MICHAEL M. DUBOSE
Chief
Computer Crime & Intellectual Property Section
Criminal Division - Department Of Justice

Presented to the
United States Sentencing Commission
Public Hearing on the Identity Theft Restitution and Enforcement Act of 2008

MARCH 17, 2009

Chairman Hinojosa, distinguished members of the Commission — thank you for inviting the Department of Justice to present testimony today on the Identity Theft Restitution and Enforcement Act of 2008 ("ITERA"). It is a pleasure to appear before you again.

Section 209 of ITERA directs the Commission to "review its guidelines and policy statements applicable to persons convicted of offenses under §§ 1028, 1028A, 1030, 2511, and 2701 of Title 18, United States Code, and any other relevant provisions of law, in order to reflect the intent of Congress that such penalties be increased in comparison to those currently provided by such guidelines and policy statements," in light of several enumerated factors. The Federal Register notice contains several proposed amendments to the guidelines as well as a number of issues for comment corresponding to the factors identified in § 209 of ITERA.[1]

Background

In 2003, the Commission last reviewed the Sentencing Guidelines applicable to cybercrime and other related crimes such as identity theft. *See* United States Sentencing Commission, *Report to Congress: Increased Penalties for Cyber Security Offenses* (May 2003) ("*Cyber Security Report*"). Since that time, the landscape of cyber and identity theft crime has changed significantly. For example, in 2003, the Commission cited data suggesting that "many 18 U.S.C. § 1030 offenses are relatively unsophisticated." *See Cyber Security Report*, at 8. The same cannot be said today.

The Commission held a public briefing session on November 20, 2008. At that briefing, the Department advised the Commission that cyber-criminals are increasingly using sophisticated technological tools like "proxies" to evade detection and prosecution by taking advantage of the difficulties faced by law enforcement in conducting investigations involving multiple U.S. and foreign jurisdictions. *See* Michael DuBose, *Measuring Harm in Cybercrime and ID Theft Cases* (PowerPoint Presentation to the United States Sentencing Commission, November 20, 2008) ("*CCIPS Presentation*"), at slides 5-6. The increasing sophistication of cyber-crime was also

[1]The Department supports the adoption of the Commission's proposed Technical Amendments, *see* Proposed Amendments to the Sentencing Guidelines, pp. 22-24 (Subsection "O").

emphasized by the representative of the Business Software Alliance ("BSA"), who informed the Commission at that same briefing that:

> [C]ybercrime is increasingly technologically sophisticated. Because cybercrime has become a profession, and because it is financially motivated, criminals have a tremendous incentive to innovate. In particular, the rise of vast surreptitiously controlled computer networks called "botnets," has led to an explosion in the number and types of cybercrime committed . . . .

Bruce J. Heiman, *Written Testimony of the Business Software Alliance on Implementing the Identity Theft Enforcement and Restitution Act of 2008* (November 20, 2008) ("*BSA Written Testimony*"); *see also* Business Software Alliance, *The Fight for Cyberspace: High Tech and Law Enforcement Experts on Defeating Today's Cyber Criminals* (2007), available at http://www.bsa.org/~/media/9CA4C9DFEDE24250AA16F16F0ED297A6.ashx. Additionally, cybercriminals are no longer isolated actors, but now employ a division of labor that "span[s] continents." *BSA Written Testimony*, at 4. As noted by the BSA, "[t]he criminals themselves may be in one country but control 'zombie' computers in virtually every region of the world." *Id*.

The growing opportunity for financial gain combined with increased technological sophistication has resulted in an explosion of cybercrime and identity theft. Since 2003 – when the Commission provided the *Cyber Security Report* to Congress – there has been a rash of large scale data breaches involving major financial institutions such as Citigroup, large retailers such as TJ Maxx, and global leaders in information management services such as Acxiom, each affecting tens of millions of individuals. *CCIPS Presentation*, at slides 4, 8-10. And 2008 saw a sharp rise in the number of reported data breaches from the previous year. *CCIPS Presentation*, at slide 3. The United States now experiences 30% of all malicious cyber-activity in the world, more than any other country, and Americans now face a one-in-four chance of becoming a victim of cyber-crime. *See BSA Written Testimony*, at 4 (*citing* the 2007 Consumer Reports "*State of the Net*" survey). Indeed, according to the FTC, identity theft became the fastest growing crime in 2008, affecting 10 million Americans, an increase from 8 million reported victims in 2005. *See* Senator Patrick Leahy, *Statement On Passage Of The Former Vice President Protection Act of 2008, H.R. 5938* (September 15, 2008); and http://www.sun-sentinel.com/business/custom/consumer/ sfl-flhlpidpredictions1230sbdec30,0,928121.story.

In response to this changing landscape, the Senate passed the cyber-crime provisions of ITERA, signed into law in September 2008. As Senator Leahy noted at the time of its passage by the Senate, ITERA was intended to provide law enforcement with additional tools to wage a more aggressive fight against identity theft and cyber-crime. Among the explicit recommendations considered by Congress to fight this explosion of cyber-crime was "stiffening the penalties to deter potential cyber-criminals," which ITERA accomplishes by "direct[ing] the Sentencing Commission to review its guidelines for identity theft and other cyber-crimes." Senator Patrick Leahy, *Statement On Passage Of The Former Vice President Protection Act of 2008, H.R. 5938* (September 15, 2008).

Congress recognized the growing sophistication and scale of cyber-crime and that the

changes the Commission made to sentencing policy in this area in 2003 are now inadequate to address the current cyber-crime threat. The clear and unambiguous intent of Congress is for the Commission to revisit the guidelines pertaining to cyber-crime and identity theft and stiffen the existing penalties where appropriate.

A. Level of Sophistication and Planning of the Offense.

Sophisticated Means Enhancement (USSG §2B1.1(b)(9))

The Federal Register notice recognizes the need to clarify "whether, in a case involving computers, the defendant's use of any technology or software to conceal the identity or geographic location of the perpetrator, qualifies as 'especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense'" under the Sophisticated Means Enhancement, USSG §2B1.1(b)(9) & Application Note 8. Proposed Amendments to the Sentencing Guideline ("*Reader Friendly*"), at 6. The Commission's proposed amendment addresses this concern by adding the following clarifying language to application note 8(B): "In a scheme involving computers, using any software or technology to conceal the identity or geographic location of the perpetrator ordinarily indicates sophisticated means." *Id.* The Department strongly supports this proposed amendment.

The use of proxies by cyber-criminals is of increasing concern to law enforcement. Proxies are a technology used by cyber-criminals to make it appear as if communications over the Internet are originating from a computer other than the computer used by the perpetrator. *See CCIPS Presentation*, at slides 5-6. Proxies are often created by infecting victim computers with malicious software that permits the cyber-criminal to use the victim computer as a proxy without the owner's knowledge or consent. Because the proxy is typically located in a different U.S. or foreign jurisdiction than the perpetrator, law enforcement authorities must spend significant time and resources attempting to ascertain the correct identity and geographic location of the perpetrator, frustrating the investigation and prosecution of cyber-criminals.

The current language of the Sophisticated Means Enhancement under §2B1.1(b)(9), Application Note 8(B) – applying to "especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense" – is plainly broad enough to cover crimes involving sophisticated technologies such as proxies which are used to evade detection and prosecution. However, given the increasing prevalence of computer crimes involving the use of proxies, probation officers and sentencing judges will need to decide whether computer technologies such as proxies qualify as "sophisticated means" under §2B1.1(b)(9). Since most judges and probation officers may not be familiar with such sophisticated computer techniques, the proposed amendment will prevent any confusion by reflecting the Commission's unambiguous intent to include such sophisticated techniques within the scope of the enhancement.

Moreover, the Commission's proposed amendment fits neatly within the structure and meaning of Application Note 8(B), which already includes examples of "sophisticated means" commonly used in criminal schemes: the use of offices in multiple jurisdictions, shell corporations,

fictitious names, and offshore accounts. The use of proxies to mask the true location of a hacker's computer is essentially analogous to the use, in a fraud scheme, of offices in multiple jurisdictions; both techniques make it more difficult for law enforcement to detect and prosecute offenders because they take advantage of jurisdictional boundaries to confound investigators. Consequently, the Commission's proposed amendment does not alter the scope of the enhancement, but rather clarifies the Commission's intent to include sophisticated computer techniques such as proxies within the scope of §2B1.1(b)(9).

Finally, the proposed amendment appropriately uses technology-neutral language. Such language obviates any concern that the rapid pace of technological change will quickly lead to the amendment's obsolescence. By making it clear that the enhancement applies to "any software or technology to conceal the identity or geographic location of the perpetrator" (*Reader Friendly*, at 6), the Commission ensures that the inevitable development of other technologies to conceal the identity and location of cyber-criminals will not require further revision of the guidelines.

The Commission has also invited comment on whether the present 2-level enhancement under §2B1.1(b)(9) sufficiently addresses Congress' concern that the guidelines adequately reflect the level of sophistication and planning of the offense. We believe it does.

Abuse of Position of Trust or Use of Special Skill (USSG §3B1.3)

The guidelines currently provide for a 2-level increase "[i]f the defendant abused a position of public or private trust, or used a special skill, in a manner that significantly facilitated the commission or concealment of the offense . . . ." USSG §3B1.3. The Commission has invited comment as to whether this enhancement "should apply to a person who has self-trained computer skills." *Reader Friendly*, at 7. The Department believes the enhancement should apply in these circumstances.

It is important to recognize that the skills acquired by carders – those who steal, resell, and commit fraud using credit and debit card account numbers – and hackers are not possessed by the general public, and are also typically not acquired through formal education or training. Criminal hackers and carders generally learn by talking with other criminals and posting information on underground internet forums, as well as through direct experience. The fact that these skills do not come with a diploma does not lessen the impact or seriousness of the crimes they make possible. For these reasons, the Department opposes any revisions to the guidelines which exclude self-taught skills from the scope of the Special Skills Enhancement under §3B1.3.

This position is supported by the present language of §3B1.3 and Application Note 4. The guideline itself only requires that the "special skill" be used "in a manner that significantly facilitated the commission or concealment of the offense." USSG §3B1.3, Application Note 4 limits such special skills to those "not possessed by members of the general public." Three Circuit Courts of Appeals have decided that while Application Note 4 states that the enhancement applies to those skills "usually requiring substantial education, training, or licensing," the Commission's use of the word "usually" reflects an intent not to exclude self-taught skills from the scope of the enhancement.

United States v. Urban, 140 F.3d 229, 235 (3d Cir. 1998) (self-taught bomb making skills qualified as special skill). *See also, United States v. Lavin*, 27 F.3d 40, 41 (2d Cir. 1994) (installation of equipment on ATM machines permitting theft of account numbers and creation of counterfeit ATM cards qualified as special skill); *United States v. Petersen*, 98 F.3d 502, 506-07 (9th Cir. 1996) (self-taught computer abilities were special skill). This interpretation follows the plain meaning of the guidelines. Consequently, limiting §3B1.3 to formally acquired skills might require the Commission to revise the present scope of the guidelines, which would impact cases beyond the realm of those impacted by ITERA.

The Department would welcome an amendment to clarify that skills which are self-taught, or otherwise acquired without formal education, can qualify as "specials skills" under the enhancement.

B. Whether the Offense Was Committed For the Purpose of Commercial Advantage or Private Financial Benefit.

Congress directed the Commission to consider whether the guidelines adequately account for identity theft and computer crimes motivated by commercial gain. Several guidelines provisions identified in the Federal Register Notice – §§2B1.1 (economic crimes, including identity theft and cyber-crime, and unauthorized access of stored communications), 2B2.3 (trespass, including computer trespass), and 2B5.3 (criminal copyright infringement) – already impose proportional sentences based on the monetary loss caused, and thus we believe these guidelines adequately take into account a motive for commercial gain. However, we believe §2H3.1 does not adequately account for wiretapping offenses committed for commercial gain.

Section 2H3.1 (Interception of Communications)

Advances in technology have made it easier to conduct illegal electronic wiretaps, and criminals have taken advantage of the technologies to sell wiretapping services to others for their own pecuniary gain. The Department is concerned that these increasingly prevalent crimes are not adequately deterred and punished under the current guidelines.

Section 2H3.1 currently imposes a 3-level increase if "the purpose of the offense was to obtain direct or indirect commercial advantage or economic gain . . . ." For cases in which the economic gain exceeds $10,000, this sentencing enhancement is less severe than the graduated sentencing enhancements imposed under the loss table in §2B1.1. This results in unwarranted sentencing disparities between defendants convicted of computer crimes and other frauds with a financial purpose and those convicted of wiretapping *with the exact same purpose*. For example, in 2005, the creator and seller of a program named Loverspy, designed to collect personal information surreptitiously from target computers, was indicted on numerous charges, including computer hacking and illegal wiretapping. The program was sold for a price of $89 to over 1000 purchasers, and the scheme affected more than 2000 victims. *See* China Martens, "'Loverspy' Spyware Creator Indicted, On the Run," *PC World.com* (August 29, 2005), available at http://www.pdesign.net/SED/SED%20Articles/Loverspy%20Spyware%20Creator%20Indicted,%20On%20The%20Run.htm.

Had the defendant broken into computers and stolen sensitive *stored* information causing losses of $89,000, he would be exposed to an adjusted offense level of 14 (a base level of 8 plus a 6-level enhancement based on the loss amount, resulting in guidelines range in Zone D for a first offender). Because he earned $89,000 by assisting others to steal sensitive information *in transit* (illegal wiretapping), the guidelines range under §2H3.1 was only 12 (base level of 9 plus a 3-level enhancement because the crime was motivated by commercial gain, resulting in a guidelines range in Zone C for a first offender), despite an identical financial purpose. This disparity rapidly increases as the commercial motive increases (as measured in dollar amounts). There is no good reason for this result. Indeed, as the Loverspy case illustrates, technology permitting wiretapping offenses is readily available in the marketplace, and conduct involving illegal wiretapping requires the same deterrence and punishment as other offenses.

The Department believes this disparity should be corrected with a mechanism similar to that in the guidelines §§2B2.3 (trespass, including computer trespass) and 2B5.3 (criminal copyright infringement) which impose sentences based on the loss table in §2B1.1(b)(1). The Commission should amend §2H3.1 to include an enhancement based on the defendant's gain as measured by amounts listed in the loss table.

C. The Potential and Actual Loss Resulting from the Offense Including (A) the Value of the Information Obtained from a Protected Computer, Regardless of Whether the Owner Was Deprived of the Use of the Information; and (B) Where the Information Obtained Constitutes a Trade Secret or Other Proprietary Information, the Cost the Victim Incurred in Developing or Compiling the Information

Definition and Estimation of Loss (USSG §2B1.1, Application Notes 3(A)(v)(III) and (C))

Section 2B1.1 is the principal guideline provision for computer offenses involving the theft of information as well as for offenses involving theft of trade secrets. The guidelines provide a specific rule of construction for cases brought under 18 U.S.C. § 1030. This rule includes remedial costs within the definition of actual losses sustained as a result of the offense, in addition to the direct financial losses typically taken into account under §2B1.1. *See* USSG §2B1.1, Application Note 3(A)(v)(III). There is no similar rule of construction that applies to trade secret cases. However, the guideline does provide a list of factors for estimating loss in all cases covered by the guideline. This list permits courts to consider a list of non-exclusive factors, including but not limited to the fair market value of the information. *See* Application Note 3(C). The use of fair market value in estimating loss applies, by the terms of Application Note 3(C), to "property unlawfully taken or destroyed," and where calculating fair market value is not feasible, courts can consider replacement cost as a measure of loss. Application Note 3(C)(i).

The Department believes that these provisions – geared to typical economic crimes such as fraud, theft, or damage to property – fail to address an important class of offenses involving the theft of information. Some of these are computer hacking offenses involving large scale data breaches,

such as the Axciom case described by the Department at the Commission's November 20, 2008 public briefing. *See CCIPS Presentation*, at slides 8-10; *see* <u>*also*</u> *United States v. Levine*, 477 F.3d 596 (8th Cir. 2001). Others involve the theft of valuable trade secrets. *See e.g.*, *United States v. Ameri*, 412 F.3d 893, 900 (8th Cir. 2005); *United States v. Four Pillars Enterprises Company, Ltd.*, 253 Fed. Appx. 502, 512 (6th Cir. 2007).

In each of these instances – data-breaches and theft of trade secrets – §2B1.1 fails to take into account two significant factors which make crimes involving the theft of information different from other economic crimes such as fraud and theft or damage to property. *First*, unlike those crimes, the theft of information usually involves the copying of information, and thus does not deprive the owner of the use of that information. However, the guideline restricts consideration of fair market value in calculating loss to situations in which "property" is "taken or destroyed" – a formulation that is ambiguous and can be construed as inapplicable to situations in which information is merely copied. The value of the stolen information is an appropriate measure of the seriousness of the offense, even if the victim was not deprived of its use, because it reflects the scale of the criminal conduct. If the fair market value of information cannot be used to estimate loss in theft of information cases, courts may impose sentences that tend to understate the seriousness of such offenses.

Second, even if courts conclude that they may consider the fair market value of copied information as a measure of loss, there are certain types of stolen information for which it may be difficult or impossible to ascertain a fair market value. Some types of information, such as a customer list, have a market value that can be established at trial through expert testimony or by introducing evidence that the offender sold it to another person. However, other types of information – for example trade secrets, strategic business plans, or programming source code – might not have readily ascertainable market values. In cases involving trade secrets and other types of information that are difficult to value, the Department believes that development costs can provide an appropriate measure of offense severity. Trade secrets are, by definition, valuable to the company that develops them so long as they remain secret. A company that invests resources in developing a trade secret does so anticipating that the information will remain confidential. Theft of those secrets and disclosure to one or more competitors can destroy the expected profit, and thus the anticipated benefit of investing in the secret. A company would not have invested the resources to develop the trade secret, or deployed those resources elsewhere, if it knew that secrecy would be breached. Consequently, using development costs in determining loss makes sense.

The Commission offers two alternative proposals for revising §2B1.1 to address this problem. The first proposal ("Option 1") would revise the rule of construction in Application Note 3(A)(v)(III) to include "any reduction in the value of proprietary information (*e.g.*, trade secrets) that resulted from the offense" within the definition of actual loss. *Reader Friendly*, at 9. The alternative proposal ("Option 2") would amend Application Note 3(C) to permit courts to consider (i) the fair market value of the information where the information is copied, and (ii) development costs or diminution in the value of the information in the case of proprietary information such as trade secrets. *Id.* 9-10. Of these two alternatives, the Department strongly

supports the adoption of Option 2.

The Department believes that Option 1 contains two principal flaws. *First*, this proposal only revises Application Note 3(A)(v)(III), a rule of construction limited solely to § 1030 offenses. Because of this limitation, the revision would not apply to an important class of cases which are of equal concern to the Department – trade secret cases brought under 18 U.S.C. §§ 1831 and 1832, or where the information is not electronic or is stolen by means other than the unauthorized access to a computer. *Second*, the measure for offense severity proposed in Option 1 – the diminution in value of the information – is at best incomplete and, at worst, ineffective as an alternative to the existing measures of loss. On the one hand, it does explicitly provide *one* alternative to the direct financial loss and remedial costs in theft of information cases. However, the diminution in value of stolen information does not adequately reflect offense severity in certain types of data-breach cases. For example, in the Axciom case described in the CCIPS Presentation, the data-breach did not diminish the value of the stolen confidential records in any meaningful way. It is far better to allow courts flexibility to apply the proper measure of offense severity to the particular facts before it.

In contrast, the Department believes that Option 2 directly addresses the principal issues raised in cases involving the theft of information. This proposal seeks to allow courts to consider fair market value in estimating loss where information is "copied". *Reader Friendly*, at 9. The proposal also permits courts to consider both the development costs and the diminution in value of information in theft of information cases. *Id.*, 9-10. Because Option 2 provides additional factors other than diminution in value which courts may consider in estimating loss, and because it would apply to offenses under §§ 1831 & 1832, it is a significant improvement over Option 1.

Option 2 has an additional benefit: each of the listed factors has already been used by courts in imposing sentences under USSG §2B1.1. In the Axciom case, for example, lacking other tools to estimate loss, the sentencing court relied on an estimation of the fair market value as a factor in determining loss. *See Levine*, 477 F.3d at 603-04. Courts have also recognized that estimation of the fair market value of trade secrets "not generally available for sale" is infeasible, and development costs are a more appropriate measure of loss. *See United States v. Ameri*, 412 F.3d 893, 900 (8th Cir. 2005); *see also United States v. Four Pillars Enterprises Company, Ltd.*, 253 Fed. Appx. 502 (6th Cir. 2007) (sentencing court adopted development costs as a measure of loss in theft of trade secrets case). Indeed, in a written statement to the Commission, the Federal Defenders acknowledge that courts readily use development costs in estimating loss. *See* J. Martin Richey, *Written Statement on behalf of the Federal Public and Community Defenders and the Federal Defender Sentencing Guidelines Committee to the Commission, dated December 8, 2008 ("Federal Defenders' Letter")*, at 4.

Thus, by incorporating fair market value and development costs as factors in the estimation of loss for offenses involving the theft of information, the Commission would be fulfilling its mission to monitor federal law and practice and revise the guidelines accordingly. Any revision along these lines would ensure nationwide consistency by promoting the consideration of these factors by probation officers and sentencing courts in all cases, rather than

on an *ad hoc* basis.

The Department does, however, propose two technical changes to the language in Option 2. *First*, the current proposal permits courts to consider the fair market value of "property unlawfully taken, copied, or destroyed . . ." *Reader Friendly*, at 9. While the term "property" in this formulation appears to include trade secrets and other types of corporate information, it is somewhat peculiar to refer to property as being copied. The language could easily be revised to remedy this potential ambiguity by referring to: "***information or*** property unlawfully taken, ***copied***, or destroyed."

Second, Option 2 permits courts to consider either development costs *or* "diminution in value" in trade secret and theft of information cases. However, as a practical matter ascertaining the diminution in value of stolen information can be difficult and even infeasible. Consequently, diminution in value might not be a useful measure in many cases, although it may be appropriate and provable in some cases. It might, therefore, make sense to use language which permits courts to first consider development costs in estimating loss, before considering diminution in value, or other appropriate factors.

This could be accomplished with the following language:

(ii) *In the case of proprietary information (e.g., trade secrets), the cost of developing the information may be appropriate in many cases. Courts may consider other appropriate factors, including the reduction that resulted from the offense in the value of that information or the fair market value of the information;*

Stipulated Loss in Cases involving Small Harms to Many Victims

The Commission has invited comment on whether §2B1.1 should be revised to include a special rule providing a stipulated loss amount for offenses in cases involving information obtained from a protected computer without depriving the owner of the use of the information, or cases involving proprietary information such as trade secrets. *See Reader Friendly*, at 10. As stated above, the Department believes the better approach in cases involving theft of information is to permit courts to consider alternative measures of loss, such as fair market value and development costs. The losses suffered by victims in such cases are often fact specific to the type of information stolen, and sentencing typically would not be aided by adopting an approach that stipulates a loss amount.

The Department does believe, however, that the guidelines should be revised to include a stipulated loss provision similar to that adopted in Application Note 3(F)(i) (relating to credit cards) in a different set of cases – those involving damage to protected computers in violation of 18 U.S.C. § 1030(a)(5). ITERA amended § 1030(a)(5) to permit felony prosecutions of individuals causing damage to 10 or more computers, without the need to prove that the victims' loss exceeded $5,000, the minimal threshold for felony prosecutions under prior law. *See* 18 U.S.C. § 1030(a)(5) & (c)(4)(i)(VI). This change was directed at the proliferation of malware

designed to infect, and in some cases hijack, victim computers without the knowledge or authorization of their owners. As noted by Senator Leahy upon ITERA's passage in the Senate: "the amendment addresses the increasing number of cyber attacks on multiple computers, by making it a felony to employ spyware or keyloggers to damage 10 or more computers, regardless of the aggregate amount of damage caused. By making this crime a felony, the amendment ensures that the most egregious identity thieves will not escape with minimal punishment under Federal cyber crime laws." Senator Patrick Leahy, *Statement On Passage Of The Former Vice President Protection Act of 2008, H.R. 5938* (September 15, 2008).

The amendment also targets individuals involved in the proliferation of "botnets", which are networks of computers that have been infected with malicious software (sometimes referred to as "bot code") that permits an offender to hijack a computer without the individual's authorization or knowledge. *See BSA Written Testimony*, at 4 (noting that the new law "targets botnets by criminalizing cyber attacks on ten or more computers without also having to prove $5,000 in economic loss"). Botnets can range in size from hundreds of infected computers to hundreds of thousands of computers. Once assembled, botnets facilitate a variety of criminal conduct, including the sending of illegal spam and the launching of "denial of service" attacks that disable targeted computer systems. Infected computers within a botnet can also be used as proxies to conceal the identity and location of cyber-criminals. As described by the Business Software Alliance in its written testimony to the Commission on November 20, 2008:

> Cybercrime is increasingly technologically sophisticated. Because cybercrime has become a profession, and because it is financially motivated, criminals have a tremendous incentive to innovate. In particular, the rise of vast surreptitiously controlled computer networks called "botnets," has led to an explosion in the number and types of cyber crimes committed. The cyber criminal – or "bot herder" as he is known – sends out malicious code that takes over tens, or thousands, or tens of thousands of computers – known as "zombies" – and can effectively control them remotely using them to carry out anything from spam, to phishing, to denial of service

BSA Written Testimony, at 3.

In the aggregate, the damages from botnets can be huge. A recent study by the consulting firm Computer Economics argues that the so-called SdBot – a large botnet which also installed keyloggers and stole sensitive information from infected computers – resulted in an estimated worldwide impact of $950 million in 2006. That estimate was based on factors such as the labor costs of repairing infected computers, the loss of user productivity, potential and direct losses of revenue due to sub-optimal computer performance, and other direct costs such as the purchase of anti-virus software to prevent compromise. *See* Computer Economics, *2007 Malware Report*, at 4, 38, 42, found at http://www.computereconomics.com/page.cfm?name=Malware%20Report ("Computer Economics Study"). The study estimated that the aggregate cost of malware attacks

in 2006 was $13.3 billion. *Computer Economics Study*, at 33. Plainly, the harm caused by these crimes is immense.

However, proving actual monetary losses suffered by individual victims can be extremely difficult for several reasons. The impact on the victim can range from a slow down in an infected computer's functions with little economic impact; to the need to spend hours to buy, download, and run a program to remove the infection; to a trip to a repair technician who can charge $200 to clean-up and repair infected computers. In some cases, victims have reported that their computers are so damaged by the malware that they simply throw them away. Attempting to calculate actual losses in a case involving even 1,000 infected computers can be infeasible. The larger the botnet, the less feasible calculations of actual loss become. This raises difficult problems at sentencing, and it creates a situation where the government can establish criminal liability as Congress plainly intended, only to find that the actual provable loss vastly understates the seriousness of the offense.

Courts, of course, are empowered to estimate actual losses, but this task can be time consuming, expensive, and result in disparate sentences. The better course is for the Commission to decide on a conservative figure that fairly represents the minimum loss per computer, much as it did in the context of stolen credit cards. *See* USSG §2B1.1, Application Note 3(F)(i).

But what should the stipulated loss amount be? Based on a small sample set of botnets, Computer Economics has estimated the aggregate damages to business owners to be $11,000 for 19 infected machines, or $578 per infected machine. *See Computer Economics Study*, at 32. The study also looked at losses caused by other types of malware, such as destructive viruses and spyware. The average attack caused over $26,000 loss as a result of infecting 141 machines, or $181 per computer. *Id*. These figures are estimates based on available data and provide a rough guide to the losses these crimes cause. In addition, malware infections impose costs on Internet service providers that are not easily captured in loss calculations, including costs associated with increased traffic due to denial of service attacks and spam and increased costs incurred in taking adequate security precautions to guard against malware attacks. The Department believes that using a conservative figure such as $50 per computer would provide an appropriate minimum measure for sentencing purposes.

The Department's Proposed Amendment:

Application Note 3(F) to §2B1.1 should be amended to add a new Special Rule that reads as follows:

> (F) Special Rules. - Notwithstanding subdivision (A), the following special rules shall be used to assist in determining loss in the cases indicated: --
>
> * * *

(viii) Damage to Computers. In cases involving violations of § 1030(a)(5), loss includes any reasonable cost to any victim, as set forth in Application Note 3(A)(v)(III), and shall not be less than $50 per affected computer.

Definition of Victim under §2B1.1

The Commission has also invited comment on how to resolve a circuit split on the issue of whether the term "victim" as used in §2B1.1 includes individuals who are fully reimbursed for financial losses by a third party. *Reader Friendly*, at 11. There is a three way circuit split on this issue. The Fifth and Sixth Circuits have held that individuals who have been fully reimbursed for temporary financial losses are not victims, *see United States v. Connor*, 537 F.3d 480, 489 (5th Cir. 2008) and *United States v. Yagar*, 404 F.3d 967, 971 (6th Cir.2005), while the Eleventh Circuit has reached the opposite conclusion, *see United States v. Lee*, 427 F.3d 881, 895 (11th Cir. 2005). The Second and Ninth Circuits have staked out the intermediate position that individuals who suffer temporary financial losses and who are reimbursed can be considered "victims" for guidelines purposes if they suffered additional adverse affects that can be measured in monetary terms – such as the loss of time spent acquiring reimbursement or taking other steps to mitigate harm. *See United States v. Abiodun*, 536 F.3d 162, 168 (2d Cir. 2008); *United States v. Pham*, 545 F.3d 712, 721 (9th Cir. 2008).

The Department believes that the intermediate position taken by the Second and Ninth circuits is correct. In order to be a victim under §2B1.1, an individual must have suffered an actual loss, defined as a "reasonably foreseeable pecuniary harm that resulted from the offense." USSG §2B1.1, Application Notes 1 & 3(A)(i). The most common cases of individuals who are reimbursed for financial losses involve credit card fraud and similar offenses. In these cases, as a practical matter, individuals who have sustained temporary losses do not suffer financial harm since the financial intermediaries, such as credit card companies and banks, typically suspend payment for any disputed amounts pending investigation. In some cases, the companies may discover the fraud and reverse the charges before the customer is even aware that a fraud has occurred. If the customer is alerted, the company typically reverses the charges once the fraud is confirmed, and it cancels the amount due, or takes other actions to ensure that affected individuals are not out of pocket any money. Consequently, affected individuals never actually suffer financial harm measured by the fraudulent charges or fraudulent bank withdrawals. The true victims in these cases are the financial institutions such as the banks and credit card companies who suffer the aggregate out of pocket losses of their customers. Thus, these types of individuals affected by credit card fraud, bank fraud and other similar offenses cannot – and should not – be considered "victims" under the Guidelines.

Nevertheless, a smaller class of affected individuals does incur actual losses as a result of such types of fraud. Some credit card customers are liable for a deductible for fraudulent charges – typically around $50. These individuals are plainly victims under the guidelines. Others expend time resolving fraudulent charges or repairing credit histories. As noted in written testimony by the Federal Defenders, this is the non-financial harm most cited by victims

of identity theft. *See Federal Defenders Letter,* at 8. Additionally ITERA amended 18 U.S.C. § 3663(b)(6) to allow for restitution in the case of an offense under 18 U.S.C. §§ 1028(a)(7) or 1028A(a) for "an amount equal to the value of the time reasonably spent by the victim in an attempt to remediate the intended or actual harm incurred by the victim from the offense." It therefore makes sense to treat as "victims" those who expend measurable time taking remedial actions to mitigate the harm.

Enhancement for Abuse of Position of Trust or Use of Special Skill (§3B1.3)

The Commission has invited comment on whether the Abuse of Trust enhancement under §3B1.3 should apply to an "officer, employee or insider" of a business who participates in an offense involving the theft of "proprietary information," such as trade secrets. The Department believes the current guideline encompasses officer, directors, and high-level supervisory employees in trade secret cases. It has been our experience, however, that some courts have been reluctant to apply the enhancement in trade secret cases. Therefore, the Department recommends that the Application Note 1 to the guideline be amended to clarify that the Abuse of Trust enhancement should apply to officers, directors, fiduciaries, or other high-level, supervisory employees of a business or other entity, who participate in an offense involving theft of trade secrets from that business or entity.

The Department further recommends that, as in cases involving embezzlement of funds from a bank or other business, the guideline continue to distinguish between ordinary employees and officers, directors, fiduciaries, and high-level supervisory employees. All employees owe some duty to their employer, especially in cases in which they have been specifically entrusted with the safe-keeping of company property or confidential information including trade secrets. Officers, directors, and fiduciaries and other supervisory employees, however, owe an even greater duty to serve the company's interests; thus, their "abuse of trust" in misappropriating company trade secrets is more deserving of sanction. Moreover, supervisory and managerial employees can exploit their authority within a company to gain access to assets or information by coercing or co-opting lower level employees into aiding an offense against the company, and pressure subordinates not to question or second-guess improper conduct by the supervisor or manager. For these reasons, the Department believes it is appropriate to continue to hold officers, directors, fiduciaries, and other high-level supervisory employees who use their positions to facilitate or conceal a trade secret theft more culpable than lower level employees who engage in similar conduct, and we recommend that the §3B1.3 Abuse of Trust enhancement continue to be available against higher-level employees and not low-level employees.

The Department recommends the following amendment to Application Note 1 to USSG §3B1.3 to clarify that the guideline applies in trade secret cases.

The Department's Proposed Amendment:

Amend Application Note 1 to USSG §3B1.3 to read as follows:

1. Definition of "Public or Private Trust". – "Public or private trust" refers to a position of public or private trust characterized by professional or managerial discretion (i.e., substantial discretionary judgment that is ordinarily given considerable deference) . . . .This adjustment, for example, applies in the case of an embezzlement of a client's funds by an attorney serving as a guardian, a bank executive's fraudulent loan scheme, or criminal sexual abuse of a patient by a physician under the guise of an examination, ***or the theft of trade secrets in violation of 18 U.S.C. §§ 1831 or 1832 from a company or other entity by an officer, director, or fiduciary of the same company or entity.*** This adjustment does not apply in the case of an embezzlement or theft by an ordinary bank teller or hotel clerk because such positions are not characterized by the above-described factors.

D. Whether the Defendant Acted with Intent to Cause Either Physical Injury or Property Harm In Committing the Offense.

The Commission has invited comment on whether the guidelines adequately address situations in which an offense identified by Congress in ITERA (§§ 1028, 1030, 2511, and 2701) involved an intent to cause either physical or property harm. As the Commission indicates, §2B1.1 currently calls for higher sentences where the defendant had the requisite mental state. In particular, §2B1.1(b)(13) requires a two-level increase "[i]f the offense involved . . . the conscious or reckless risk of death or serious bodily injury." Additionally, §2B1.1 gives courts broad discretion to issue sentences above the guideline range if the offense caused or risked substantial non-monetary harm, such as physical harm, or "in a 1030 offense involving damage to a protected computer, if, as a result of that offense, death resulted." *See* USSG §2B1.1, Application Note 19(A)(ii).

The Department has not been able to identify a case of a death that resulted from the identified offenses. However, there have been incidents involving attacks on infrastructures suggesting that such cases may be on the horizon. For example, in 1998, a hacker pled guilty to recklessly damaging a telecommunications switch that interrupted service at a regional airport in Massachusetts. *See* the Department's Press Release, dated March 18, 1998, located at http://www.usdoj.gov/criminal/cybercrime/juvenilepld.htm. For hours, approaching pilots were unable to activate the runway landing lights, and communications with emergency services were inoperable. A similar risk to life and limb occurred when Rajib Mitra disrupted police radio service in Madison, Wisconsin, on Halloween, 2003. Mitra was convicted after a jury trial of intentionally causing damage to a protected computer in violation of 18 U.S.C. § 1030(a)(5). *United States v. Mitra*, 405 F.3d 492, 493 (7th Cir. 2005). Although no physical injuries were reported, it was undoubtedly in part the threat of such harm that caused the judge to sentence Mitra to eight years in prison.

More recently, in 2007, the U.S. Attorney in Dallas indicted several defendants for their roles in a so-called "swatting" conspiracy. "Swatting" refers to falsely reporting an emergency situation to a police department in order to provoke an armed Special Weapons and Tactics

(SWAT) response to a target address. Offenders ensure that police respond to a target address by making it appear as if an emergency 911 call requiring an armed response is being placed from the target residence rather than from the telephone being used by the culprit. The conspirators indicted in 2007 were responsible for "swatting" more than 250 victims. The 3 lead defendants, Stuart Rosoff, Jason Trowbridge and Chad Ward, pled guilty to conspiracy to use access devices to modify telecommunications instruments and to access protected telecommunications computers, and were each sentenced to 60 months' imprisonment. *See* the Department's Press Release ("Ringleaders in 'Swatting/Spoofing' Conspiracy Sentenced"), dated May 15, 2008, located at http://www.usdoj.gov/criminal/cybercrime/rosoffSent.htm. That sentence reflected the significant harms caused by the defendants' conduct, including some victim injuries, but the crimes could have resulted in death of a police officer or victim if the confusing circumstances during the police raid resulted in shooting.

Recent revisions of statutory provisions governing cyber-crime reflect congressional intent to reach computer crimes that may cause serious bodily injury or death or substantially endanger health and public safety. For example, Congress strengthened the statutory maximum penalties in the 2002 Homeland Security Act, adding a 20-year maximum for an offender who knowingly or recklessly causes serious bodily injury, and a maximum of life in prison for an offender who knowingly or recklessly causes death. Therefore, it is not surprising that Congress has directed the Commission to consider increasing penalties where the offender has the intent to cause physical harm.

The current 2-level enhancement for covered offenses where the defendant acted with conscious or reckless risk of bodily harm – along with the upward departure for substantial non-monetary harm – might be appropriate to handle outlier cases where a hacker causes harm. The Department believes that the enhancement does not adequately deal with a situation where a hacker intentionally causes death, or where the offense involved the conscious or reckless risk of death, and death resulted. It is not surprising that §2B1.1 does not specifically deal with such situations, since this provision is primarily designed to punish individuals who engage in a variety of economic crimes, which are not typically perpetrated by individuals intending to cause death. However, § 1030 covers a variety of criminal conduct, some of which – for example, computer fraud in violation of § 1030(a)(4) – fit easily within the basic structure of USSG §2B1.1, and some of which – like intentional damage to critical infrastructure computers in violation of § 1030(a)(5) – do not.

Fortunately, the current provisions of §2B1.1 suggest a manner of dealing with situations such as this. As the Commission itself indicates, §2B1.1(c) provides a cross reference which permits the application of firearms or explosives guideline if firearms or explosives are involved. *Reader Friendly*, at 12. This same mechanism is used in other guidelines provisions as well. *See, e.g.*, USSG §2H3.1(c) (permitting application of another guideline in the case of a wiretapping offense if its purpose was to facilitate another offense; cited at *Reader Friendly*, at 12). The Department recommends revising §2B1.1 to permit cross reference to the homicide guidelines, *see* §§2A1.1 through 2A1.4, where the offense involved the requisite intent to cause

death. This could be accomplished either by including a reference to homicide guidelines in Appendix A itself, or through an amendment along the following lines.

The Department's Proposed Amendment:

Amend §2B1.1(c) by adding the following new subsection:

(5) In the case of crimes sentenced under 18 U.S.C. § 1030(c)(4)(E), if death resulted, apply the appropriate homicide guideline from §§2A1.1-4, if the resulting offense level is greater than that determined under this guideline.

E. The Extent to Which the Offense Violated the Privacy Rights of Individuals

Interception of Communications (§2H3.1)

The Commission has proposed two alternative amendments to USSG §2H3.1 to take into account wiretapping offenses that breach privacy interests. The Commission acknowledges that breaches of privacy are difficult to capture within the guidelines regime because they are difficult, if not impossible to quantify. *See Reader Friendly*, at 15. Section 2H3.1 as currently written attempts to address the harm caused by breaches of privacy by providing an upward departure in cases resulting in "a substantial invasion of [a] privacy interest" in which "private or protected information" was obtained. *See* USSG §2H3.1, Application Note 5. The Commission seeks to address Congressional concern that sentences do not adequately reflect the extent to which privacy interests were breached through two alternative proposals. The first ("Option 1") creates a specific offense characteristic providing incremental punishment for offenses under 18 U.S.C. § 2511 (wiretapping) depending on the number of individuals whose "personal information" or "means of identification" was obtained through the offense, adopting the definition of personal information from §2B1.1, Application Note 13, and the definition of means of identification from 18 U.S.C. § 1028(d)(7). *See Reader Friendly*, at 13-14. This approach is similar to the approach taken in §2B1.1(b)(2), which also provides incremental punishment based on the number of victims. The second ("Option 2") provides authority for a court to depart upwards where the offense involves either "personal information" (as defined in §2B1.1) or "means of identification" of a real person (as defined in 18 U.S.C. § 1028(d)(7)).

Of the two options, the Department favors Option 1. However, the Department believes that both approaches are flawed for one essential reason: they attempt to provide incremental punishments based on the harms caused by the unlawful interception of *specific categories of information*: personal information and/or means of identification. Criminal liability in wiretapping cases, unlike in identity theft offenses, turns on the interception of *any* communication, whether or not that communication contains personal information or a means of identification. The wiretapping statute itself defines the specific privacy interest that merits protection – *any* intercepted oral or electronic communication. Moreover, private communication is personal and worthy of protection whether or not it conveys personal

information or a means of identification as defined in the proposed amendment. For example, a private conversation between two lovers could convey information worthy of more protection than a conversation where a victim provides a name, address, or telephone number. Consequently an approach based on categories of private information will fail to adequately reflect the seriousness of the offense conduct. A better approach would be to measure the significance of the offense based on the number of individuals affected, since the scope of the privacy breach increases in proportion to the number of individuals affected.

From this perspective, a revised version of Option 1 would offer the most direct way of determining the extent of the privacy breach: the number of individuals whose communications were intercepted. This approach to increasing sentences based on the number of victims is similar to the approach taken in §2B1.1(b)(2). This outcome could be accomplished by slightly revising the language of "Option 1" along the following lines:

The Department's Proposed Amendment:

§2H31. Interception of Communications; Disclosure of Certain Private or Protected Information

(b) Specific Offense Characteristics

* * *

(3) (Apply the greatest) If the defendant is convicted under 18 U.S.C. § 2511 and the offense involved intercepting the communications of –

(A) 10 - 50 or more individuals, increase by 2 levels;

(B) 50 - 250 or more individuals, increase by 4 levels; or

(C) 250 - 1,000 or more individuals, increase by 6 levels.

F. The Effect of the Offense upon the Operation of an Agency of the United States Government, or of a State or Local Government.

G. Whether the Offense Involved a Computer Used by the United States Government, a State, or a Local Government in Furtherance of National Defense, National Security, or the Administration of Justice.

H. Whether the Offense Was Intended to, or Had the Effect of, Significantly Interfering with or Disrupting a Critical Infrastructure.

I. Whether the Offense Was Intended to, or Had the Effect of, Creating a Threat to Public Health or Safety, Causing Injury to Any Person, or Causing Death.

The Commission has invited comment on whether the current guidelines adequately address several factors identified by Congress in ITERA that deal with the impact of cyber-crime on certain categories of government computers and "critical infrastructures" as defined by the guidelines.

Computer intrusions involving government computers often cause harms that cannot be measured in monetary terms. For example, elections increasingly rely on computers for storing and utilizing voter roles and for the casting and the tallying of votes. Disruption of a computer used to tally votes on an election day may be relatively inexpensive to repair, but it can have a significant impact on the perception of fairness among the voters.

Computer networks are also used in furtherance of the administration of justice – by state, local, and federal law enforcement agencies, by jail and prison agencies, by probation and parole offices, and by local, state and federal courts. Such networks play an important role in ensuring that the justice system performs effectively and efficiently so that dangerous criminals are kept off the streets. In one notable case, a convicted felon hacked into the computer network in San Bernadino County, California, and changed the records to show that charges pending against him were dismissed. *See* David Seaton, "Hacker Accesses Computer System for Riverside County, Calif., Superior Court," *The Press-Enterprise* (Riverside, CA), June 14, 2002, available at 2002 WLNR 9026366. If criminals can modify their sentences, gain early release, or disrupt the functioning of the courts, it could cause a grave impact on the public's faith in the fairness of the criminal justice system.

Computers are also used extensively by the military. Attacks on military computers and other computers used in furtherance of national defense can cause harms far beyond those that can be measured by the cost of cleaning up a damaged computer network. For example, a computer intrusion that discloses troop and equipment locations could gravely harm national security and endanger soldiers on the battlefield. Because of the importance of such government functions and because it is generally impossible to measure these harms solely in terms of repair costs or lost profits, courts should give careful consideration to these factors in sentencing offenders.

The current guidelines provide for increased penalties for intrusions into some, but not all, government systems. Section 2B1.1(b)(15)(A)(i) provides for a two-level increase for any intrusion into "a computer system used to maintain or operate a critical infrastructure, or used by or for a government entity in furtherance of the administration of justice, national defense, or

national security." This provision appropriately reflects the gravity of such attacks: offenders should be strongly deterred from such conduct.

The guidelines also provide a 6-level enhancement for "a substantial disruption of a 'critical infrastructure'". Application Note 13(A) to §2B1.1 defines "critical infrastructure" as "systems and assets vital to national defense, national security, economic security, public health or safety, or any combination of those matters" and provides an illustrative list. Strangely absent from this list is the administration of justice. The list does include "government operations that provide essential services to the public." However, this definition does not unambiguously cover the administration of justice. Indeed, sentencing courts and probation officers might conclude that the Commission's silence as to whether the administration of justice falls within the definition of a critical infrastructure shows that the Commission intended that it did not. Thus an offender who corrupted the functioning of a court computer network would apparently be subject to the 2-level enhancement under §2B1.1(b)(15)(A)(i), but not the 6-level enhancement under (A)(ii).

The Department believes that a clarification of these matters is appropriate, and that the Commission could adopt a revision along the following lines.

The Department's Proposed Amendment:

Amend the definition of "critical infrastructure" in Application Note 19 to §2B1.1 to read as follows:

> "Critical infrastructure" means systems and assets vital to national defense, national security, economic security, public health or safety, or any combination of those matters. A critical infrastructure may be publicly or privately owned. Examples of critical infrastructures include gas and oil production, storage, and delivery systems, water supply systems, telecommunications networks, electrical power delivery systems, financing and banking systems, emergency services (including medical, police, fire, and rescue services), transportation systems and services (including highways, mass transit, airlines, and airports), and government operations ~~that provide essential services to the public~~***, such as national defense, the administration of elections, and the administration of justice.***

J. Whether the Defendant Purposefully involved a Juvenile in the Commission of the Offense.

The Commission also invited comment on whether a defendant's purposeful involvement of a juvenile in the commission of the offense is adequately reflected in the guidelines. Section 3B1.4 of the guidelines provides for a 2-level upward adjustment in all cases where "the defendant used or attempted to use a person less than eighteen years of age to commit the offense or assist in avoiding detection of, or apprehension for, the offense . . . ." Since Chapter 3 is applied uniformly to all guidelines cases, it will apply with full force to sentences under those

statutory provisions identified in ITERA. The Department does not seek an amendment to this guideline.

K. Whether the Defendant's Intent to Cause Damage or Intent to Obtain Personal Information Should be Disaggregated and Considered Separately from the Other Factors Set Forth in §2B1.1(b)(15).

In addition to the more conceptual directives contained in § 209 of ITERA, Congress specifically directed the Sentencing Commission to consider "whether the defendant's intent to cause damage or intent to obtain personal information should be disaggregated and considered separately from the other factors set forth in §2B1.1(b)(15)." The Commission has responded to this Congressional directive by inviting comment on how to accommodate Congress' concern. *Reader Friendly*, at 19. The Commission also specifically asked whether any disaggregation of the factors in §2B1.1(b)(15) should only apply to offenses under 18 U.S.C. § 1030. *Id.*

In its current form, §2B1.1(b)(15) provides enhanced sentences for §1030 offenses; it does not apply to any other crime. The provision was designed to provide enhanced sentences based on differences in offenders' purpose and intent. Under this scheme, an offender who intends to steal personal information and one who intends to damage a computer both receive enhancements, but the intentional damage of a computer results in a *extra* 2-level enhancement (*i.e.*, a 4-level rather than a 2-level enhancement) to take into account that more serious nature of that criminal conduct. The provision also mandates longer sentences depending on the degree of damage to critical infrastructure computers. Affecting any critical infrastructure or government computer earns a 2-level enhancement, but causing "a substantial disruption of a critical infrastructure" results in a 6-level enhancement to take into account the more serious harm.

Unfortunately, in some cases, this provision mandates the same sentence for strikingly dissimilar conduct, and thus frustrates the goal of incremental punishment that the provision was intended to achieve. For example, §2B1.1(b)(15)(A)(i) imposes the same 2-level enhancement if a hacker acted with the intent to obtain personal information from either a grocery store computer or a critical infrastructure computer. Additionally, under the present structure, a hacker who *intentionally* damages a military computer gets the same 4-level enhancement as the hacker who intentionally damages an individual's home computer. Even more notable, an individual who accidentally causes a substantial disruption of a critical infrastructure computer gets the same 6-level enhancement as an offender who *intentionally* causes that harm.

In each of these pairs of scenarios, the same sentences result despite different offense severity. Critical infrastructure computers and the types of government computers identified in this guidelines section (*i.e.* computers involved in the administration of justice, public health or safety, national defense, or national security) typically contain far more sensitive information than other types of computers, such as sensitive medical records and classified information. Obtaining personal information from these types of computers clearly warrants more severe punishment. Similarly, intentionally damaging infrastructure computers should carry a higher penalty than intentionally damaging an individual's home computer – the social harm is greater,

as is the need to deter such conduct. And an individual who intentionally causes a substantial disruption to a critical infrastructure computer is more individually culpable than on who does so accidentally. Yet, the current guidelines do not differentiate the punishment in these instances.

The Commission's own statistics provide some evidence that, pursuant to this guideline provision, similar sentences are being imposed for these types of dissimilar criminal conduct. For example, in 2003, the Commission reported to Congress that nearly 7% (7/104) of the cases qualifying for a 2-level enhancement under this section involved a critical infrastructure or government computer. *Cyber Security Report*, at 4.[2] Thus, in approximately 7% of 18 U.S.C. § 1030 cases, more serious crimes were punished the same as less serious ones.

Congress undoubtedly directed the Commission to review disaggregation of these factors in order to remedy this defect. The source of the problem is the instruction in §2B1.1(b)(15)(A) to "Apply the Greatest" of the four enhancements enumerated in that section rather than permitting a court to apply each enhancement separately – and cumulatively – as the circumstances require. For these reasons, the Department strongly supports revisions to §2B1.1(b)(15)(A) as detailed below.

With respect to the specific question of whether this provision – in part or in whole – should apply to non-§ 1030 offenses, the Department sees no reason at this time to expand the scope of §2B1.1(b)(15)(A) to include other offenses. The proposal was designed to address gradations in harm arising from different types of § 1030 offenses, and the revision proposed by the Department would remedy what appears to be a technical flaw without altering the original scope.

The Department's Proposed Amendment:

Amend USSG §2B1.1(b)(15) to read as follows:

(15) --

(A) If the defendant was convicted of an offense under 18 U.S.C. § 1030 and the offense involved an intent to obtain personal information, increase by 2 levels.

(B) If the defendant was convicted of an offense under 18 U.S.C. § 1030(a)(5)(A)[3], increase by 4 levels.

---

[2] An additional 14.4% of the cases resulted in the 4-level enhancement, but the Commission did not specify which of these cases involved intentional damage to private computers rather than to government or critical infrastructure computers.

[3] ITERA changed the section numbering in 18 U.S.C. § 1030. The new section number for offenses involving intentional damage is § 1030(a)(5)(A).

~~(B) If subdivision (A)(iii) applies, and the offense level is less than level **24**, increase level to **24**.~~

(C) ~~(A)~~(Apply the greatest) If the defendant was convicted of an offense ***under 18 U.S.C. § 1030, and***:

(i) ~~under 18 U.S.C. § 1030, and~~ the offense involved ~~(I)~~ a computer system used to maintain or operate a critical infrastructure, or used by or for a government entity in furtherance of the administration of justice, national defense, or national security~~; or (II) an intent to obtain personal information,~~ increase by **2** levels.

~~(ii) 18 U.S.C. § 1030(A)(5)(A)(i), increase by 4 levels.~~

~~(iii) 18 U.S.C. § 1030, and offense caused a substantial disruption of critical infrastructure, increase by 6 levels.~~

(ii) the offense caused a substantial disruption of a critical infrastructure, increase by 6 levels. If the resulting offense level is less than level 24, increase to level 24.

L. Whether the Term "Victim" as Used in §2B1.1 Should Include Individuals Whose Privacy Was Violated as a Result of the Offense in Addition to Individuals Who Suffered Monetary Harm as a Result of the Offense.

The Commission invites comment on whether the scope of the term "victim" as used in the guidelines should be expanded to include individuals whose privacy was violated. Individuals affected by cyber-crime and identity theft suffer indirect harms in addition to the direct monetary losses attributable to the offense. Application Note 1 to USSG §2B1.1 defines a "victim" as one who suffers an "actual loss" as captured by the loss table. *See* USSG §2B1.1, Application Note 1; *see also Reader Friendly*, at 20. While some indirect harms are included in the definition of loss, there are other important interests – whose violation results in tangible and quantifiable harm – that are not.

Specifically, although subparagraph (v)(III) of Application Note 3(A) includes as "actual loss" the costs of restoring data, programs, systems, or information to its condition prior to the offense, it does so *only* for offenses charged under 18 U.S.C. § 1030. Many identity theft offenses are not charged under § 1030, however, but rather are charged as violations of 18 U.S.C. § 1028. Thus, many victims of identity theft offenses may not be treated as a "victim" for purposes of §2B1.1 because the costs of remediating the harm caused by the identity theft does not qualify as "actual loss." This is counter-intuitive for several reasons.

First, as the Federal Defenders have noted in written testimony before the Commission, the non-monetary harm most cited by victims of identity theft is the loss of time associated with

attempts to restore one's credit. *Federal Defenders Letter*, at 8. Second, 18 U.S.C. § 3663(b)(6), as amended by § 202 of ITERA, now allows for restitution in the case of an offense under 18 U.S.C. §§ 1028(a)(7) or 1028A(a) for "an amount equal to the value of the time reasonably spent by the victim in an attempt to remediate the intended or actual harm incurred by the victim from the offense." If an individual can obtain restitution for lost time, it only makes sense to construe that individual as a victim under the guidelines. This could be accomplished by permitting lost time in restoring credit to be included as a factor in determining loss under Application Note 3 to §2B1.1.

In sum, clarifying changes to Application Note 3 are needed to ensure that "actual loss" includes the pecuniary harms enumerated above for all identity theft offenses, whether they are charged as violations of 18 U.S.C. §1028 or 18 U.S.C. §1030.

The Department's Proposed Amendment:

Amend §2B1.1, Application Note 3 along the following lines:

3. Loss Under Subsection (b)(1). – This application note applies to the determination of loss under subsection (b)(1).

* * *

(v) Rules of Construction in Certain Cases. – In the cases described in subdivision (I) through (III), reasonably foreseeable pecuniary harm shall be considered to include the pecuniary harm specified for those cases as follows:

* * *

(III) Offenses ***that involve conduct described in 18 U.S.C. 1028, 1028A, or 1030***. – In the case of ***an offense that involved conduct described in 18 U.S.C. §§1028, 1028A and 1030***, actual loss includes the following pecuniary harm, regardless of whether such pecuniary harm was reasonably foreseeable: ***any reasonable cost to the victim, including: the cost of time reasonably spent attempting to remediate the intended or actual harm; the cost to the victim of correcting business, financial, and government records that erroneously indicate the victim's responsibility for particular transactions or applications;*** the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service.

M. Whether the Defendant Disclosed Personal Information Obtained During the Commission of the Offense.

As computers have become increasingly ubiquitous in our society, the amount of personal information stored in digital format continues to multiply. Companies store vast amounts of sensitive information about people, such as medical and financial records. Individuals have also taken advantage of computer resources, storing information such as diaries, personal correspondence, online banking and investing records, wills, tax returns, and calendars. As more and more computer networks serve as repositories for private information, computer intrusions now have unprecedented potential to expose the personal information of hundreds or thousands of users at once.

As highlighted by Michael DuBose, Chief of the Department's Computer Crime and Intellectual Property Section to the Commission in his presentation on November 20, 2008, the private information of public figures – whether confidential medical records, private photographs, or personal communications such as emails – have become an increasingly vulnerable target for hackers who seek to gain notoriety or cause significant embarrassment. *CCIPS Presentation*, at slides 12-16.

The current Sentencing Guidelines do address certain situations in which the principal harm is the violation of the victims' privacy interests. Section 2B1.1(b)(15)(A)(i)(II) prescribes a 2-level increase where the offense involves the intent to obtain "personal information," the definition of which contains the following non-exclusive list:

> "Personal information" means sensitive or private information (including such information in the possession of a third party), including (i) medical records; (ii) wills; (iii) diaries; (iv) private correspondence, including e-mail; (v) financial records; (vi) photographs of a sensitive or private nature; or (vii) similar information.

Application Note 13(A) to USSG §2B1.1. Additionally, the guidelines provide broad discretion for an upward departure where the facts of a particular case demonstrate a "substantial" privacy invasion. *See* Application note 19(A)(ii) to USSG §2B1.1 (expressly recommending an upward departure from the guideline range that would otherwise apply where "[t]he offense caused or risked substantial non-monetary harm").

However, the Commission should recall from the Miley Cyrus case described during the CCIPS Presentation that hackers are increasingly brazen about seeking fame and increasingly confident of their ability to evade punishment. The Department believes that the current 2-level enhancement is insufficient to adequately punish and deter offenses involving breaches of confidential personal information. Despite the clear need to deter such increasingly common conduct, potential sentences remain low. *See e.g.*, *CCIPS Presentation*, at slide 14 (offender who obtained hospital records of Tammy Wynette received a 6-month sentence). For example, a first time offender convicted of an offense under 18 U.S.C. § 1030 for hacking into a personal

email account, without causing significant economic loss, would face an adjusted criminal offense level of 9, reflecting a base level of 7 and a 2-level enhancement for the intent to obtain personal information. This would result in a Zone B guidelines range of 4-10 months, part of which could be non-custodial.

A revision of the guidelines that increases the enhancement for intent to obtain personal information to 4-levels would, under these same circumstances, result in an adjusted offense level of 11. This would correspond to a Zone C range of 8-14 months, resulting in a custodial guidelines sentence. Such a sentence would provide more effective deterrence, as well as punishment for the conduct commensurate with the seriousness of the offense.

Additionally, a particularly important situation that the guidelines do not address occurs when private information is publicly disclosed by the individual who gains unauthorized access to it. In the Tammy Wynette case referenced in the CCIPS Presentation, the defendant provided sensitive medical records to a tabloid, which published the information. *CCIPS Presentation*, at slide 14. It is one thing to obtain the medical records of an individual. It is quite another to publish that information. Because publication virtually always increases the significance of the privacy invasion, the Department seeks an amendment to the guidelines that would impose an additional two-level increase for the publication of personal information.

The Department's Proposed Amendments:

Amend USSG §2B1.1(b)(15) to include an additional "Specific Offense Characteristic":

(15) (A) (Apply the greatest) If the defendant was convicted of an offense

> (i) under 18 U.S.C. § 1030, and the offense involved (I) a computer system used to maintain or operate a critical infrastructure, or used by or for a government entity in furtherance of the administration of justice, national defense, or national security; or (ii) an intent to obtain personal information, increase by ~~**2**~~ ***4*** levels. ***Increase by an additional 2 levels if the offense involved an intent to disclose personal information to the public, or if the offense involved the public disclosure of personal information, and such public disclosure was reasonably foreseeable.***

Conclusion

We greatly appreciate the work of the Commission and its staff on these important sentencing issues, and we remain ready to assist you going forward.