U.S. Department of Justice

Criminal Division

Office of Policy and Legislation *Washington, D.C. 20530*

March 27, 2009

The Honorable Ricardo H. Hinojosa
Acting Chair, U.S. Sentencing Commission
One Columbus Circle, NE
Suite 2-500, South Lobby
Washington, DC 20002-8002

Dear Judge Hinojosa:

On behalf of the Department of Justice, we submit the following comments regarding the proposed amendments to the federal sentencing guidelines and issues for comment published in the Federal Register in January 2009. We appreciate the opportunity to comment on these matters, and we look forward to continuing our work with the Commission to promote a fair and effective federal sentencing system.

Beyond the specific guideline issues contained in the Federal Register notice, we are very pleased with the Commission's decision to continue its evaluation of the impact of *United States v. Booker*, 543 U.S. 220 (2005), and other recent Supreme Court decisions on the federal sentencing landscape. The full impact of these decisions remains unclear, and we believe the Commission's review, which includes the regional hearings now underway, will be extremely helpful in setting a path forward for federal sentencing. The Sentencing Commission is in the unique position of documenting and analyzing how these cases are changing the way in which federal defendants are sentenced in the United States.

We continue to urge the Commission to focus its study on both the micro and macro impact of recent changes to federal sentencing. Unlike any other body, the Commission is exceptionally well suited to paint a national picture of current sentencing practices. Similarly, the Commission is uniquely positioned to break down the national statistics. To provide meaningful insight into how the system is working, we believe the Commission should isolate sentencing practices based on individual crime types, region, race, and other factors to better examine how sentencing decisions are now being made. We have begun our own review of the federal sentencing system, and we look forward to working with the Commission on these systemic issues over the coming year.

TABLE OF CONTENTS

1. THE IDENTITY THEFT ENFORCEMENT AND RESTITUTION ACT OF 2008

In September 2008, Congress passed the Identity Theft Enforcement and Restitution Act of 2008 ("ITERA"). 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.[2] 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."[3] 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. The increasing sophistication of cyber-crime was also 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 . . . .[4]

---

[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").

[2] *See* United States Sentencing Commission, *Report to Congress: Increased Penalties for Cyber Security Offenses* (May 2003) ("*Cyber Security Report*").

[3] *See Cyber Security Report* at 8.

[4] 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*

Additionally, cybercriminals are no longer isolated actors, but now employ a division of labor that "span[s] continents."[5] 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."[6]

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. And 2008 saw a sharp rise in the number of reported data breaches from the previous year. 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.[7] 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.[8]

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."[9]

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

---

Enforcement Experts on Defeating Today's Cyber Criminals (2007), available at http://www.bsa.org/~/media/9CA4C9DFEDE24250AA16F16F0ED297A6.ashx.

[5] *BSA Written Testimony* at 4.

[6] *Id.*

[7] *See BSA Written Testimony* at 4 (*citing* the 2007 Consumer Reports "*State of the Net*" survey).

[8] *See* Senator Patrick Leahy, *Statement on Passage of the Former Vice President Protection Act of 2008, H.R. 5938* (Sept. 15, 2008); and http://www.sun-sentinel.com/business/custom/consumer/sfl-flhlpidpredictions1230sbdec30,0,928121.story.

[9] Senator Patrick Leahy, *Statement on Passage of the Former Vice President Protection Act of 2008, H.R. 5938* (Sept. 15, 2008).

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.[10] 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."[11] 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. 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 that 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,

---

[10] *Proposed Amendments to the Sentencing Guideline* ("*Reader Friendly*") at 6.

[11] *Id.*

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).

At the public hearing held on March 17, 2009, representatives from the Electronic Frontier Foundation – who oppose this revision – indicated in response to questioning that limiting application of the enhancement to the use of proxies intended to conceal the perpetrator's geographic location or identity would raise fewer concerns. The Department believes that application of the sophisticated means enhancement to the use of proxies and similar technologies should be limited to these situations. More importantly, the current language proposed by the Commission already limits application to "using any software or technology to conceal the identity or geographic location of the perpetrator." This language plainly excludes inadvertent use of a corporate VPN or other proxy technology during the commission of a crime, and thus adequately addresses any concern that the inadvertent use of a proxy might lead to an unfair increase in sentences. However, should the Commission want to narrow this application note further, we suggest revising it to:

"In addition, using computers in multiple jurisdictions in order to conceal identity or geographic location of the perpetrator ordinarily indicates sophisticated means."

Furthermore, the Department strongly supports the Commission's proposed language permitting application of the enhancement for the use of proxies in any "scheme involving computers" – not only convictions under 18 U.S.C. § 1030. Proxies are used by criminals in a variety of criminal schemes – including but not limited to identity theft under 18 U.S.C. §§ 1028, 1028A – to evade detection by law enforcement. Any language that limits application of the enhancement to the use of proxies in §1030 cases is therefore unwarranted.

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", 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.[12]

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.

---

[12] *Reader Friendly* at 6.

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."[13] 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.[14] 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 that 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

---

[13] *Id.* at 7.

[14] *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).

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.[15]

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 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.

---

[15] *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.

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 Acxiom case described by the Department at the Commission's November 20, 2008 public briefing.[16] Others involve the theft of valuable trade secrets.[17]

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 understate the seriousness of such offenses.

---

[16] *See also United States v. Levine*, 477 F.3d 596 (8th Cir. 2001).

[17] *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).

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.[18] 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.[19] Of these two alternatives, the Department strongly supports the adoption of Option 2, and opposes the adoption of Option 1.

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 at the November public briefing session, 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. Indeed, this problem would persist if the Commission chose to enact both options, since courts sentencing a § 1030 offense would be constrained by the more specific

[18] *Reader Friendly* at 9.

[19] *Id.* at 9-10.

language that pertains only to § 1030 offenses. For this reason, the Department opposes adoption of Option 1 either alone, or in combination with the adoption of Option 2.

In contrast, the Department believes that Option 2 by itself 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."[20] The proposal also permits courts to consider both the development costs and the diminution in value of information in theft of information cases. 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.[21] 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.[22] Indeed, in a written statement to the Commission, the Federal Defenders acknowledge that courts readily use development costs in estimating loss.[23]

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 . . ."[24] 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

---

[20] *Reader Friendly* at 9.

[21] *See Levine*, 477 F.3d at 603-04.

[22] *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).

[23] *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.

[24] *Reader Friendly* at 9.

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.[25] As stated above, the Department believes the best 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."[26]

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

---

[25] *See Reader Friendly* at 10.

[26] Senator Patrick Leahy, *Statement on Passage of the Former Vice President Protection Act of 2008, H.R. 5938* (Sept. 15, 2008).

or knowledge.[27] 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.[28]

In recent years, the prosecution of those involved in the creation, use and sale of botnets has been a high priority for the Department. The first major botnet investigations resulted in convictions in 2005 and 2006. In 2005, for example, an Oregon man was convicted of using a botnet to launch a denial of service attack targeting eBay.[29] In 2006, a Californian pled guilty for his role in creating a botnet that infected numerous computers worldwide, including hospital and military computers, and that actually disabled a hospital computer system.[30] In 2007, the FBI completed a nationwide operation known as "Bot Roast," that resulted in numerous indictments and convictions.[31] More recently, in 2008, a Brazilian man was arrested in the Netherlands and indicted by a grand jury in New Orleans for his role in the creation, maintenance and sale of a

---

[27] *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").

[28] *BSA Written Testimony* at 3.

[29] *See* the Department's Press Release, "Man Pleads Guilty to Infecting Thousands of Computers Using Worm Program then Launching them in Denial of Service Attacks", dated December 28, 2005, found at http://www.cybercrime.gov/clarkPlea.htm.

[30] *See* the Department's Press Release, "California Man Pleads Guilty in 'Botnet' Attack That Impacted Seattle Hospital and Defense Department", dated May 4, 2006, found at http://www.cybercrime.gov/maxwellPlea.htm.

[31] *See, e.g.*, the FBI's Press Release, "'Operation Bot Roast II" Nets 8 Individuals,'" dated November 29, 2007, found at http://www.fbi.gov/pressrel/pressrel07/botroast112907.htm; Michael Cooney, "FBI: Operation Bot Roast finds 1 million botnet victims", *Computerworld Security* (June 14, 2005), found at http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9024718.

botnet consisting of more than 100,000 infected computers worldwide.[32] As these examples illustrate, botnets are a real, substantial, and growing problem.

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.[33] The study estimated that the aggregate cost of malware attacks in 2006 was $13.3 billion.[34] 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.[35] The study also looked at losses caused by other types of malware, such as destructive viruses and spyware. The average attack caused over

---

[32] *See* the Department's Press Release, Brazilian Man Charged in Conspiracy to Infect More Than 100,000 Computers WorldWide with Malicious Software", dated August 21, 2008, found at http://www.usdoj.gov/criminal/cybercrime/netoIndict.pdf.

[33] *See* Computer Economics, *2007 Malware Report* at 4, 38, 42, found at http://www.computereconomics.com/page.cfm?name=Malware%20Report ("Computer Economics Study").

[34] *Computer Economics Study* at 33.

[35] *See Computer Economics Study* at 32.

$26,000 loss as a result of infecting 141 machines, or $181 per computer.[36] 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.[37] 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.[38] The Eleventh Circuit has reached the opposite conclusion.[39] 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.[40]

---

[36] *Id.*

[37] *Reader Friendly* at 11.

[38] *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).

[39] *See United States v. Lee*, 427 F.3d 881, 895 (11th Cir. 2005).

[40] *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.[41] 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 (USSG §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

[41] *See Federal Defenders Letter* at 8.

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.[42] 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).[43] 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.[44] 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

---

[42] *See* the Department's Press Release, dated March 18, 1998, located at http://www.usdoj.gov/criminal/cybercrime/juvenilepld.htm.

[43] *United States v. Mitra*, 405 F.3d 492, 493 (7th Cir. 2005).

[44] *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.

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.[45] This same mechanism is used in other guidelines provisions as well.[46] 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 (USSG §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.[47] 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

---

[45] *Reader Friendly* at 12.

[46] *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).

[47] *See Reader Friendly* at 15.

from §2B1.1, Application Note 13, and the definition of means of identification from 18 U.S.C. § 1028(d)(7).[48] 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;

[48] *See Reader Friendly* at 13-14.

(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.[49] 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

[49] *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.

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.[50] 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.[51]

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.

---

[50] *Reader Friendly* at 19.

[51] *Id.*

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.[52] 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)[53], increase by 4 levels.

---

[52] *Cyber Security Report* at 4. 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.

[53] 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.[54] 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.[55] Second, 18 U.S.C. § 3663(b)(6), as amended by § 202 of

---

[54] *See also Reader Friendly* at 20.

[55] *Federal Defenders Letter* at 8.

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.

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 November public briefing session 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. 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 8, reflecting a base level of 6 and a 2-level enhancement for the intent to obtain personal information. This would result in a Zone A guidelines range of 0-6 months, all 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 10. This would correspond to a Zone B range of 6-12 months, resulting in a sentence that would require some degree of confinement. 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 November public briefing session, the defendant provided sensitive medical records to a tabloid, which published the information. It is one thing to obtain the medical records of an individual. It is quite another to disclose or publish that information. Because disclosure 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 disclosure of personal information. The Department believes that this could be accomplished by adding a 2-level enhancement to §2B1.1(b)(15)(A) for disclosures of personal information which the defendant knew, intended, or had reason to believe could cause or risk substantial non-monetary harm. For purposes of making this determination, the Department believes that the definition of "personal information" contained in application Note 13(A) is sufficient.

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 the disclosure of personal information of an individual and the defendant knew, intended, or had reason to believe that the disclosure would cause or risk substantial non-monetary harm to that individual.***

2. RYAN HAIGHT ONLINE PHARMACY CONSUMER PROTECTION ACT OF 2008

The Ryan Haight Online Pharmacy Consumer Protection Act of 2008, Pub.L. 110-425, (the Act) created two new offenses under the Controlled Substances Act (CSA), and increased the penalties authorized by the CSA for offenses involving Schedules III, IV, and V controlled substances. In response, the Commission has proposed amendments and solicited comments on whether and how these changes to the CSA should be reflected in the guidelines. The Department previously has provided the Commission with testimony and a detailed written submission explaining its views on how and why the guidelines should be amended to reflect the increased punishments available under the CSA for offenses involving Schedules III, IV, and V controlled substances. In particular, we have emphasized the very real and growing problems presented by wide-spread abuse of hydrocodone, a Schedule III controlled substance. Hydrocodone is readily available from rogue Internet pharmacies, and the Act provides new statutory penalties commensurate with the danger the drug poses. The Department believes that, at a minimum, the guidelines should reflect these increased penalties for offenses involving large quantities of hydrocodone.

The Department's comprehensive proposal is briefly reiterated below. We also incorporate our more extensive prior comments by reference, and provide input on several related issues that were not addressed in our previous submissions.[56]

Taking the latter first, the Department agrees with the Commission that the new offense contained in 21 U.S.C. § 841(h) (using the Internet to deliver, distribute, or dispense a controlled substance), should be referenced directly to §2D1.1 in Appendix A. Likewise, the Department agrees that the new prohibition against using the Internet to advertise the unlawful sale of controlled substances, contained in 21 U.S.C. § 843(c)(2)(A), is adequately and appropriately referenced to §2D3.1 in Appendix A.

With respect to the alternatives proposed for offenses involving Schedule III controlled substances that result in death or serious bodily injury, the Department endorses Option 1, setting an alternative base offense level. We suggest, moreover, that the alternative base offense level be set no lower than 30. The Department prefers the alternative base offense level because it is consistent with the way the guidelines treat offenses involving Schedules I and II controlled substances that result in death or serious bodily injury.

We recognize that when death or serious bodily injury results from an offense involving a Schedule I or II controlled substance, the CSA generally provides a mandatory minimum sentence.

---

[56] The Department's input to date has focused on the base offense levels we believe should be applicable to CSA offenses involving Schedules III, IV, and V controlled substances, and in particular hydrocodone, a Schedule III controlled substance. We have also proposed changes to the Drug Equivalency Tables contained in §2D1.1, Application Note 10(E). We have not previously provided views on how the new offenses created by the Act should be reflected in the guidelines or the method by which the guidelines should address the sentencing enhancement provided by the Act for offenses involving Schedule III controlled substances that result in death or serious bodily injury.

21 U.S.C. § 841(b)(1). It makes sense for the guidelines to reflect this policy by setting the alternative base offense level at a point that encompasses the mandatory minimum.[57] The converse, however, is not true. That is, the fact that an offense involving a Schedule III controlled substance that results in death or serious bodily injury carries no mandatory minimum is not a sufficient reason to ignore the consequence of the crime when setting the base offense level.

We recommend that the alternative base offense level be set no lower than 30 to reflect the judgment of Congress. Congress has determined that offenses involving Schedule III controlled substances that result in death or serious bodily injury should be subject to a maximum punishment substantially greater than would be available if death or serious bodily injury does not result. The current maximum base offense level for offenses involving Schedule III controlled substances (other than Ketamine) is 20. As a result, an alternative base offense level of 30 when the offense results in death or serious bodily injury would be appropriate and consistent with statutory law.[58]

An alternative base offense level no lower than 30 would also ensure that, for the most serious offenders, the guideline sentencing range would encompass or approach the statutory maximum. At level 30,[59] defendants with little or no criminal history will face a substantial sentence, but one still significantly less than 15 years.[60] For offenders with extensive criminal histories, however, level 30 would encompass the statutory maximum when death or serious bodily results from an offense involving a Schedule III controlled substance. This result is not only consistent with congressional intent, but with sound principles of graduated sentencing.

If, instead of an alternative base offense level, the Commission creates a specific offense characteristic for this sentencing enhancement, we strongly urge the Commission to set a floor that reflects the gravity of the offense. Because base offense levels for the distribution of Schedule III controlled substances are determined by drug quantity, it is possible that simply adding some number of levels when death or serious injury results will not adequately reflect the seriousness of the crime. For example, death or serious injury can result from the distribution of a relatively

---

[57] In fact, the current alternative base offense level for most offenses involving Schedule I and II controlled substances, where the defendant has no prior similar convictions, and which result in death or serious bodily injury is set at 38. For persons with no criminal history, level 38 calls for a sentence between 235 and 293 months. The mandatory minimum – 240 months – is near the bottom of that range.

[58] An alternative base offense level of 30 for offenses resulting in death or serious bodily injury might be considered lenient if, as we have also suggested, the Commission raises the base offense level cap for offenses involving large quantities of Schedule III controlled substances, regardless of whether they result in death or serious bodily injury.

[59] We understand, of course, that the base offense level is subject to a variety of adjustments that will affect the ultimate sentencing range.

[60] For defendants in criminal history category I, level 30 equates to a sentencing range of 97-121 months. For criminal history category II, level 30 equates to a sentencing range of 108-135 months.

small number of dosage units, amounts that would translate to base offense levels of just eight, or ten. Without an appropriate floor, simply adding 6, 8, or even 10 levels when death or serious bodily injury results could produce an inadequate sentencing range. For example, if death or serious bodily injury resulted from the distribution of 750 dosage units of hydrocodone, and 8 levels were added to the base offenses level, the result would be a final offense level of 16. This translates to a sentencing range of between two and three years, even for defendants with significant criminal histories.[61] We think this is inadequate for drug traffickers responsible for another person's death or serious bodily injury. For the reasons articulated above, we suggest that an appropriate floor should be no lower than level 30.

The Department is opposed to Option 3, which would invite an upward departure when death or serious bodily injury results from an offense involving Schedule III controlled substances. This option would be inconsistent with the approaches employed by the guidelines for most other offenses involving violations of the CSA.[62] More importantly, relying upon an invited upward departure will tend to produce inconsistent sentencing results for similar offenders.

The Commission has also identified four issues for comment, each of which addresses the increased punishments for offenses involving Schedules III, IV, and V controlled substances authorized by the Ryan Haight Online Pharmacy Consumer Protection Act of 2008.
We previously provided recommendations and justifications that respond to each of the four issues identified by the Commission. We briefly reiterate that information here.

A. Schedule III Controlled Substances

Schedule III Hydrocodone

We recommend:

- Revising the drug equivalency table with respect to Schedule III hydrocodone (currently listed on page 155 of the Guidelines Manual), using as a model the current approach for oxycodone. The hydrocodone equivalency would be based on the actual amount of active ingredient and with no base offense level cap. Specifically, we recommend using one-fourth (1/4) the current conversion ratio for oxycodone: 1 gm of Schedule III hydrocodone (actual) = 1675 gm of marijuana (with no cap).

As we have demonstrated in detail in our previous submissions, the abuse (nonmedical use) of Schedule III hydrocodone products has risen dramatically in recent years, with hydrocodone now being the most widely abused pharmaceutical controlled substance in the United States. All

---

[61] The guideline range for a defendant with five criminal history points at level 16 is 27-33 months.

[62] As noted, for offenses involving Schedule I and II controlled substances, an alternative base offense level is provided when the offense results in death or serious bodily injury. For certain offenses involving the manufacture of controlled substances, the guidelines provide an alternative base offense level and/or a specific offense characteristic when human life is endangered.

reliable studies indicate that the number of persons currently abusing hydrocodone is even greater than for oxycodone. Because of the increased demand among abusers for hydrocodone, trafficking in hydrocodone is more lucrative than ever and the quantities of the drug being sold illegally are, in many cases, greater than ever (*e.g.*, often well in excess of the minimum quantity associated with the guidelines cap, which, as a practical matter, allows no additional penalties for amounts exceeding 40,000 dosage units). The current sentencing guidelines do not provide a sufficient deterrent to inhibit this large-scale and extremely profitable trafficking in hydrocodone.

Because of the similarities between hydrocodone and oxycodone in terms of the scope of trafficking, abuse, and the resultant harms, we are suggesting a modification to the guidelines for hydrocodone similar to the approach taken by the Commission in response to the rise in abuse of oxycodone. Under the current guidelines, the conversion ratio for oxycodone is "1 gm of Oxycodone (actual) = 6700 gm of marihuana." Given that the statutory maximum penalty for trafficking in oxycodone is 20 years, 21 U.S.C. § 841(b)(1)(C), and the statutory maximum penalty for trafficking in Schedule III hydrocodone is now 10 years, the Department considered proposing using one-half the current ratio for oxycodone (which would be 3350 gm of marijuana for every gram of hydrocodone). Although the Department believes that such a ratio is reasonable, using one-quarter of the oxycodone ratio (1675 gms of marijuana for every gram of hydrocodone) would be a more conservative approach and would result in sentencing levels that provide a minimally acceptable deterrent effect. In addition, for this ratio to be effective in large-scale trafficking cases, the Department also recommends that the current guidelines cap (base offense level 20) be eliminated.

By way of example, if the Department's foregoing suggestions were adopted, an individual convicted of trafficking in 10,000 tablets of 10 mg hydrocodone (the strongest dosage available) would receive a base offense level of 26. Assuming no criminal history or aggravating or mitigating factors, this resulting guideline range would be 63-78 months, still well below the statutory maximum. The guideline range would encompass the maximum sentence only for a defendant with a substantial criminal history (Category V or VI).

All Other Schedule III Controlled Substances (Other Than Hydrocodone)

We recommend eliminating the cap (currently at level 20) or raising the cap to level 26. Recognizing that hydrocodone is by far the most widely trafficked and abused Schedule III controlled substance, the Department suggests that the guidelines for other Schedule III controlled substances need not be altered significantly. However, the current level 20 cap does not adequately address those instances in which the trafficker is convicted of dealing in extremely large amounts of these other Schedule III controlled substances. For example, if the cap is eliminated or raised, a trafficker in Schedule III controlled substances (other than hydrocodone, assuming our proposal above is adopted) would not reach offense level 26 unless the offense conduct involved the distribution of 100,000 or more dosage units.

B. For Schedule IV Controlled Substances

We recommend:

- Eliminating the current offense level cap (currently at level 12) or raising the cap to level 24; and

- Increasing the marijuana equivalency from the current ratio of 1 unit = 0.0625 grams of marijuana to 1 unit = 0.125 grams of marijuana.

While we believe raising guideline penalties for hydrocodone should be the Commission's the top priority, we also believe some adjustment to the Schedule IV guidelines is warranted in order to provide a sufficient deterrent commensurate with the current nature and scope of offenses involving such drugs. In this respect, we note that the second-most widely abused pharmaceutical in the United States is alprazolam (*e.g.*, Xanax®), a Schedule IV substance. Using the current equivalency ratio, but without a cap, a convicted trafficker's offense conduct would need to involve the distribution of more than 1 million dosage units of a Schedule IV substance before reaching offense level 24. Even a modest increase in the equivalency ratio (*e.g.*, doubling it to .1250 grams), would not raise the guidelines to a range encompassing the statutory maximum sentence (five years) unless the convicted trafficker's offense conduct involved dealing an extremely large quantities (160,000 dosage units or more), and the defendant had a substantial criminal history (Category V).

C. For Schedule V Controlled Substances

We recommend revising the current offense level cap beyond its current level (level 8) as warranted to allow the guideline range to encompass the new statutory maximum of 4 years for a defendant dealing in large quantities and with a significant criminal history.

Although this proposal is our lowest priority among the proposed revisions to the guidelines, we think it appropriate that the statutory maximum sentence be available under the guidelines for the most serious offenders. For example, under the current equivalency ratio (1 dosage unit of a Schedule V controlled substance equals .00625 grams of marijuana), if the cap is raised to base offense level 16, a defendant would not qualify for a guidelines range that encompassed the statutory maximum unless he had a substantial criminal history (Category V or VI) and was convicted of dealing more than 1.5 million dosage units.

3. DRUG TRAFFICKING VESSEL INTERDICTION ACT OF 2008

On October 13, 2008, the President signed into law the Drug Trafficking Vessel Interdiction Act of 2008, Pub. L. No. 110-407. The Act prohibits "the operation of submersible vessels and semi-submersible vessels without nationality." *See* 18 U.S.C. § 2285 (Operation of Submersible Vessel or Semi-submersible Vessel Without Nationality). The Commission has published a proposal to create a new guideline with a proposed base offense level between 12 and 34 and has identified three issues for comment.

A. Creation of a New Guideline

First, the Department urges the Commission to promulgate a new guideline at 2X7.2, rather than linking it to 2X5.1. This statute is not about drug possession, and it should reflect the congressional finding that these stateless vessels, regardless of the cargo they may carry – drugs, persons, firearms, etc. – present a serious threat to the security of the United States and maritime navigation generally. In those self-propelled semi-submersible ("SPSS") cases where the government recovers drug evidence, the government intends to charge the case under the Maritime Drug Law Enforcement Act ("MDLEA"). On the other hand, in the cases where the SPSS sinks and contraband cannot be recovered, the government intends to use this new statute. Given the unique elements and dangers inherent in committing this offense, congressional intent is best served by creating a separate guideline, not a reference to a general felony guideline.

B. Setting the Base Offense Level

The Department urges the Commission to set the base offense level at the top offense level of 34. Only at this level does the guideline provide trial judges with a standard that properly reflects the specific congressional findings that stateless submersible vessels present a serious threat to the security of the United States. Most importantly, a base offense set at 34 results in sentences that are commensurate with those typically imposed on individuals convicted under the MDLEA. Anything less, and sentences under the Drug Trafficking Vessel Interdiction Act would be lighter than those under the MDLEA for cooperating witnesses/defendants. Perversely, maritime drug traffickers would actually have an incentive to continue their use of submersible vessels and to scuttle those vessels when law enforcement is detected. Only by setting the base offense level at the top level does the proposed guideline remove that unintended incentive and ensure that district courts impose sentences that are substantial and reflect the serious nature of the criminal activity and the national security threat from these SPSS vessels.

C. Accounting for Lesser Culpability

The Commission should not offer an alternative base offense level where the mitigating role applies. An alternative base offense level for mitigating role is simply not appropriate, particularly given the evidence that none of the crew members in a submersible performs a minor or minimal role. Each of the crew members on board performs an important role and gets paid highly for his work, especially in comparison to crew members for other maritime cocaine movements. For example, cooperating defendants have revealed that a sailor or crew member in a "go fast" boat carrying cocaine gets paid an average of $10,000 to $15,000 per trip. By contrast, the average pay for a sailor or crew member in an SPSS ranges from $40,000 to $80,000 per trip.

Pay for the other crew members pay is even higher, ranging from $150,000 to $200,000 for a captain, as opposed to $60,000 to $120,000 for "go fast" captains; and from $100,000 to $150,000 for an SPSS mechanic, compared to $10,000 to $20,000 for a "go fast" mechanic. .

Given the lucrative, difficult, and dangerous nature of working on an SPSS, it is difficult to envision any crew member being routinely considered a minor player. In those cases where a court may find that a particular defendant's conduct is that of a mitigating and cooperative nature, the court can always impose a downward adjustment.

If the Commission insists on establishing an alternative base offense level for mitigating role within §2X7.2, we would urge the Commission to make that level consistent with that of a defendant with a mitigating role under §2D1.1. Failing to do so would result in lower sentences under the SPSS guideline than under MDLEA, thus giving drug traffickers an incentive to continue their use of submersible vessels, and undermining the intent of the Drug Trafficking Vessel Interdiction Act.

4. COURT SECURITY IMPROVEMENT ACT OF 2007

In 2007, Congress passed the Court Security Improvement Act ("Act"), which created new maximum penalties for assaulting a federal official with intent to impede his performance, or to retaliate for the performance of his official duties. *See* 18 U.S.C. § 115. The Act also changed the penalties for witness tampering. Congress directed the Commission to review whether Internet threats should be treated differently under the guidelines, and to consider whether three factors – the number of threats, the intended recipient of the threats, and whether the person making the threat was acting individually or as part of a group – should be addressed in the guidelines.

A. Increases in Statutory Maximum Penalties

The question whether the guidelines are adequate as they apply to the revised offenses of 18 U.S.C. §§ 115 and 1112 is complicated by the fact that the existing guidelines apply to dozens of other offenses. We take seriously the offense conduct at issue in the Act and believe that it should be punished appropriately. At the same time, we understand the far-reaching impact of any changes to these guidelines, particularly those involving offenses against the person. Accordingly, before undertaking a wholesale adjustment of the impacted guidelines, we recommend the Commission comprehensively study the impact of changing these guidelines on other offenses.

However, the Department supports amending Appendix A to refer offenses under § 1513 to guidelines other than §2J1.2 (Obstruction of Justice). Specifically, the Department believes that the guidelines should be amended to refer not only to obstruction of justice guidelines, but also to guidelines for crimes against the person, such as §§2A1.1, 2A1.2, 2A2.1, 2A2.2, 2A2.3. Congress has indicated that the most serious of these offenses, particularly those that involve violence against a person, should be treated more severely in the guidelines. Amending Appendix A by providing references to the appropriate Chapter 2, Part A guidelines will capture the more serious conduct at issue while treating like conduct similarly.

B. Official Victims

The Commission has also asked for comment on (1) whether the existing Chapter 3 adjustments adequately address the new statute for offenses involving an official victim or member of the family of such an official; and (2) whether the current guidelines are adequate as they apply to non-official victims. The Department believes that the existing guidelines are inadequate – particularly as they apply to non-official victims, such as witnesses, jurors, or informants. Our interest is to ensure that the penalties for threatening violence against victims – whether official or unofficial – are commensurate to the violent act. For that reason, we believe if the Commission refers § 1513 to the offenses against the person guidelines in Part 2A, as outlined above, the guidelines will then provide for the necessary penalties.

C. Directive to the Commission

Section 209 of the Act directs the Commission to review threats made in violation of § 115 that occur over the Internet to determine whether and how that circumstance should aggravate the punishment of this crime. As U.S. Marshal Michael Prout and psychologist Mario Scalora noted in their testimony to the Commission, the most serious threats are those that are made publicly – regardless of the forum. Unlike a letter or an email, incendiary comments posted on an Internet

website or made on the radio or television have the potential to incite countless numbers of persons and spur additional threats against the victim. Furthermore, public postings of restricted personal information of a victim, such as a home address or Social Security number, can facilitate acts of violence against the victim, often requiring the expenditure of extraordinary resources to ensure the victim's safety. Although these cases do not necessarily create volumes of victims; they do create volumes of potential threateners. Accordingly, we recommend an amendment to the guidelines to reflect the increased threat to public safety when a defendant violates 18 U.S.C. § 115 by publicly threatening an official, including by posting private information on the Internet.

5. WILLIAM WILBERFORCE TRAFFICKING VICTIMS PROTECTION REAUTHORIZATION ACT OF 2008

The William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008 was signed into law on December 23, 2008. The law created several new crimes, including the obstruction of human trafficking investigations and fraudulently luring a person to the United States to work. It also directed the Commission to review penalties for the organizers or leaders of alien harboring offenses committed in furtherance of prostitution.

On March 17, several witnesses testified before the Commission regarding the directive and the new crimes. Based on the testimony, we believe many of these issues can be resolved during this amendment cycle. For this reason, we submit the following detailed comments on the Act for the Commission's consideration. Given the short time since the enactment of the Act, however, we are continuing to review these matters.

A. Directive to the Commission

Section 222(g) of the Act directs the Commission to:

> review and, if appropriate, amend the sentencing guidelines and policy statements applicable to persons convicted of alien harboring to ensure conformity with the sentencing guidelines applicable to persons convicted of promoting a commercial sex act if –
>
> (1) the harboring was committed in furtherance of prostitution; and
> (2) the defendant to be sentenced is an organizer, leader, manager, or supervisor of the criminal activity.

The Commission requests comment regarding whether "the guidelines should be amended to ensure conformity between the guidelines applicable to persons convicted of alien harboring (*i.e.* §2L1.1) and the guidelines applicable to persons convicted of promoting a commercial sex act (*i.e.* §§2G1.1 and 2G1.3)." We believe the guidelines should be modified in line with the congressional directive and that it is most appropriate to do so by adding specific offense characteristics to §2L1.1: one addressing prostitution-related conduct generally and one addressing the prostitution of minors.

Interests in Conformity: Achieving Proportionality While Recognizing Relevant Distinctions in Criminal Conduct

In considering the interests in conformity between alien harboring guidelines and commercial sex guidelines, it is important to recognize there is a spectrum of criminal conduct related to commercial sexual exploitation. While all forms of commercial sexual exploitation are reprehensible and must be appropriately punished, there are gradations in the nature and severity of prostitution-related criminal conduct warranting distinctions in sentencing. The current guidelines recognize such gradations by specifying varying offense levels depending on the particular offense of conviction.

The relevant sexual exploitation guidelines, USSG §§2G1.1 and 2G1.3, apply to an array of distinct offenses, including sex trafficking in violation of 18 U.S.C. § 1591, interstate transportation for prostitution in violation of 18 U.S.C. §§ 2421 or 2423, and importation for prostitution in violation of 8 U.S.C. § 1328. The base offense levels within these guidelines vary, as follows, according to the nature of the offense:

Offense	**Base Offense Level**	**Applicable Guideline**
§ 1328, § 2421 (adult)	14	§2G1.1(a)(2)
§ 1328, § 2421 (minor)	24	§2G1.3(a)(4)
§ 2423 (minor)	28	§2G1.3(a)(3)
§ 1591 (minor aged 14-18, no force, fraud, or coercion)	30	§2G1.3(a)(2)
§ 1591 (minor by force, fraud, or coercion, or minor under 14)	34	§2G1.3(a)(1)
§ 1591 (adult by force, fraud, or coercion)	34	§2G1.1(a)(1)

According to the current sentencing scheme under §§2G1.1 and 2G1.3, the offenses involving the most vulnerable victims and the most egregious forms of coercion carry the highest base offense levels, while related criminal conduct, such as interstate transportation or importation for prostitution, carries correspondingly lower base offense levels. These distinctions appropriately recognize that while each of the above offenses warrant substantial penalties, the use of force, fraud, or coercion to deliberately overcome a victim's will, and the exploitation of particularly vulnerable victims, involve added dimensions of criminality that warrant enhanced offense levels. It is important to maintain the graduated approach established in the existing guidelines, which recognizes varying degrees of criminal culpability depending on each defendant's culpability in the prostitution-related conduct.

Further, the existing guidelines recognize that defendants convicted of interstate transportation and importation for prostitution crimes in violation of 18 U.S.C. §§ 2421 or 2423, or 8 U.S.C. § 1328, are more criminally culpable than defendants convicted only of alien harboring, even where relevant conduct is related to prostitution. Specifically, §§ 2421, 2423, and 1328 offenses all require a specific criminal purpose of prostitution. The alien harboring offense, by contrast, requires no specific criminal intent to further prostitution.

For example, the alien harboring statute, 8 U.S.C. § 1324, could be violated by a landlord taking steps to conceal undocumented tenants, knowing or in reckless disregard of their undocumented status. Such defendants may have knowledge or suspicion that prostitution-related activities are occurring at their properties, but may not share in the specific criminal purpose to further such activities in the same manner as defendants who commit the specific-intent crimes of violating §§ 2421, 2423, or 1328. Moreover, individuals convicted only of alien harboring may have less substantial and extensive contact with the prostitution operation than defendants engaged in interstate transportation or importation for prostitution in violation of §§ 2421, 2423, or 1328. Experience shows interstate transportation or international importation schemes tend to be more extensive and elaborate than the types of localized activity that could constitute harboring.

Increased Offense Levels to Penalize Relevant Criminal Conduct

Despite the potential difference in culpability between offenders, Congress asked the Commission to reconsider the alien harboring guidelines, now sentenced under §2L1.1, with a base offense level of 12. The alien harboring guidelines are two levels below the level 14 base offense level applicable to some prostitution-related offenses under §2G1.1, specifically § 2421 or § 1328 offenses involving adults. To account for the enhanced criminality that distinguishes prostitution-related harboring crimes from other alien harboring offenses, we suggest that the guidelines be amended to enhance penalties when an alien harboring defendant acts *knowingly or in reckless disregard* of the fact that the harboring is in furtherance of prostitution. They should be further increased, we believe, as discussed more specifically below, where the conduct is in furtherance of the prostitution of minors.

1. Add a 2-level SOC for prostitution-related harboring of aliens

The existing disparity between the harboring and prostitution offense guidelines could be effectively addressed by the inclusion in USSG §2L1.1 of additional SOCs. We suggest increasing the §2L1.1 offense level through the addition of a 2-level specific offense characteristic for offenses where the smuggling, harboring, or transportation of the alien was knowingly and intentionally committed in furtherance of prostitution, and where the defendant is an organizer, leader, manager, or supervisor of the criminal activity. The significant advantage of adding an enhancement to §2L1.1 as opposed to inserting a cross-reference would be retaining the applicability of the §2L1.1(b)(2) and (b)(3) for, respectively, number of aliens harbored and prior immigration offenses. These enhancements together could result in significantly increased sentences where the alien harboring conduct is substantial.[63] By addressing the prostitution-related conduct this way, the guidelines would most effectively address both the enhanced immigration-related criminal conduct not addressed under §§2G1.1 or 2G1.3, and the enhanced prostitution-related conduct. A defendant convicted of alien harboring would then face increased offense levels for both immigration-related offense conduct and prostitution-related offense conduct.

The directive only specifies that the organizer/leader role must be in connection with "the criminal activity." To avoid inappropriately including less culpable offenders, we believe that any such enhancement should require a finding of knowledge or reckless disregard of the furtherance of prostitution. As long as there is a knowledge requirement, a leadership role in *either* the immigration-related conduct or the prostitution-related conduct would be sufficient to warrant the application of the enhancement. An application note in this regard might also provide useful guidance.

We believe that limiting the SOC to those defendants who act as an organizer, leader, manager, or supervisor would ensure that only the most culpable defendants receive this enhanced

---

[63] Specifically, the harboring-related conduct addressed under §2L1.1(b)(2)-(b)(3) could result in a combined increase of up to 13 levels for a defendant with two prior immigration-related convictions implicated in the harboring of 100 or more aliens; up to 8 levels for one prior immigration offense and 25 or more aliens, or a five-level increase for one prior immigration offense and 6 or more aliens.

sentence. The enhancement would, at the same time, redress the current failure of §2L1.1 to distinguish between prostitution-related harboring offenses and other forms of harboring offenses that may lack the additional criminality and societal harm associated with prostitution. Because the organizer/leader requirement is a limiting precondition and is not itself a further enhancement based on role, it would not present any double-counting issue with regard to any applicable role adjustment pursuant to §3B1.1. Thus, while defendants whose offense levels are increased by the prostitution-related enhancement will likely receive the role adjustment under §3B1.1, their sentence would not be increased twice because of role. It would be increased once because of furthering prostitution, and once because of role. An application note so explaining may be beneficial.

2. Additional Recommended Enhancement in Cases Involving Prostituted Minors

In the case of prostituted minors, the lowest base offense level under §2G1.3 is level 24, making the disparity with §2L1.1 more significant than in the case of adults, where offense levels under §2G1.3 begin at level 14. USSG §2L1.1(b)(4) currently adds two levels where the person harbored is a minor unaccompanied by a parent or grandparent. The proposed enhancement discussed above would bring the offense level to 16 in the case of alien harboring in furtherance of prostitution where the person harbored is a minor.

If the Commission were to adopt the two-level specific offense characteristic we propose including in §2L1.1, in cases involving the prostitution of alien minors, there would still be an eight-level disparity between the alien harboring offense under §2L1.1 (level 16) and the base offense level of 24 under §2G1.3. Therefore, we would suggest adding an additional four levels where the defendant's harboring furthers the prostitution of a minor, and where the defendant acts knowingly or in reckless disregard of the fact that the harboring was in furtherance of the prostitution of a minor. This further enhancement would bring the offense level under §2L1.1 to level 20.

While this second new enhancement would not achieve precise parity between the prostitution-related harboring of minors and other commercial sex offenses of minors, it would substantially reconcile the offense levels in the two types of cases. Additionally, we believe some disparity is appropriate because, as discussed above in connection with the adult cases, the commercial sex offenses now sentenced under §2G1.3 require proof of more purposeful exploitation and more extensive criminal conduct.

B. New Offenses

Section 1593A, Benefitting Financially From Certain Crimes

The Act creates a new offense, codified at 18 U.S.C. § 1593A, criminalizing knowingly benefitting financially from Chapter 77 offenses such as peonage in violation of § 1581 and document servitude in violation of § 1592.[64] Prior to enactment of the TVPRA of 2008, only the

[64] Section 1593A erroneously references § 1595(a) rather than § 1594(a). Section 1595(a) creates a private civil right of action, whereas § 1594(a) criminalizes attempts to violate Chapter 77. As discussed below, separate amendments to 18 U.S.C. § 1589 include an internal

sex trafficking statute, 18 U.S.C. § 1591, contained a provision criminalizing benefiting financially from participation in the trafficking venture.

Section 1593A articulates additional theories of liability for previously existing offenses, rather than creating qualitatively distinct offenses. The "benefitting financially" theory of culpability holds those who knowingly participate for profit in a venture that engages in Chapter 77 offenses criminally liable to the same extent as those who commit the offenses themselves. Acts of benefitting financially from participation in a venture in violation of § 1593A should therefore be sentenced to the same extent as the underlying Chapter 77 violations committed by the venture.

Because each of the three underlying violations referenced in § 1593A is sentenced under USSG §2H4.1, we believe § 1593A should also be indexed to §2H4.1. Section 2H4.1(a)(2) applies a lower base offense level to document servitude offenses in violation of 18 U.S.C. § 1592. Violations of § 1593A that are based on participation in a venture that engages in document servitude in violation of 18 U.S.C. § 1592 should also be sentenced with the lower base offense level applicable to § 1592. Section 2H4.1(a)(2) should so clarify through amended language specifying that the base offense level of 18 set forth in §2H4.1(a)(2) applies to violations of § 1592, violations of § 1593A where the Chapter 77 offense engaged in by the venture is a violation only of § 1592, and attempts in violation of § 1594(a) to violate § 1592.[65]

§ 1351 – Fraud in Foreign Labor Contracting

The new fraud in foreign labor contracting offense created by the Act makes it unlawful to knowingly and with intent to defraud recruit, solicit, or hire a person outside the United States for purposes of employment in the United States by means of materially false or fraudulent pretenses, representations or promises regarding that employment.

As both the plain language and the legislative history make clear, this offense is distinct from Chapter 77 offenses, such as forced labor that involve compelling or coercing a person's labor or service against his or her will by prohibited means, and is intended to apply to criminal acts that fall short of the forms of coercion proscribed in Chapter 77. As stated in the legislative history, 154 Cong. Rec. H10888-01,

> "This statute is intended to capture situations in which exploitative employers and recruiters have lured heavily-indebted workers to the United States, but *did not obtain their*

"benefitting financially" provision.

[65] Section 2H4.1(a), in setting forth distinct base offense levels, includes the language "apply the greater." This language is inappropriate, we believe, as §§2H4.1(a)(1) and (a)(2) each apply to distinct types of offenses. We recommended that the words "apply the greater" be removed, that language be added in subsection (a)(1) to the effect of "in the case of offenses not described in subsection (a)(2)," and that under subsection (a)(2) the language "offense under 18 U.S.C. § 1592" be amended to read "offense under 18 U.S.C. § 1592, or under § 1593A where the venture has engaged in an act in violation of § 1592, or under § 1594(a) where the attempt was an attempt to violate § 1592."

labor or services through coercion sufficient to reach the level of the Chapter 77 Slavery/Trafficking offenses.... This Section [has] a five year statutory maximum in recognition that the victims of fraudulent labor recruiting are *at high risk of being held in servitude, and that prosecutors should not have to wait for the abuse to rise to the highest levels of criminality* before dismantling these criminal organizations."

Id. at * 10904. Thus, as the legislative history emphasizes, § 1351 fraud offense involves a lower level of criminality than Chapter 77 offenses. As such, we believe lower base offense levels should be applied to the § 1351 fraud offense than to Chapter 77 offenses. One option would be to reference this new crime to §2B1.1. However, the structure of that guideline, including the loss tables, are heavily focused on financial loss rather than worker exploitation, and may not be ideally suited to capturing the characteristics and gradations of criminal conduct in this context.

Another alternative would be to index the offense to §2H4.2, which governs another worker exploitation offense, the willful violation of the Migrant and Seasonal Agricultural Worker Protection Act, which, like § 1351, addresses worker exploitation that falls short of the forms of exploitation criminalized in Chapter 77 and sentenced under §2H4.1. This guideline, like many fraud offenses sentenced under §2B1.1, has a base offense level of 6. Additional specific offense characteristics, beyond those already set forth under §2H4.2(b) pertaining to serious harm and previous acts of similar misconduct, might appropriately be added. These might include enhancements similar to those set forth in §2L1.1, to increase offense levels where the offense involved 6-24 workers, 25-99 workers, or 100 or more workers.

Further enhancements might be added where the defendant engaged in coercive conduct. Examples might include confiscation of the workers' identification documents, manipulation of debts to intimidate the workers, and overcrowded, unsanitary living conditions. Such enhancements would address the added harms from mistreatment of the workers.

C. Other Modifications to Chapter 77

As the Commission notes, Subtitle C of Title II of the TVPRA of 2008 made amendments to 18 U.S.C. §§ 1583, 1584, 1589, 1590, 1591, and 1592.

Obstruction Subsections

The TVPRA of 2008 added subsections to several Chapter 77 offenses that criminalize obstructing the enforcement of those trafficking statutes. Because the obstruction subsections are contained within the respective statutes, they would, absent further Commission action, be indexed to the underlying offense criminalized in each statute. For example, 18 U.S.C. § 1581 – the only Chapter 77 statute already containing an internal obstruction subsection prior to the TVPRA of 2008 – is indexed to §2H4.1. This guideline applies regardless of whether the defendant committed peonage itself, as proscribed in § 1581(a), or obstructed the peonage investigation in violation of § 1581(b).

These new obstruction provisions are critically important to enforcing anti-trafficking statutes. Most obstruction offenses, such as those prohibited under 18 U.S.C. §§ 1503 and 1512, apply only *after* a federal investigation or federal proceeding is initiated. The new Chapter 77 obstruction provisions, however, contain no such limitation. Thus, these new statutes provide a

powerful means of punishing the obstructive conduct that often perpetuates trafficking offenses. Such conduct includes threatening victim-witnesses and third-party witnesses, quickly returning victims to their home country if they complain or threaten to take action, or altering, concealing, or destroying evidence of the offense. For that reason, the Commission, consistent with its prior treatment of obstructing a peonage investigation, should index the obstruction offenses with the underlying trafficking offenses.

Additional Amendments

An amendment to § 1589 imposed criminal liability for "benefitting financially" from forced labor offenses in violation of § 1589. No amendment to the guidelines is necessary regarding this provision as it articulates an alternate theory of liability for violating the forced labor statute and should be sentenced as any other § 1589 violation (just as "benefitting financially" violations of § 1591 which prior to the Act already contained a similar internal "benefitting financially" provision and has always been sentenced like other sex trafficking violations.

Further statutory amendments clarify the definitions of terms such as "serious harm" and "abuse of the legal process." Because these amendments clarify rather than alter the scope of the crimes defined in these statutes, 154 Cong. Rec. H10888-01, at * H10904 ("Section 222 further clarifies these concepts to reflect the various and subtle forms of coercion used by traffickers in light of the experiences of prosecutors and non-governmental organizations in combating trafficking and assisting victims), they do not warrant amendment of the applicable guidelines.

Nonetheless, the Department respectfully draws the Commission's attention to several issues. First, while the title of Chapter 77 was amended after the enactment of the Trafficking Victims Protection Act of 2000 from "Peonage and Slavery" to "Peonage, Slavery, and Trafficking in Persons," the title of §2H4.1 was not correspondingly amended. We recommend that the Commission now amend the title of this guideline to "Peonage, Slavery, and Trafficking in Persons," or "Peonage, Slavery, Forced Labor, Document Servitude, and Trafficking in Persons," to accurately reflect the scope of the applicability of that guideline.[66]

Similarly, at several points within §2H4.1, the guidelines incorporate the outdated and under-inclusive "peonage or involuntary servitude" language referencing the pre-TVPA scope of Chapter 77 rather than the updated reference to all Chapter 77 offenses sentenced thereunder. Specifically, §2H4.1(b)(3) references the duration of the "condition of peonage or involuntary servitude," and should be amended to reference more accurately either the duration of the "condition of peonage, involuntary servitude, forced labor, or document servitude . . ." or the duration of "service in violation of Chapter 77."

---

[66] The current issues for comment, under the heading of "Miscellaneous Amendments," suggest changing the title of §2H4.1 to incorporate the new recruitment or use of child soldiers offense codified at 18 U.S.C. § 2442. We oppose referencing the new Child Soldiers offense to this guideline, as set forth in detail below.

Likewise, in §2H4.1(b)(4), the language "during the commission of, or in connection with, the peonage or involuntary servitude offense," should be amended to read "during the commission of, or in connection with, the Chapter 77 offense," or, alternatively, during the commission of, or in connection with, the peonage, involuntary servitude, forced labor, or document servitude offense."

Moreover, the commentary to §2H4.1, at paragraph 3, states that "if the offense involved the holding of more than ten victims in a condition of peonage or involuntary servitude, an upward departure may be warranted." This commentary, if retained as commentary, should similarly be amended to clarify that it applies to any Chapter 77 offense. As a separate point, however, the Department respectfully recommends that the Commission consider removing this commentary and replacing it with an additional enhancement based on the number of victims, similar to the comparable enhancement under §2L1.1. While the multiple-count adjustment under USSG §3D1.4 adds up to five levels, some trafficking cases have involved the exploitation of dozens or hundreds of victims. Under §2L1.1(b)(2), conduct implicating over 25 persons would add six levels, and conduct implicating over 100 persons would add nine levels. Because courts may be more likely to apply an enhancement to formulate a within-guidelines sentence than to grant an upward departure beyond the guidelines range, consideration should be given to adding specific offense characteristics based on significant numbers of victims in place of the commentary pertaining to an upward departure.

We raise one final issue concerning the guidelines for 18 U.S.C. § 1591 offenses. USSG §2G1.3(b)(4) includes a specific offense characteristic that calls for a 2 level increase if the offense involved the commission of a sex act or sexual contact, or if the defendant was convicted of violating 2422(b) or 2423(a) or another non-1591 offense. It is not clear when that specific offense characteristic would not apply. Our understanding from conversations with Commission staff is that the SOC was meant to distinguish between attempt cases or cases where no sex act took place and those where the child actually engaged in a sex act. It would be useful if the Commission would create an application note that clarifies when the SOC should be applied.

6. MISCELLANEOUS AMENDMENTS

We have comments on two of the eleven miscellaneous amendments: Part B – Proposed amendments to include offenses created or amended by the Consumer Product Safety Improvement Act of 2008; and Part E – Proposed Amendments to include an offense created by the Child Soldiers Accountability Act of 2008. We also submit comments on the proposed changes made in response to the new offense criminalizing the creation of "morphed images" under the PROTECT Our Children Act of 2008.

Part B – Proposed Amendments to Include Offenses Created or Amended by the Consumer Product Safety Improvement Act of 2008

The Commission's proposal with respect to the Consumer Product Safety Act ("CPSA") (15 U.S.C. §§ 2051-2089), the Federal Hazardous Substances Act ("FHSA") (15 U.S.C. §§ 1261-1278), and the Flammable Fabrics Act ("FFA") (15 U.S.C. §§ 1191-1204) is required by recent congressional amendments to those Acts ("the Acts"). The proposed amendments add violations of those Acts to existing guideline §2N2.1 and amends Appendix A (Statutory Index) to include the Acts.[67] The Department of Justice opposes the amendment proposed by the Sentencing Commission. While we agree that the guidelines need to be amended to respond to recent changes to the CPSA, FHSA, and FFA, DOJ and the CPSC believe the Commission's proposal is premature. The sentencing issues raised by the CPSIA are many and complex and deserve a complete review by the Commission. We think this review should include consultations with prosecutors and the CPSC. Given the congressional concern and seriousness of the offenses, we believe it appropriate for the Commission to continue work on the sentencing issues raised by the Act beyond the current amendment year, with a goal of completing implementing guidelines in the next amendment year. To address the Commission's proposal fully, we first summarize briefly the recent changes to the Acts, all of which deal with consumer products.

Background on Recent Changes to Consumer Product Laws

News stories of dangerous consumer products, from lead paint in toys to dangerous cribs, have led to increasing public concern over the last decade. "Over the last year we have read distressing reports in the newspapers of tainted pet food, toothpaste, and other products from China. These are troubling revelations, made even more disconcerting by the reports of lead tainted toys; lead is a substance which can stunt the mental and physical development of children." 154 Cong. Rec. E1709-01, 110th Cong. (2008) (statement on conference report of Rep. Rush D. Holt). Congress responded to this concern last year by holding numerous hearings on the issue of consumer product safety.[68] Congress' interest in the subject culminated with the passage of the

---

[67] The proposed amendment specifically references 15 U.S.C. §§ 1192, 1197(b), 1202(c), 1263, and 2068 to guideline §2N2.1.

[68] *See, e.g., Safety of Phthalates in Consumer Products: Hearing before the Subcomm. on Commerce, Trade, and Consumer Protection of the House Energy and Commerce Comm.*, 110th Cong. (June 10, 2008); *Children's Product Safety and Consumer Product Safety Commission Reform: Hearing before the Subcomm. on Commerce. Trade, and Consumer Protection of the House Energy and Commerce Comm.*, 110th Cong. (Nov. 6, 2007); *Enhancing the Safety of Our*

Consumer Product Safety Improvement Act of 2008 ("CPSIA"). The CPSIA amended three of the statutes administered by the Consumer Product Safety Commission ("CPSC") – the CPSA, the FHSA, and the FFA. Among other things, these amendments greatly increased the criminal penalties for violations of the CPSA, FHSA, and FFA.

A. Regulatory Scheme Prior to the CPSIA

Prior to passage of the CPSIA, the maximum sentence for a knowing and willful violation of the CPSA was one year. Prosecutions under the CPSA were very rare for two reasons. First, a defendant had to be notified of noncompliance by the CPSC before being prosecuted. Second, at the time, violations of the CPSA were merely Class A misdemeanors.

Likewise, the FFA, prior to amendment, was only punishable as a Class A misdemeanor for willful conduct. On the other hand, the FHSA had a two-tiered penalty scheme. Strict liability offenses were Class B misdemeanors, and second and subsequent offenses or offenses committed with the intent to defraud or mislead were Class A misdemeanors.

Consequently, the deterrent value of prosecutions of violations of the Acts was low; and as a result, the most serious cases were brought using other statutes under which more stringent penalties could be obtained.

B. Increased Sentences Under the CPSIA

In enacting the CPSIA, Congress greatly enhanced the maximum sentences under the CPSA, FHSA, and FFA. Penalties for knowing and willful violations of the CPSA and FFA were increased from one-year misdemeanors to five-year felonies. Strict liability offenses under the FHSA remain Class B misdemeanors; however, penalties for second and subsequent offenses or offenses committed with the intent to defraud or mislead were increased from one-year misdemeanors to five-year felonies.[69]

Proposed Amendment to Establish a New Guideline §2N4.1

The Sentencing Commission's proposal would severely impact effective enforcement of the CPSA, FHSA, and FFA. Section 2N2.1 currently establishes a base offense level of 6, with a cross reference to §2B1.1 for offenses involving fraud. Felonies under the CPSA and FFA do not require a showing of fraud. The criminal provisions of the CPSA and FFA require that the offense

---

Toys: Lead Paint, the CPSC, and Toy Safety Standards: Special Senate Hearings, 110th Cong. (Sept. 12, June 18, 2007).

[69] Congress also illustrated its intent to provide harsher penalties for violations of the CPSA, the FHSA, and FFA in the context of civil penalties. The CPSIA increased civil penalties under the all three statutes from a maximum of $1.825 million for any series of related violations to $15 million for any series of related violations.

be committed knowingly and willfully. Under the current proposal, the maximum offense level for a knowing and willful violation of the CPSA or FFA would be 6. The resulting sentencing range (0-6 months with Criminal History Category I) is too low given the statutory mandate of a five-year maximum. 15 U.S.C. §§ 1196, 2070. Congress has determined that violations of these statutes should receive a greater sentence than the current proposal establishes.

The Department of Justice instead proposes establishing a new guideline §2N4.1.[70] Such a guideline would ensure that sentences reflect the gravity and magnitude of the conduct at issue. As explained below, these higher sentences would be accomplished by boosting the underlying offense level in circumstances of aggravated and/or repeat conduct, adding a specific offense characteristic for violations of the CPSA and FFA, and cross referencing §2B1.1 for violations of the FHSA committed with the intent to defraud.

A. Proposed New Guideline, §2N4.1:

(a) Base Offense Level: **6**

(b) Specific Offense Characteristic

(1) If the offense resulted in a substantial likelihood of death or serious bodily injury, increase by **8** levels.

(2) If the defendant was convicted under 15 U.S.C. § 1263 after sustaining a prior conviction under 15 U.S.C. § 1263, increase by **4** levels.

(3) If the defendant was convicted under 15 U.S.C. §§ 1192, 1197(b), 1202(c), or 2068, and the gain resulting from the offense exceeded $5,000, increase by the number of levels from the table in §2B1.1 (Theft, Property Destruction, and Fraud) corresponding to that amount.[71]

(c) Cross References

(1) If the offense involved fraud, apply §2B1.1 (Theft, Property Destruction, and Fraud).[72]

(2) If the offense was committed in furtherance of, or to conceal, an offense covered by another offense guideline, apply that other offense guideline if the resulting offense level is greater than that determined above.

---

[70] DOJ agrees that Part N and Subpart 2 should be amended to add "consumer products."

[71] *See* §2B1.4 for an existing Guideline with virtually identical language.

[72] Language taken from §2N2.1.

Commentary

Statutory Provisions: 15 U.S.C. §§ 1192, 1197(b), 1202(c), 1263, 2068.

B. Substantial Likelihood of Death or Serious Bodily Injury

Although courts may always consider upward departures, the Department believes that an upward adjustment for endangering the public is an appropriate increase. Without this provision, a defendant convicted of a misdemeanor violation of the FHSA that resulted in a substantial likelihood of death or serious bodily injury could avoid imposition of a term of imprisonment.[73]

C. Repeat Offenses

We also propose a specific offense characteristic that would result in an upward adjustment of 4 levels for repeat offenses under the FHSA. This upward adjustment is appropriate because under the FHSA's penalty provision, 15 U.S.C. § 1264, a second offense is punishable as a five-year felony, even absent the "intent to defraud or mislead" that otherwise is a necessary element of a felony offense.

D. Mens Rea

We also believe that §2N4.1 should contain a cross reference that applies §2B1.1 if the offense involves fraud (FHSA offenses). This proposed cross reference is identical to the cross reference in §2N2.1 for violations of the Food, Drug, and Cosmetic Act ("FDCA"). This cross reference is appropriate because both the FHSA and FDCA require an "intent to defraud or mislead." 15 U.S.C. § 1264. Thus, fraud violations of the FHSA should be treated similarly to fraud violations of the FDCA.

Our proposal also adds a specific offense characteristic in order to account for the different mens rea requirements of the Acts. The FHSA contains a different mens rea requirement than the CPSA and FFA. Felony violations of the FHSA require an "intent to defraud or mislead." 15 U.S.C. § 1264. Felony violations of the CPSA and FFA require knowing and willful conduct. 15 U.S.C. §§ 1196, 2070. Because of the discrepancy in mens rea for the Acts, an additional specific offense characteristic is necessary to adequately address sentencing for the CPSA and FFA.

---

[73] Under the Commission's proposal, the defendant would receive an offense level of 6 because the FHSA misdemeanor provisions are strict liability and §2B1.1 would not apply. *See* 15 U.S.C. § 1264.

E. Gain in CPSA and FFA Cases

We include in our proposal a specific offense characteristic accounting for "gain" identical to the one in §2B1.4. Adoption of an offense characteristic that specifically references "gain" is appropriate because loss is difficult to identify in consumer product cases. For example, in one case, the defendant hired employees to remove the child restraint mechanism from lighters. *See United States v. Anthony*, 280 F.3d 694 (6th Cir. 2002). "Loss" in this type of case, like other consumer products cases, is extremely difficult to determine. A much easier to determine (and more accurate) measure of culpability in these cases is the gain that resulted from the offense.

We recognize that §2B1.1 currently instructs courts to "use the gain that resulted from the offense as an alternative measure of loss only if there is a loss but it reasonably cannot be determined." USSG §2B1.1, Application Note 3. However, because courts have struggled to adapt the basic economic offenses table to offenses where the loss is not readily quantifiable, we believe that inclusion of gain in the specific offense characteristic will facilitate the use of gain as a measure of loss. *Id.* (providing rules for construction of loss).

Part E – Amendments to include an offense created by the Child Soldiers Accountability Act

In 2008, Congress passed the Child Soldiers Accountability Act, Public Law No. 110-340, demonstrating its commitment to punishing violations of human rights committed in the United States and abroad. This new law provides an important tool to end the recruitment and use of child soldiers under the age of 15 to engage in hostilities. Jurisdiction under this statute extends to anyone who is present in the United States, regardless of where they committed the crime. The Commission now seeks views on whether the new offense found at 18 U.S.C. § 2442 should refer to §2H4.1 (Peonage, Involuntary Servitude and Slave Trade) or one or more other existing guidelines. Alternatively, the Commission proposes undertaking a broader review of human rights offenses generally, and including the new offense concerning child soldiers as part of that review.

The Department of Justice opposes referring the new child soldiers crime, 18 U.S.C. § 2442, to §2H4.1 or to other existing guidelines. Section 2H4.1, which addresses "involuntary servitude" and focuses primarily on uncompensated labor, is wholly inadequate to capture the criminal conduct at issue in the child soldier offense. The use and recruitment of child soldiers – which takes place almost exclusively during time of war or active armed conflict – involves much more than the use of forced labor; it involves the use of children to take up arms to kill, rape, and maim others – including their own family members. Additionally, child soldiers are often raped, disabled, or maimed, denied educating and are inured to violence, thereby complicating their possibility rehabilitation and re-assimilation into society. The aggravating elements of this crime are not represented in §2H4.1.

If the Commission insists on referring this crime to §2H4.1, we strongly recommend creating significant enhancements to be applied where children are used to kill or to commit other offenses. Additional specific offense characteristics would be needed to address the fact

that the recruitment and use of child soldiers almost always involves multiple victims — usually hundreds, if not thousands, of children.

We think the better course of action is for the Commission to postpone referencing this crime to a particular guideline during this amendment year, and instead, undertake a broader review of this and other similar crime that could result in the promulgation of a new umbrella guideline for human rights offenses, including Genocide (18 U.S.C. § 1091), War Crimes (18 U.S.C. § 2441), Torture (18 U.S.C. § 2340A) and Maiming with Intent to Commit Torture (18 U.S.C. § 114). As we have noted in previous correspondence with the Commission, these crimes are different from traditional criminal conduct in terms of their far-reaching societal impact and the international acknowledgement of their gravity. Significantly, most human rights offenders, unlike many domestic criminals, have no cognizable criminal history in the United States. Likewise, their treatment in the federal sentencing guidelines has never been comprehensively reviewed by the Commission. For example, to date, there is no governing guideline applicable to war crimes.

Because of the limitations of the existing guidelines with respect to human rights violations, we ask the Sentencing Commission to conduct research and hold hearings into the kinds of conduct covered by these statutes and to create a guideline that is unique to human rights violations over the next two amendment years.

Issue for Comment – PROTECT our Children Act of 2008 and "Morphed Images"

The Commission is considering whether any action is needed with respect to the new crime found at 18 U.S.C. § 2252A(a)(7), which prohibits the creation of an image of "child pornography that is an adapted or modified depiction of an identifiable minor." If the Commission does nothing, defendants who are convicted of this crime would be sentenced pursuant to §2G2.2. As we have made clear in previous correspondence with the Commission, the defendants who create these images should not be treated on par with those who distribute, receive, and possess them. Their conduct is more culpable, and the guidelines should reflect that fact.

We acknowledge that an individual who photographs the actual molestation of a child has engaged in more serious conduct than someone who alters an otherwise innocent image so that it now depicts sexual conduct. We do not advocate that those who violate § 2252A(a)(7) should be treated identically to those who violate § 2251. However, we categorically reject any notion that the production of a morphed image of child pornography and the introduction of that image to this illegal market is on the same level as the simple distribution of such images. Defendants who violate 2252A(a)(7) have inflicted permanent and significant reputational harm on the real children they victimized. Once on the Internet, these humiliating and degrading images will haunt the children for their entire lives. Moreover, defendants who produce morphed images add to the supply of child pornography, thereby stoking the appetites of pedophiles and leading to even greater demand for such material.

Prior to the creation of this crime, there were essentially two categories of criminality: those who produce these images and those who trade and collect them. A violation of §

2252A(a)(7) does not fall within either of those categories. The culpability of this kind of offender falls in-between those two categories. He has done something more serious than distribution, but less serious than production of an image through the molestation of a child. The guidelines must acknowledge this fact to prevent a fundamental misunderstanding about the seriousness of this new offense.

Given the unique nature of this crime, it may be most appropriate to create a stand-alone guideline to address this offense. Alternatively, the sentence for this offense could be calculated pursuant to §2G2.1, but with a reduction in the sentencing level to reflect the fact that the minor depicted in the sexually explicit images was not in fact engaging in sexually explicit conduct. Another option would be to apply §2G2.2 to this crime, but with an increased base offense level to reflect that the defendant did more than trade in images, he actually created them.

7. INFLUENCING A MINOR

The Commission has proposed an amendment that attempts to resolve a three-way circuit split with respect to the applicability of the undue influence enhancement found in §2A3.2 and §2G1.3. The Eleventh Circuit has found that the enhancement applies in all applicable cases, including those involving undercover officers posing as children. *United States v. Root*, 296 F.3d 1222 (11th Cir. 2002). In contrast, the Seventh Circuit has held that the enhancement does not apply to cases involving undercover officers. *United States v. Mitchell*, 353 F.3d 552 (7th Cir. 2003). The Seventh Circuit then goes further, holding that the enhancement also does not apply in cases where there is a child victim but the defendant and the victim never engaged in illicit sexual conduct. The Sixth Circuit split the difference in *United States v. Chriswell*, 401 F.3d 459 (6th Cir. 2005). In that case, the Sixth Circuit also ruled that the undue influence enhancement does not apply to undercover cases. However, the Sixth Circuit disagreed with the Seventh Circuit, and concluded that the enhancement does apply in cases involving attempted sexual conduct with an actual minor.

We recommend that the Commission resolve this circuit conflict by adopting Option 1 of the three proposals published for comment. With respect to the applicability of the undue influence enhancement in attempt cases involving real minors, we recommend that the Commission clarify that the enhancement should apply in such cases, rejecting the approach taken by the Seventh Circuit on that particular issue. A defendant could have used undue influence on a minor even in cases where the sex act was not completed. This is especially so in cases where the act was not completed due to law enforcement intervention. As such, the guidelines should clearly permit the application of this enhancement in attempt cases.

We also believe the undue influence enhancement should apply in cases involving undercover operations for two primary reasons. First, one of the purposes of the guidelines is to punish more serious conduct more severely, and to punish comparable conduct in a similar fashion. If the undue influence enhancement did not apply to defendants caught in undercover operations, we believe the guidelines would fail to meet this core aim. Restricting the application of the undue influence enhancement would necessarily result in scenarios where two defendants who engaged in comparable criminal behavior would not receive the same guideline calculation simply because one had targeted a real child and one had, unknowingly, targeted an adult whom he thought was a child. The defendant who had unwittingly targeted an undercover officer is no less culpable, but he would nonetheless essentially receive a two-level benefit due to a fact entirely beyond his intent or control.

Next, the application of the undue influence enhancement to undercover cases is necessary to preserve the internal consistency of the relevant guidelines. As pointed out by the Eleventh Circuit in *Root*, the application notes define "victim" to include "an undercover law enforcement officer who represented to a participant that the officer had not attained the age of 16 years." The authority of this declaration, which was made to ensure that offenders caught in this manner are appropriately punished, would be undermined if the Commission began carving out exceptions to the rule.

We are not unsympathetic to the concerns raised by the Sixth and Seventh Circuits concerning possible difficulties in the application of this enhancement to cases born from undercover operations, specifically, concerns as to how the district court should or could determine whether the "victim's" will was overborne through the use of undue influence. We also acknowledge that there may be some concerns that law enforcement may tailor their interactions with defendants to induce behavior that may trigger the application of this enhancement. While we acknowledge those points, we ultimately do not find them persuasive.

As a matter of policy, we think it would be a mistake to limit application of this enhancement out of concern for the outlier case, whether that be one with murky facts or possible law enforcement over-reaching. Every sentencing is an intensive, fact-based inquiry. That process can properly identify those cases where application of the enhancement is inappropriate. There is no need to categorically take the option off of the table. The district courts are capable of assessing the defendants' conduct, as well as that of the law enforcement officers, and making the appropriate determination.

We also think that the Sixth and Seventh Circuits' concern about the application of the enhancement could be addressed by adding a comment in the Application Notes that would direct the courts in undercover cases to focus on the defendant's conduct and to consider what he attempted to accomplish with his statements, rather than on whether the "minor's" will was actually overcome. This would make clear that the courts need not engage in hypothetical exercises in which they attempt to assess whether the defendant's activity would have overcome the will of a real child.

Finally, we are skeptical that law enforcement officers could truly tailor the interactions in such a way that would "trick" the defendant into using excessive influence. For example, there is a rebuttable presumption that the enhancement applies in cases where there is an age difference of more than 10 years. In virtually all cases, the officers must pose as a child who is under the age of 16. They have no control over the actual age of the defendant, or how old the defendant represents himself to be. There is no meaningful opportunity to manipulate the situation to trigger the rebuttable presumption in favor of application of the enhancement.

8. COMMISSION OF OFFENSE WHILE ON RELEASE

The Department of Justice has no comment on the proposed changes to this guideline.

9. COUNTERFEITING AND "BLEACHED NOTES"

The Commission has proposed an amendment to guideline applicable to counterfeiting offenses, §2B5.1, to address counterfeiting offenses involving "bleached notes."

The U.S. Secret Service (USSS) and the Department of Justice fully support the proposed changes to §2B5.1 and Appendix A, and we recommend the Commission adopt these changes as set forth in the proposal. Currency illegally produced on genuine paper is counterfeit. Furthermore, defendants who "bleach" genuine United States currency paper typically manufacture a highly deceptive counterfeit note that is easier to pass to unsuspecting victims. These counterfeiters rely on the "distinctive counterfeit deterrents" and unique feel of genuine currency paper to create counterfeit currency that is often difficult to detect or identify. Consequently, "bleached note" counterfeiters should be sentenced as counterfeiters, subject to the provisions governing the manufacturing of counterfeit currency.

We believe this amendment should only have a minimal impact, if any, on the current enforcement of counterfeiting laws under Chapter 25 of Title 18. Since the agency's inception in 1865, the USSS has been actively investigating individuals who engage in the production and distribution of counterfeit currency. The USSS will continue, as it always has, to place a high investigative priority on combating counterfeit currency.

We are hopeful the increase of prison sentences under the proposed amendment to §2B5.1 will not only deter those considering engaging in the counterfeiting of U.S. currency but also those already convicted of crimes identified in the counterfeiting statutes.

- - -

Thank you for the opportunity to provide our views, comments, and suggestions on the published proposals and issues for comments. We appreciate all the hard work done by the Commission and the Commission staff in fulfilling the Commission's statutory mandate to review and amend the sentencing guidelines. We look forward to continuing to work with the Commission in this important area of the law.

Sincerely,

Jonathan J. Wroblewski
Director, Office of Policy and Legislation
Criminal Division

cc: U.S. Sentencing Commissioners
Judy Sheon, Staff Director