident. Companies and state and local governments that violate the law and share communications and other information for inappropriate purposes, or who fail to strip out irrelevant identifying information, or who violate the privacy policies and procedures, are immune from civil and criminal liability under *all other laws* if they relied in good faith on their own determination that their conduct was permitted in the proposed statute. Finally, the DOJ – a law enforcement agency – would decide which information could be disclosed for law enforcement purposes.

We urge you to assert jurisdiction over cybersecurity information sharing within the purview of the Committee, and to take a more nuanced approach.

b. An Alternative Approach

First, Congress should determine exactly what information should be shared that is not shared currently. Improving information sharing should proceed incrementally. It should start with an understanding of why existing structures, such as the U.S. Computer Emergency Readiness Team ("U.S. CERT")[16] and the public-private partnerships represented by the Information

[16] U.S. CERT is the operational arm of the Department of Homeland Security's National Cyber Security Division. It helps federal agencies in the .gov space to defend against and respond to cyber attacks. It also supports information sharing and collaboration on cybersecurity with the private sector operators of critical infrastructures and with state and local governments.

Sharing and Analysis Centers (ISACs),[17] are inadequate. The Government Accountability Office (GAO) has made a series of suggestions for improving the performance of U.S. CERT.[18] Those suggestions included giving U.S. CERT analytical and technical resources to analyze multiple, simultaneous cyber incidents and to issue more timely and actionable warnings; developing more trusted relationships to encourage information sharing; and providing U.S. CERT sustained leadership within DHS that could make cyber analysis and warning a priority. All of these suggestions merit attention.

Second, an assessment should be made of whether the newly-established National Cybersecurity and Communications Integration Center (NCCIC) has addressed some of the information sharing issues that have arisen. The NCCIC is a round-the-clock watch and warning center established at DHS. It combines U.S. CERT and the National Coordinating Center for Communications and is designed to provide integrated incident response to protect infrastructure and networks.[19] Industry is now represented at the NCCIC[20] and its presence there should facilitate the sharing of cybersecurity information about incidents.

Third, Congress must make a realistic assessment as to whether an information sharing model that puts the government at the center – receiving information, analyzing it, and sharing the resulting analysis and even the raw information itself with industry – could ever be the basis for a rapid-response center possessing adequate expertise to effectively protect an overwhelmingly diverse set of private systems and enough speed and flexibility to respond to fast-moving threats. We have serious doubts. An industry-based model, subject to strong privacy protections, might be able to act more quickly and would raise few, if any, of the Fourth Amendment concerns associated with a government-centric model.

An information sharing approach that relies on the expertise of network operators would be far less disruptive of the current legal framework. Current law already gives communications service providers authority to monitor their own systems and to disclose both to governmental entities and to their own peers information about cyberattack incidents for the purpose of protecting their own networks. In particular, the federal Wiretap Act provides that it is lawful for any provider of electronic communications service to intercept, disclose, or use communications passing over its network while engaged in any activity that is a necessary incident to the protection of the rights and property of the provider.[21] This includes the authority to disclose

[17] Each critical infrastructure industry sector defined in Presidential Decision Directive 63 has established an Information Sharing and Analysis Center (ISAC) to facilitate communication among critical infrastructure industry representatives, a corresponding government agency, and other ISACs about threats, vulnerabilities, and protective strategies. *See* Memorandum from President Bill Clinton on Critical Infrastructure Protection (Presidential Decision Directive/NSC-63) (May 22, 1998), http://www.fas.org/irp/offdocs/pdd/pdd-63.htm. The ISACs are linked through an ISAC Council, and they can play an important role in critical infrastructure protection. *See* The Role of Information Sharing and Analysis Centers (ISACs) in Private/Public Sector Critical Infrastructure Protection 1 (January 2009), http://www.isaccouncil.org/whitepapers/files/ISAC_Role_in_CIP.pdf.

[18] *See* Government Accountability Office, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability* (July 2008), http://www.gao.gov/products/GAO-08-588.

[19] *See* DHS Press Release announcing opening of the NCCIC, http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm.

[20] *See* DHS Press Release announcing that it has agreed with the Information Technology Information Sharing and Analysis Center (IT-ISAC) to embed a full time IT-ISAC analyst at the NCCIC, November 18, 2010, http://www.dhs.gov/ynews/releases/pr_1290115887831.shtm.

[21] 18 U.S.C. § 2511(2)(a)(i).

communications to the government or to another private entity when doing so is necessary to protect the service provider's network. Likewise, under the Electronic Communications Privacy Act (ECPA), a service provider, when necessary to protect its system, can disclose stored communications[22] and customer records[23] to any governmental or private entity.[24] Furthermore, the Wiretap Act provides that it is lawful for a service provider to invite in the government to intercept the communications of a "computer trespasser"[25] if the owner or operator of the computer authorizes the interception and there are reasonable grounds to believe that the communication will be relevant to investigation of the trespass.[26]

These provisions do not, in our view, authorize ongoing or routine disclosure of traffic by the private sector to any governmental entity. To interpret them so broadly would destroy the promise of privacy in the Wiretap Act and ECPA. Furthermore, the extent of service provider disclosures to the government for self-defense purposes is not known publicly. We urge the Subcommittee to consider imposing a requirement that the extent of such information sharing be publicly reported, in de-identified form, both to assess the extent to which beneficial information sharing is occurring and to guard against ongoing or routine disclosure of Internet traffic to the government under the self-defense exception.

While current law authorizes providers to monitor their own systems and to disclose voluntarily communications and records necessary to protect their own systems, the law does not authorize service providers to make disclosures to other service providers or to the government to help protect the systems of those other service providers. Perhaps it should. There may be a need for a very narrow exception to the Wiretap Act, ECPA, FISA, and other laws that would permit disclosures about specific attacks and malicious code on a voluntary basis and that would immunize companies against liability for these disclosures.

The exception would have to be narrow so that routine disclosure of Internet traffic to the government or other service providers remained clearly prohibited. It would thus need to focus on the categories of information that many believe are most important to share: cyberattack signatures and attribution data associated with suspected cyberattacks. Under the approach we envision, these narrowly defined categories of information could be shared more widely, permitting service providers to share directly with each other without going through the government. Rather than taking the dangerous step of overriding the surveillance statutes, such a narrow exception could operate within them, limiting the impact of cybersecurity information sharing on personal privacy. CDT is drafting such an exception and is seeking comment in an effort to ensure that it is effective, is not overbroad, and includes appropriate enforcement and reporting requirements in order to prevent misuse.

Moreover, we urge the Subcommittee, before making any amendments that weaken the controls and privacy protections of the surveillance laws, to consider counterbalancing such

[22] 18 U.S.C. § 2702(b)(3).

[23] 18 U.S.C. § 2702(c)(5).

[24] Another set of exceptions authorizes disclosure if "the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications [or information] relating to the emergency." 18 U.S.C. §§ 2702(b)(8) and (c)(4).

[25] A "computer trespasser" is someone who accesses a computer used in interstate commerce without authorization. 18 U.S.C. § 2510(21).

[26] 18 U.S.C. § 2511(2)(i).

changes with legislation to update ECPA by making its privacy protections more relevant to today's digital environment.[27] We would welcome the opportunity to work with the Subcommittee on such legislation.

c. Inter-agency Information Sharing To Prevent Intrusions Into Government Networks

Just as private sector network operators should, and do, monitor their systems for intrusions, the federal government clearly has the responsibility to monitor and protect its own systems. At the same time, such efforts must start with the understanding that citizens' communication with their government implicates the exercise of the First Amendment rights of free speech and petitioning the government, which will be chilled if communications between Americans and their government are routinely shared with law enforcement and intelligence agencies. While the Fourth Amendment may not be implicated in citizen-to-government communications (because those communicating with governmental entities necessarily reveal their communications – including content – to the government), the privacy and civil liberties inquiry does not stop there. Protecting privacy in this context is absolutely critical to giving Americans the necessary comfort to communicate with their government, whether to access services or to criticize government actions.

The White House proposal puts the responsibility to monitor government civilian networks right where it belongs: on the shoulders of the Department of Homeland Security. Under the bill, DHS is charged broadly with engaging in cybersecurity and information infrastructure protection for civilian government systems in what would become new Sections 243 and 244 of the Homeland Security Act. Among other things, DHS would conduct risk assessments of federal systems and maintain a cybersecurity center that would serve as a focal point for cybersecurity information flowing from other governmental agencies at the federal, state, and local level and from the private sector.

We are concerned, though, about the vast scope of the information that could flow to the DHS cybersecurity center from other federal agencies under the White House proposal. The center would be authorized, notwithstanding any law, to intercept, retain, use, and disclose communications traffic to, from, or on any federal system and to deploy countermeasures that block or modify data packets on an automated basis, for cybersecurity purposes.[28] Communications content could be retained, used, and disclosed for cybersecurity purposes when associated with a known or suspected threat, and disclosed to law enforcement when it constitutes evidence of a crime. Users of federal systems would have to be given notice of the monitoring and potential for onward disclosure, but such blanket, mandatory "consent" is not true consent and does not address the First Amendment and privacy concerns. DHS would issue its own privacy and civil liberties policies and procedures in connection with this program, but there would be no independent oversight or auditing to ensure that only traffic to and from government systems is accessed and that ECPA is not being violated through access to purely private communications. Instead, the Secretary of DHS would annually certify the department's

[27] Specifically, the Judiciary Committee should take up the reforms proposed by the Chairman in the Electronic Communications Privacy Act Amendments Act of 2011 (S. 1011) introduced on May 17. There is widespread support for updating ECPA. Digital Due Process, a coalition of technology companies, communications service providers, academics, think tanks, and advocacy groups spanning the political spectrum, has recommended targeted, reasonable updates to ECPA. *See* www.digitalddueprocess.org. The Center for Democracy & Technology is a leading member of DDP.

[28] White House proposal, proposed Section 244(b) of the Homeland Security Act.

compliance with these provisions. No penalty is specified for violations.

While we recognize the right and responsibility of the federal government to monitor its networks for intrusion, the scope of this authorization and lack of independent oversight give us pause because the legislation appears to authorize significantly more activity than is necessary to facilitate operation of DHS's Einstein intrusion detection and prevention system.[29] At a minimum, Congress should consider requiring information collected by the center to be disposed of after a set period; requiring independent audits to ensure that only communications traffic with the government is acquired, retained, and used; and requiring DHS to provide an assessment of the federal laws that are being overridden to permit this monitoring program.

White House Data Breach Notification Proposal A Good Starting Point

The White House proposal would require business entities that hold "sensitive personally identifiable information" (SPII) about more than 10,000 people to notify such persons when the business entity suffers a cybersecurity breach that results in disclosure of SPII, unless the breach involves no reasonable risk of harm to the individual. The White House data breach notification proposal is similar in many respects to the data breach notification provisions in the Personal Data Privacy and Security Act (S. 1151) that Senator Leahy introduced on June 7, 2011.[30] Both contain the same coverage threshold (business entities holding SPII of at least 10,000 people), the same harm standard that obviates notice only when there is no reasonable risk of harm, and similar enforcement schemes.

Data breach notification serves cybersecurity purposes by encouraging large business entities that hold personally identifiable information to better protect that information. It also helps defend against the theft of identity, a problem that can undermine cybersecurity in some contexts. Because most states have already adopted data breach notification laws, breach notification is already effectively the law of the land.[31] The White House proposal would pre-empt those laws and therefore warrants special scrutiny to protect against eliminating current protections or other unintended consequences. It would wisely permit enforcement by state attorneys general and includes an innovative provision to authorize the Federal Trade Commission to adjust the categories of SPII it is intended to protect.

Data breach notification, however, is primarily a consumer privacy matter that CDT believes should be part of comprehensive consumer privacy legislation. We urge that you not miss the forest for the trees: what is needed is legislation to protect consumer privacy in the online and

---

[29] The Einstein system is designed to detect and interdict malicious communications traffic to or from federal networks. It assesses network traffic against a pre-defined database of malicious signatures and detects and reports anomalies in network traffic. Einstein operates on the network of an ISP providing service to the government instead of operating on the network of the agency being protected, creating a risk that Einstein could monitor communications traffic that is not to or from a government entity. More about the program can be found in the Einstein 2 Privacy Impact Assessment (PIA) (May 19, 2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf, in the PIA for the Einstein Initiative Three Exercise (March 18, 2010), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3exercise.pdf, and in legal opinions issued by the Department of Justice concluding that the Einstein program operates lawfully: http://www.justice.gov/olc/2009/e2-issues.pdf (January 9, 2009), and http://www.justice.gov/olc/2009/legality-of-e2.pdf (August 14, 2009).

[30] The data breach notification provisions in the Personal Privacy and Security Act are in Sections 311-322 of the bill, S. 1151.

[31] *See, e.g.*, http://www.cdt.org/policy/congressional-committee-revives-data-security-legislation.

offline world that incorporates the full range of Fair Information Practice Principles. The effort to adopt data breach notification should not undermine the push for baseline consumer privacy legislation. That said, we believe that if Congress does enact federal data breach notification legislation, the White House proposal is a good starting point, although it should be improved as outlined below.

Definition of Sensitive Personally Identifiable Information. The definition in the White House proposal of "sensitive personally identifiable information" should include health data tied to a name or another identifier. Unless this change is made, the bill would pre-empt several state breach notice laws – such as California's[32] – that cover health data linked to the individual's name. The provision empowering the FTC to modify the definition of sensitive information in rulemaking should be retained to help keep the statute up to date as technology evolves, new categories of sensitive data are put at risk, and new identifiers are developed.

Preemption. The White House proposal would override any provision of state law relating to notification by a business entity "of a security breach of computerized data," but it only requires notice of a subset of such breaches: breaches of data containing specifically defined "sensitive personally identifiable information." As a result, for example, given the definitional problem we noted above, notice of breaches involving personally identifiable health data appears to be outside the scope of the proposed notice requirement but within the scope of the preemption section. That one example can and should be fixed in the statute, but the broader problem of the disconnect between coverage and preemption would remain. Preemption of state law should be limited to the data covered by the federal law, permitting states to develop their own laws to address breach of information categories not covered under the proposal.

Notification Trigger. Businesses must notify consumers of data breaches involving SPII under the White House proposal unless the business determines that there is "no reasonable risk of harm or fraud to consumers." Under this formulation, once a company reasonably determines that a breach has occurred, notice is the default and must be given *unless* there is an affirmative finding of no risk. "Harm" should be construed to include reputational harm or embarrassment, and some disclosures of personally identifiable information, such as health information, should be considered harmful per se; with such a construction, the proposal's trigger appears to be effective while avoiding notification regarding truly inconsequential data breaches. We would caution against requiring notification only where harm has occurred or is likely to occur, or only where there was a determination of a significant risk of harm. If a business determines that there is no reasonable risk of harm and that it is not obligated to notify consumers of a breach, the proposal would require the business to submit its risk assessment to the FTC – a critical safeguard for which CDT has advocated.[33]

Delays for Law Enforcement. Under the White House proposal, federal law enforcement agencies can require businesses to delay notification of a breach if the agencies determine that notification would impede a criminal investigation or national security activity. While such a

[32] California's data breach law can be found in its Civil Code at Sections 1798.25-1798.29, http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29. The White House proposal could also be modified to include an exception, such as is found in California law, specifying that notification is not required for instances of good faith unauthorized access or acquisition of the data by employees or agents of the data holder, provided the data was not further used or disclosed in an unauthorized manner.

[33] http://www.cdt.org/copyright/20090505_data_p2p.pdf.

provision is appropriate, it should limit the duration of the periods of delay (e.g., 30 days) and require written authorization by a senior law enforcement official.

Computer Fraud Law Needs Tightening Before Increased Penalties Are Considered

The White House proposal includes various amendments to the Computer Fraud and Abuse Act (CFAA).[34] The White House seeks to further broaden the reach of the CFAA, eliminate its first-time offender provisions, make CFAA violations RICO predicates, impose for conspiracies and attempts the same penalties imposed for completed acts that violate the CFAA, impose mandatory minimums for some violations, and add real property to the assets that can be forfeited in civil or criminal proceedings for conduct prohibited in the CFAA.

The CFAA has served as an important component of the online trust framework, giving the federal government authority to pursue cybercrimes including hacking and identity theft. However, vague terms in the law have fueled troubling civil actions that have stretched the application of the law well beyond that which Congress intended. That stretching of the law has spread to criminal cases under the CFAA as well, and a number of activities having little to do with the kinds of computer "trespasses" that originally motivated Congress to pass the CFAA are now potential crimes. Before it is further expanded or its penalties increased, the statute needs to be tightened and limited to the type of computer hacking activity it was intended to penalize so that it more clearly focuses on conduct that threatens cybersecurity. Only then should any expansion of CFAA penalty provisions be considered.

The CFAA imposes liability when a person accesses a computer without authorization or in excess of authorization. Courts have differed significantly on the definitions of "access" and "authorization." Some courts have interpreted unauthorized access so broadly that companies, when setting the terms of service few users will ever read, effectively determine what user conduct is "criminal." In *U.S. v. Nosal*,[35] the Ninth Circuit held just two months ago that a company's former employee violated the CFAA when he acquired information from the firm's computer network and then repurposed it for his own use, because the employer had not authorized that type of access to information on its network. This prompted one online publication to headline a story about the case "Appeals Court: No Hacking Required to Be Prosecuted as a Hacker."[36] While such activity might constitute theft, or a breach of an employment contract, it is certainly not the kind of conduct that should be addressed in a cybersecurity statute.

Similarly, in the 2008 Lori Drew case, a Missouri mother who impersonated a teenage boy on MySpace in order to taunt her daughter's teenage rival was charged in California under the CFAA after the girl committed suicide. The prosecutor's theory was that Drew exceeded authorized access because the MySpace Terms of Service did not allow users to create accounts under a false name. A federal judge overturned Drew's conviction under the CFAA.[37] While Drew's actions were reprehensible, they did not constitute "hacking" in any meaningful

[34] 18 U.S.C. § 1030.

[35] C.A. 9, 10-100038, April 28, 2011

[36] David Kravetz, Appeals Court: No Hacking Required to Be Prosecuted as a Hacker, *Wired: Threat Level* (April 29, 2011), http://www.wired.com/threatlevel/2011/04/no-hacking-required.

[37] The brief in which CDT joined in the Lori Drew case can be found here: http://www.eff.org/files/filenode/US_v_Drew/Drew_Amicus.pdf.

sense. Indeed, if violations of terms of service were per se violations of the CFAA, literally millions of otherwise law-abiding Americans could be subject to criminal prosecution for signing up for a service using a false name, misrepresenting their ages, or exceeding limits on storage capacity. Given that the Ninth Circuit called the result in *Drew* into question with its decision in *Nosal*, further prosecutions for this kind of terms of service violation may well happen.

Meanwhile, plaintiffs in civil cases continue to argue for an *even broader* understanding of unauthorized access. In one recent case, a pregnant mother who sued her employer for pregnancy discrimination was countersued under the CFAA for what the company asserted was unauthorized access to its computer systems: "excessive Internet use" in violation of its acceptable use policy.[38] In another, Sony sued users of its PlayStation devices under the CFAA for tinkering with their own lawfully purchased video game consoles without authorization from the in-box license.[39] Just as early civil cases on contractual authorization led to the questionable prosecutions in Nosal and Drew, so too do these cases point the way to additional dubious uses of the CFAA.

Instead of addressing this vexing problem of overbreadth, the White House proposal would enhance CFAA penalties, encouraging more questionable prosecutions. Penalties for first-time offenders would be increased and in some cases more than doubled. A new mandatory minimum three-year sentence would be imposed on those who, as a component of a felonious violation of the CFAA, damage or attempt to damage a critical infrastructure computer, as long as such damage would "substantially impair" the operation of that computer. The CFAA used to have mandatory minimum sentences, but they were repealed in Section 814(f)[40] of the USA PATRIOT Act in a section captioned "Deterrence and Prevention of Cyberterrorism." Before considering new mandatory minimums, an assessment should be made as to why the old ones were repealed.[41]

The White House proposal also makes the CFAA a RICO predicate – adding it to the list of crimes that can be used to demonstrate a "pattern of racketeering activity" to which severe criminal penalties could be applied. Notably, listing a crime under RICO allows civil plaintiffs to sue for triple damages for violations of that crime.[42] Because of the vagueness of the law, making the CFAA a RICO predicate could have the unintended consequence of making legitimate businesses subject to civil RICO suits for routine and normal activities. While such lawsuits may be legally groundless, their reputational impact and the prospect of treble damages and attorneys fees will often drive legitimate businesses into settling unsustainable charges. Moreover, such lawsuits would intensify the feedback loop between civil and criminal

---

[38] *Lee v. PMSI, Inc.*, 2011 WL 1742028 (M.D.Fla. 2011).

[39] Orin Kerr, Today's Award for the Silliest Theory of the Computer Fraud and Abuse Act, *The Volokh Conspiracy* (January 13, 2011), http://volokh.com/2011/01/13/todays-award-for-the-lawyer-who-has-advocated-the-silliest-theory-of-the-computer-fraud-and-abuse-act/.

[40] This section required the U.S. Sentencing Commission to "amend the Federal sentencing guidelines to ensue that any individual convicted of a violation of [18 U.S.C. § 1030] can be subjected to appropriate penalties, without regard to any mandatory minimum term of punishment." It also increased potential maximum penalties under the CFAA and broadened the conduct to which it applied.

[41] Orin Kerr, Congress Considers Increasing Penalties, Adding Mandatory Minimum Sentences to the Computer Fraud and Abuse Act, *The Volokh Conspiracy* (May 24, 2011), http://volokh.com/2011/05/24/congress-considers-increasing-penalties-adding-mandatory-minimum-sentences-to-the-computer-fraud-and-abuse-act/.

[42] 18 U.S.C. § 1964(c).

law that has led to the current overbreadth on the criminal side: as civil plaintiffs, newly incentivized to sue under the CFAA, continue to take novel theories to court, the set of activities which are considered criminal will likely continue to expand.

Finally, the proposal adds "real property" to items subject to civil forfeiture, as long as that property was used or was intended to have been used to commit or facilitate the crime. This would subject to forfeiture the house of the parents of a teenage hacker who has used a computer to attempt to break into someone's network if the parents were aware of this conduct.

The conduct constituting a violation of the CFAA must be narrowed before Congress considers legislation to extend the statute and enhance the penalties under it. As Professor Orin Kerr has suggested, the statute would be significantly improved by clarifying the definition of "authorization" to state that only actions exceeding *code-based* authorization are sufficient to constitute a violation.[43] Clarifying the meaning of "access" and "damage" under the statute would help as well. Even with such changes, however, some of the administration's proposals, such as mandatory minimum sentences for certain CFAA violations, would continue to raise concerns.

Conclusion

We appreciate the opportunity to testify about the White House cybersecurity proposals. They raise critical issues that fall squarely within the Judiciary Committee's jurisdiction and within the jurisdiction of the Subcommittee. We urge you to assert jurisdiction where appropriate, and we look forward to working with you to make progress on these important matters, while at the same time protecting the privacy rights of Americans.

[43] Orin S. Kerr, Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes, 78 *N.Y.U. L. Rev.* pp. 1596-1668 (November, 2003) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=399740.

Testimony of Julie Stewart
President, Families Against Mandatory Minimums (FAMM)

Hearing on
"Cybercrime: Updating the Computer Fraud and Abuse Act to Protect Cyberspace and Combat Emerging Threats"

Senate Judiciary Committee

September 7, 2011

Chairman Leahy, Ranking Member Grassley, and members of the committee, thank you for the opportunity to submit this statement on behalf of Families Against Mandatory Minimums (FAMM). FAMM is a national nonprofit, nonpartisan organization that supports sentencing laws that allow judicial discretion and maintain public safety.

We believe that sentences should be individualized, fair, and proportionate while advancing the purposes of sentencing: deterrence, public safety, just punishment, and rehabilitation. Our strong commitment to individualized sentencing compels us to oppose the new mandatory minimum sentence in the administration's Cybersecurity Legislative Proposal unveiled in May.

FAMM agrees with the proposal's purpose: The administration and members of Congress should work together to protect our nation's critical infrastructure in our new digital world. We simply disagree with the path the administration takes to get there.

18 U.S.C.§ 1030, commonly referred to as the Computer Fraud and Abuse Act (CFAA), presently includes several substantive offenses ranging from stealing classified national security information to trafficking in stolen electronic passwords. A person who "knowingly accesses a computer without authorization, or having accessed a computer without authorization, uses the opportunity such access provides for purposes to which such access does not extend," can be prosecuted under the CFAA. Conspiracies and attempts to violate any of these subsections are subject to be punished as if the offense had been completed. None of the punishments for these offenses currently include mandatory minimum sentences. Depending on which subsection is violated, sentences are calculated under the federal sentencing guidelines using U.S.S.G. §§ 2M3.2, 2B1.1, 2B2.3, or 2B3.2.

The administration's proposal increases the statutory maximum penalties for CFAA offenses. A violation of § 1030(a)(2), for example, which involves any type of unauthorized conduct involving any computer anywhere in the world, currently a misdemeanor, would become a felony punishable by up to three years in prison.

The proposal also adds a new section, § 1030A, to CFAA, entitled "Specific Criminalization of Damaging Critical Infrastructure Computers." It establishes a new three-year mandatory minimum sentence for anyone who "during and in relation to a felony violation of section 1030 ... knowingly causes or attempts 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 of the operation of the critical infrastructure computer or of the critical infrastructure associated with such computer." (Proposed 18 U.S.C. § 1030A(a)(1).)

The new mandatory minimum sentence is to be added to any punishment imposed for an underlying felony violation of 18 U.S.C. § 1030. The proposal further requires that "in determining any term of imprisonment to be imposed for the felony violation of Title 18, United States Code, Section 1030, a court shall not *in any way* reduce the term to be imposed for such crime *to compensate for, or otherwise take into account*, any separate term of imprisonment imposed or to be imposed for a violation" of section 1030A. (Proposed 18 U.S.C. § 1030A(b)(3) (emphasis added).)

FAMM has three main concerns with the sentencing provisions in the administration's proposal.

1. We believe that increasing criminal penalties, especially pursuant to a mandatory minimum sentencing provision, requires extreme caution when the activities prohibited by the law are not clearly defined or understood;
2. We have concerns about the language that forbids courts from reducing punishments for 1030 violations when a mandatory term required by 1030A is triggered; and
3. Finally, we vigorously oppose the creation of a new mandatory minimum sentence as set forth in the proposed 1030A.

Combination of vague criminal laws and steep penalties heightens concerns

We are concerned that the administration's proposal adds new penalties on what some commentators have decried as the vague prohibitions in the existing CFAA (§ 1030).[1] FAMM is pleased to be a member of the Overcriminalization Working Group and recently joined The Heritage Foundation, Texas Public Policy Foundation, Washington Legal Foundation, and National Association of Criminal Defense Lawyers as sponsors of the "Criminal Checklist for Federal Legislators." One of the first questions we recommend that lawmakers ask themselves when proposing a new criminal statute is whether the law provides sufficient notice to individuals about the conduct the law seeks to prohibit. This notice is required by the Due Process Clause of the Fifth Amendment to the Constitution. Without clear notice, well-intentioned citizens can run afoul of the law without even trying. We agree with U.S. Supreme Court Justice Scalia's statement, "It is simply not fair to prosecute someone for a crime that has not been defined until the judicial decision that sends him to jail."[2]

With regard to the administration's cybersecurity proposal, a three-year mandatory minimum is imposed for violations of the new § 1030A. This penalty is added to whatever penalty is imposed for violations of § 1030. This poses two problems. First, as mentioned, § 1030 appears to be a fairly broad statute, having been used by creative prosecutors in the last few years to charge as unauthorized access or exceeding authorized access (1) an individual's violation of MySpace's

[1] See, e.g. Kerr, Orin S., *Vagueness Challenges to the Computer Fraud and Abuse Act* (December 22, 2009). Minnesota Law Review, 2010 ; GWU Legal Studies Research Paper No. 482; GWU Law School Public Law Research Paper No. 482.
[2] Sorich v. United States, 129 S. Ct. 1310 (2009) (Scalia, J., dissenting from denial of certiorari).

Terms of Service and (2) an employee's use of an employer's computer in a manner contrary to the employer's interest. Second, the administration's proposal increases penalties for § 1030 violations, upgrading them from misdemeanors to felonies. Thus, the mandatory minimum imposed by § 1030A will be added to the now-felony level sentence imposed for violations of § 1030, a vague statute.

For FAMM, the greatest risk to individuals comes from a combination of vague laws and severe and mandatory penalties. To continue Justice Scalia's thought, the only thing more unfair than prosecuting someone for a crime that has not been defined until the judicial decision that sends him to jail is to send him to jail for a lengthy, mandatory sentence.

§ 1030(b)(3) contravenes spirit of Booker

FAMM is concerned about language in § 1030(b)(3) that bars courts from reducing criminal punishments for § 1030 violations in consideration of the mandatory minimum required by § 1030A. It could transform the guidelines governing these offenses from their current status as advisory to mandatory when coupled with the proposed mandatory minimum. This reading suggests it would violate *United States v. Booker*. In *Booker*, the Court ruled that the U.S. Sentencing Guidelines are advisory in order to comply with the Sixth Amendment's protection of the right to a jury trial. Under *Booker* and its progeny, courts can vary up or down from a guideline sentence to comply with the purposes of punishment and sentencing considerations in 18 U.S.C. § 3553(a). The § 3553(a) factors include the following, which the court "shall consider":

> (3) *the kinds of sentences available*;
>
> (4) *the kinds of sentence and the sentencing range established for*
>
> (A) *the applicable category of offense* committed by the applicable category of defendant as set forth in the guidelines—
>
> (i) issued by the Sentencing Commission pursuant to section 994(a)(1) of title 28, United States Code, subject to any amendments made to such guidelines by act of Congress (regardless of whether such amendments have yet to be incorporated by the Sentencing Commission into amendments issued under section 994(p) of title 28); and
>
> (ii) that, except as provided in section 3742(g), are in effect on the date the defendant is sentenced.[3]

The paramount mandate to the court is that it impose a sentence "sufficient, but no greater than necessary to" comply with the purposes of punishment.[4]

[3] 18 U.S.C. § 3553(a)(3), (4) (emphasis added).

The proposed § 1030(b)(3) is problematic because it would render the guidelines mandatory under a specific set of circumstances, that is when a defendant violates §1030A.[5] In that circumstance, the court would have to impose a mandatory three-year sentence under §1030A which would run consecutive to the sentence imposed for the underlying violation of § 1030. The § 1030 sentence would be a guidelines-based sentence but would be rendered essentially mandatory under these circumstances because it could not be reduced in consideration of the mandatory consecutive critical infrastructure sentence. The Supreme Court has rejected such cherry picking, in *Booker* and most recently in *Pepper v. United States*, 131 S. Ct. 1229 (2011). In *Booker* the court invalidated the mandatory nature of the guidelines, even though their application would not always produce the Sixth Amendment violations that often occurred with mandatory guidelines. As the Court in *Pepper* explained:

> although the Government suggested in Booker that we render the Guidelines advisory only in cases in which the Constitution prohibits judicial factfinding, we rejected the two-track proposal, reasoning that "Congress would not have authorized a mandatory system in some cases and a non-mandatory system in others . . . . ."[6]

In *Dillon v. United States*, 130 S. Ct. 2683 (2010), the Court reiterated the theme, stating, "[t]he incomplete remedy we rejected in *Booker* would have required courts to treat the Guidelines differently in similar proceedings, leading potentially to unfair results and considerable administrative challenges."[7] Most recently, in *Pepper*, the Supreme Court once again struck down a scheme that would have rendered part of the guidelines mandatory under a limited set of circumstances.

Based on the language and context of § 1030A(b)(3), the apparent intent is to make the guidelines for a § 1030 violation mandatory when coupled with a conviction under § 1030A. Read this way, § 1030A(b)(3) could be deemed inconsistent with *Booker*.

It would also require courts to ignore the parsimony mandate in federal law that requires a judge to impose a sentence no greater than necessary to comport with the purposes of punishment in 18 U.S.C. § 3553(a). In cases where the three-year mandatory minimum would drive the overall sentence beyond that necessary, judges would have no way to ameliorate the undue harshness of the overall sentence.

The provision is both unwise and unjust and would, at best, invite time consuming litigation in an area where the Supreme Court has been extremely active.

---

[4] 18 U.S.C. § 3553(a).
[5] In fact a § 1030A offense is always accompanied by its predicate §1030 offense and so in every case where a defendant is convicted of damaging critical infrastructure computer he would be subject to a three year mandatory and consecutive sentence on top of a mandatory guideline sentence.
[6] *Pepper v. United States*, 131 S. Ct. 1244 (2011)
[7] *Dillon v. United States*, 130 S. Ct. 2693 (2010)

New mandatory minimum in proposed 1030A is unwarranted and unwise

Statutory mandatory minimums are often seen as a solution to address the apparent disparities that are created when seemingly similar defendants receive different sentences. Mandatory minimums, their proponents claim, help to eliminate disparity by ensuring that like offenders are treated alike. They are also promoted to ensure that tough sentencing is not undermined by lenient jurists.

As H.L. Mencken once said, "There is always an easy solution to every human problem – neat, plausible, and wrong." Mandatory minimum sentences, while a neat and even plausible response to sentencing disparities, were and are the wrong solution.

Mandatory minimums take a charge-centered approach to sentencing. Conviction for certain crimes results in a pre-determined and generally inescapable sentence. Historically, they have been considered necessary to deter would-be criminals, incapacitate offenders, and promote uniformity of punishment for similarly situated defendants. As originally designed, the only way a defendant could receive a sentence below the mandatory minimum was if he cooperated to the satisfaction of the prosecution, who held the power to move the court for a downward departure for "substantial assistance."

Mandatory minimum sentencing is plagued with problems and has led to extraordinary injustice. Intended to, among other things, reduce unwarranted disparity among similarly situated defendants, it has instead produced both unwarranted uniformity and disparity. Mandatory minimums rely on a limited number of factors to capture the entire measure of blameworthiness. For example, in drug offenses, the *type* and *weight* of a drug is alone sufficient to trigger a mandatory minimum sentence. The type and quantity of drugs are, however, poor proxies for culpability, because very different offenders, with varying degrees of culpability, can be subject to the same mandatory minimum sentence. This unwarranted uniformity means that a drug "mule" carrying a backpack filled with drugs on several occasions, for relatively small amounts of remuneration, receives the same sentence as the drug kingpin, who arranges the trips and enjoys enormous profits. In its 1991 study of mandatory minimums, the United States Sentencing Commission called the exaggerated role of drug quantity the "tariff" effect, and criticized it for prohibiting the consideration of traditional sentencing factors.[8]

The damage caused by mandatory minimum sentencing laws is not abstract. Over the past 20 years, FAMM has collected thousands of personal stories of individuals who have received inarguably unjust sentences due to state and federal mandatory minimums. Consider, for example, the cases of:

---

[8] The preceding two paragraphs are taken from FAMM Vice President and General Counsel Mary Price's article, Price, Mary. *Everything old is new again: fixing sentencing by going back to first principles*. 36 New Eng. J. on Crim. & Civ. Confinement 75-97 (2010). Please see the article for citations to primary sources.

- Orville Lee Wollard, a married father of two who was sentenced to 20 years in Florida state prison for defending his family and home with a gun. Though no one was hurt and the judge agreed that the sentence was excessive, his ability to impose a shorter sentence was eliminated by a mandatory minimum law.[9]
- Stephanie Nodd, a 23-year-old Alabama woman who was sentenced to 30 years in federal prison for a one month stint helping her boyfriend sell crack cocaine. Ms. Nodd has already served more than 21 years.[10]

The proposed mandatory minimum sentence in the Computer Fraud and Abuse Act (CFAA) is likely only to add more names to those who suffer the unintended consequences of mandatory minimum sentencing.

The mandatory minimum sentencing regime has had the effect of transferring discretion from judicial to prosecutorial control. Prosecutors control what crime to charge and which sentencing factors to bring to the court's attention, whether to drop a charge or "fact bargain" sentencing elements, and whether to charge a crime that carries a mandatory minimum sentence or one that does not. All of those decisions are made away from the public record and are unreviewable.

Mandatory minimums sentences also drive enormous prison costs. There are 171 statutes with mandatory minimums in the federal code. In 2008, 21,023 people were sentenced to 31,239 counts of conviction carrying mandatory minimum sentences. If each person were sentenced to the lowest mandatory minimum (five years), they would serve a cumulative sentence of 105,115 years at an average cost of $28,000 per person per year. Of course, the mandatory minimum sentences range from five years to ten, fifteen, twenty, and even life. So-called "stacking provisions" of 18 U.S.C. § 924(c) can generate sentences for first-time offenders of 25, 50, or 150 years, or more. Mandatory minimums cause other unintended, but very real, consequences beyond the daily and personal injustice of subjecting many defendants to sentences that are too long. They contribute to overincarceration.

As Federal Public Defender Michael Nachmanoff testified before the U.S. Sentencing Commission in 2009:

> [t]he federal prison population is currently at 206,786 inmates, a nearly five-fold increase since mandatory minimums and mandatory guidelines became law. The major cause of

---

[9] For more information on Orville Lee Wollard's case, see my *Washington Times* op-ed published on June 9, 2011, *available at* http://www.washingtontimes.com/news/2011/jun/9/second-amendment-injustice/ (last visited September 6, 2011).

[10] Ms. Nodd's sentence was driven higher than the mandatory minimum under the sentencing guidelines. However, her arbitrarily high guideline level was the result of the severe statutory mandatory minimum. For more information on Ms. Nodd, see her op-ed published in the *Chicago Tribune* on July 28, 2011, *available at* http://articles.chicagotribune.com/2011-07-28/site/ct-oped-0728-crack-20110728_1_federal-prison-crack-cocaine-drug-conspiracy (last visited September 6, 2011).

> the prison population explosion is the increase in sentence length for drug trafficking, from 23 months before the guidelines to 73 months in 2001. About 75% of this increase was due to mandatory minimums, and 25% was due to guideline increases above mandatory minimum levels. Today, the average sentence length for drug trafficking is even higher than in 2001, at 83.2 months.[11]

Since Mr. Nachmanoff delivered his testimony two years ago, the federal prison population has climbed to over 215,000 and the average cost to incarcerate an offender is $28,000. Add in state, county and local prisons and jails and the total number of individuals incarcerated in the United States hits 2.3 million.

For all of these reasons, opposition to mandatory minimum sentencing laws is growing, including in some unexpected quarters. In the past couple of years, numerous high-profile national conservative leaders have expressed opposition to mandatory minimum sentencing laws. Americans for Tax Reform President Grover Norquist, American Civil Rights Institute President Ward Connerly, National Rifle Association President David Keene, and Justice Fellowship President Pat Nolan have called mandatory minimum sentences into question.

More recently, these conservative leaders joined former House Speaker Newt Gingrich, former Attorney General Ed Meese, Family Research Council President Tony Perkins, former Florida governor Jeb Bush, former drug czar Bill Bennett and others to form Right on Crime, a group dedicated to achieving a cost-effective criminal justice system that "protects citizens, restores victims, and reforms wrongdoers." Included in the group's proposals for reform is a call to consider "eliminating many mandatory minimum sentencing laws for nonviolent offenses. These laws remove all discretion from judges who are the most intimately familiar with the facts of a case and who are well-positioned to know which defendants need to be in prison because they threaten public safety and which defendants would in fact not benefit from prison time."[12]

Nearly all of the arguments against mandatory minimums generally can be applied specifically to the administration's proposal for a new mandatory minimum sentence for certain computer fraud offenses.

To the best of our knowledge, the administration has not sufficiently set forth any evidence that serious attacks on our nation's critical infrastructure are being punished too lightly or that the threat of mandatory, longer prison sentences would deter the individuals most likely to perpetrate

---

[11] Federal Public Defender written testimony at 5 (July 9, 2009), available at http://www.ussc.gov/Legislative_and_Public_Affairs/Public_Hearings_and_Meetings/20090709-10/Nachmanoff_testimony_updated.pdf (last visited September 6, 2011).

[12] Right on Crime, Right on Crime, *The Conservative case for reform: fighting crime, prioritizing victims, and protecting taxpayers*, http://www.rightoncrime.com/priority-issues/prisons/ (last visited September 6, 2011).

such attacks. Instead, the administration proposed a new three-year mandatory minimum on the grounds that the targeted conduct was very harmful.

We appreciate the historical role that the White House, in consultation with the Department of Justice, plays in proposing strategies and plans to combat emerging national security and criminal threats. However, we think these Executive Branch leaders and Congress have an obligation to conduct, or rely on the U.S. Sentencing Commission to conduct, careful study before proposing or adopting new sentencing policies.

With regard to administration's cybersecurity proposal in particular, we think the public has a right to know the following in relation to the new mandatory minimum:

- Why was the specific prison term – three years – chosen for the offense? What factors did the administration consider and deem relevant?
- What is the average sentence currently imposed for the offense?
- What is the recidivism rate for individuals who commit the offense? and
- Is there evidence to suggest that courts are failing to punish this crime appropriately? If so, what is it?

Conclusion

Finally, Chairman Leahy and Ranking Member Grassley, we want to make an obvious but important point: the administration's cybersecurity proposal does not exist in a vacuum. If the administration's bill is enacted, we can then expect future proposals to increase penalties for other crimes and note the penalties provided by this bill as a point of comparison. In this way, federal sentencing operates like a one-way ratchet, with sentences getting longer and longer even where no purpose of punishment is served by the increases.

Thank you for the opportunity to share our views with the committee, and please do not hesitate to contact me if FAMM can provide additional information or answer any questions.

THE WALL STREET JOURNAL.
WSJ.com

September 7, 2011, 10:53 AM GMT

One Million Victims of Cybercrime a Day Says Report

Over one million adults around the world are the victim of cybercrime every day, according to figures published Wednesday.

The Norton Cybercrime Report 2011 paints a gloomy picture. The company estimates that cybercrime cost online consumers over the 24 countries surveyed a total of $388 billion in just one year. By contrast, according to Adam Palmer, Lead Advisor at Norton Cybersecurity Institute and a former U.S. Navy prosecutor, the entire global trade in cocaine, heroin and marijuana is worth $288 billion.

Globally, the most common—and most preventable—type of cybercrime is computer viruses or malware. The next two most prevalent were online scams and phishing.

All told, Symantec estimates that there are 431 million victims a year. Your chances of being a victim of cybercrime (44% of people reported being a victim) are substantially greater that being a victim of a physical crime (15%).

Those rates vary quite dramatically globally. According to Mr. Palmer, Chinese users are far more likely to suffer an attack. Some 85% of Chinese users were victims, compared to just 38% of Japanese.

European figures show Germans and Poles to be the most likely victims of cybercrime among the nations surveyed.

1. Germany **76%**
2. Poland **76%**
3. Switzerland **73%**
4. Spain **69%**
5. Italy **68%**
6. France **60%**
7. Sweden **60%**
8. Denmark **57%**
9. U.K. **51%**
10. Belgium **50%**
11. The Netherlands **41%**

In all countries surveyed, men were more likely to be victims than women, and the report identifies the riskier behaviors associated with becoming a target for cybercriminals:

1. Viewing adult content online (80% cf. 67% non-viewers of adult content).
2. Lying online (78% cf. 59% who don't lie online).
3. Using free Wi-Fi (77% cf. 62% who don't use free Wi-Fi).

A large share of the cybercrime burden is shouldered by emerging markets, with cybercrime costing China £16 billion ($25.8 billion), Brazil £9.5 billion and India £2.5 billion in the past twelve months.

The growing importance of mobile phones and mobile Internet in these markets plays a key role. While globally 10% of online adults have experienced cybercrime on their mobile phone, this triples to 31% in China where nearly three quarters of respondents (74%) access the Internet via their mobile phone.

Symantec carried out the research in 24 countries conducting 19,636 interviews.