
PUBLIC COMMENT

2003 AMENDMENT CYCLE

(March 17, 2003 Submissions)



United States Sentencing Commission

March 2003



U.S. Department of Justice

Criminal Division

Office of the Assistant Attorney General

Washington, DC 20530-0001

March 18, 2002

Honorable Diana E. Murphy
Chair, U.S. Sentencing Commission
One Columbus Circle, NE
Suite 2-500, South Lobby
Washington, DC 20002-8002

Dear Judge Murphy:

On behalf of the Department of Justice, I submit the following comments regarding the proposed amendments to the federal sentencing guidelines and issues for comment published in the Federal Register on January 17, 2003. We look forward to continuing to work with the Commission during the remainder of this amendment year on all of the published amendment proposals.

* * * * *

CAMPAIGN FINANCE

Under emergency amendment authority, the Commission promulgated a temporary guideline amendment, effective January 25, 2003, to implement the Bipartisan Campaign Reform Act of 2002. The Department of Justice supports the temporary amendment and now favors the Commission's proposal to make the amendment permanent.

BODY ARMOR

The Department supports the Commission's proposed amendment to provide a new adjustment at §3A1.5 for the use of body armor in an offense involving a crime of violence or drug trafficking crime. In response to the issue for comment, we believe the adjustment should be based on all conduct within the scope of relevant conduct but should be triggered only if the defendant (1) used body armor himself or (2) otherwise knew that the offense involved the use of body armor. This formulation would ensure that the adjustment apply only to those who knowingly participate in conduct involving body armor – conduct that significantly increases the risk of harm to law enforcement and the public at large – and thus limit the applicability of the adjustment to those culpable for such increased risk.

OXYCODONE

Noting the marked increase in abuse and diversion of OxyContin and other forms of oxycodone, the Commission published a proposed amendment to adjust penalties for offenses involving oxycodone. The proposal would base sentences for such offenses on the actual weight of oxycodone involved in the offense and would set the marijuana equivalency at 1 gram oxycodone (actual) = 6,700 grams of marijuana. On February 20, 2003, Drug Enforcement Administration officials briefed Commission staff on the abuse and trafficking of products containing oxycodone.

After careful review, the Department of Justice supports the Commission proposal. The proposed equivalency would significantly increase sentences for OxyContin pills that are more potent than 10 mg strength. For example, under the current total pill weight-based sentencing scheme, approximately 1,500 OxyContin pills (10, 20 or 40 mg strength) correspond to a base offense level of 26 (63-78 months' imprisonment). Under the Commission's actual controlled substance weight-based proposal, far fewer 20 mg pills (746) and 40 mg pills (372) would correspond to level 26. The sentences would not change for 10 mg strength OxyContin pills.

Although we support the proposal, we do so with significant reservations. We note that the proposal will result in significantly lower sentences for combination (non-controlled release) formulations of oxycodone (*e.g.*, Percocet, Percodan, and Tylox). These pills, although weighing much more than the OxyContin formulations, each contain only approximately 5 mg of actual oxycodone. Thus, while approximately 460 Percocet pills presently corresponds to offense level 26, it would take almost 3,000 pills to achieve level 26 under the Commission's proposal. These sentence reductions are of significant concern to us.

The Commission has identified 39 cases sentenced in FY2000 and 2001 that involved OxyContin products. The Commission was able to recalculate the sentences using its proposal for 24 of those cases and determined that the present median sentence of 10 months would increase to 14 months under its proposal. Given the significantly upward trends in OxyContin diversion and abuse, there is a significant federal interest in prosecuting those who illicitly distribute this frequently deadly drug. The higher sentences for the higher concentration OxyContin products that will result from the Commission's proposal will, we believe, more accurately reflect the harm attendant to offenses involving this drug and encourage appropriate federal prosecution.

We are concerned over the sentence reductions that would result with respect to the non-controlled release oxycodone products for several reasons. We are particularly concerned about losing the ability to effectively prosecute individuals who are registered to prescribe and dispense controlled substances (physicians, pharmacists, etc.) and who abuse this privilege by illicitly prescribing or distributing products such as Percocet and Tylox. In our view, the ability to prosecute such defendants is key to maintaining the integrity of the registration system. Moreover, data from the Drug Abuse Warning Network (DAWN) indicate that, although

emergency room mentions of "single-entity oxycodone" (OxyContin)¹ have skyrocketed over the last several years, neither this nor any other data indicate that OxyContin abuse has supplanted the abuse of the combination oxycodone products.

As part of its data analysis, the Commission identified 25 cases sentenced in FY2000 and 2001 that involved oxycodone combination drugs. Upon recalculating the sentences for 22 of these cases under its proposal (assuming a 5 mg potency), the Commission determined that the average sentence would drop from 45 months to 17 months. The Commission further determined that at least six of the 25 cases sentenced involved DEA registrants (4 doctors and 2 pharmacists) although one of these cases was prosecuted for simple possession. Sentences in the remaining five registrant cases ranged from 24 months' probation to 72 months' imprisonment. There is an obvious concern that the enforcement program related to these drugs will be significantly impacted if the guidelines sentences are grossly reduced. Nevertheless, even assuming that fewer prosecutions of cases involving combination (non-controlled release) oxycodone products would occur under the new guidelines, we cannot at this time fully estimate how harmful the impact of such a loss would be.

In sum, we think the Commission's proposal appropriately corrects the disproportionately low sentences that offenses involving single-entity/controlled release oxycodone formulations such as the OxyContin formulations now incur. Due to the inherent complexities of alternative approaches that we and the Commission have considered, and the fact that we believe lowering the sentences for offenses involving combination/non-controlled release oxycodone formulations will affect relatively few cases, we support the Commission's proposal. We expect that the Commission will join the Department in carefully monitoring the sentences under the new guideline and, if appropriate, will revisit the issue in the future.

THREATS AND ASSAULTS ON FEDERAL OFFICIALS

While we recognize the factors that have led the Commission to defer action on this issue, we strongly urge the Commission to make a comprehensive review of the assault and homicide guidelines a top priority in the next amendment year. As we have stated on a number of occasions, we believe the guideline penalties for homicide, other than for first degree murder, are seriously inadequate. While the number of homicides prosecuted in federal court is relatively few because of the limitations of federal jurisdiction, the relevant guidelines are extremely important because of the seriousness of the crimes involved. Similarly, offense involving threats or assaults on federal judges and other federal officials, while very rare, are nonetheless of the utmost seriousness and should be appropriately addressed by the sentencing guidelines.

¹There is one other line of relatively high-concentration oxycodone products that do not contain aspirin or acetaminophen. These products, however, are prescribed less often compared with, for example, the over 7 million prescriptions for OxyContin products in calendar year 2001 and the approximately 26.5 million prescriptions for all oxycodone products. Furthermore, there is no evidence of any significant diversion of these products.

We note that the Commission's Native American Working Group is specifically examining federal homicide and assault crimes. We think the Commission should ask the Native American Working Group to complete its work on these issue by this summer so that the Commission can promptly revisit all of the homicide and assault guidelines in the next amendment year and make adjustments to the guidelines as warranted and as required by recent legislation.

CYBERCRIME

I. Introduction

In the fall of 2002, Congress passed and the President signed into law the Cyber Security Enhancement Act of 2002, part of the Homeland Security Act of 2002, Pub. L. 107-296 (2002). In passing the Cyber Security Enhancement Act, Congress again increased some of the statutory maximum penalties for unauthorized access to or interference with computers, networked communications, and electronic information.²

Also as part of the Act, Congress expressed its intent with regard to the sentencing guidelines for these offenses unequivocally – that the Commission should “ensure that the sentencing guidelines and policy statements reflect the serious nature of [computer crimes], the growing incidence of such offenses, and the need for an effective deterrent and effective punishment to prevent such offenses.”³ To that end, Congress directed the Sentencing Commission to review and, if appropriate, amend the sentencing guidelines applicable to offenses against or involving computers and computer networks. Congress provided a list of eight discrete factors the Commission should consider in conducting its review. We comment here on the factors set forth by Congress and, more generally, on the guidelines applicable to computer crimes.

We believe several of the factors identified for review by Congress – specifically, level of sophistication, number of victims, and restitution – are adequately addressed by the current guidelines. The current guidelines do not reflect, however, the dramatic increase in reported

²In the USA-PATRIOT Act, Pub. L. No. 107-56 (2001), Congress increased the statutory maximum sentence for intentionally damaging a protected computer from five years to 10 years for first time offenders and from 10 years to 20 years for repeat offenders. *See* 18 U.S.C. § 1030(c)(4).

³*See also* 148 Cong. Rec. H4583 (daily ed. July 15, 2002) (statement of Rep. Smith) (“We must improve our Nation’s cybersecurity and strengthen our criminal laws to prevent, deter and respond to [cyber] attacks.”); 148 Cong. Rec. S8902 (daily ed. Sept. 19, 2002) (statement of Sen. Hatch) (stating Congress’s intent to “give judges greater latitude to increase a defendant’s sentence to better account for the seriousness of [a] cyber attack.”).

computer crimes,⁴ Congress's express intent to "increase[] penalties to better reflect the seriousness of cyber crime,"⁵ and the fact that such crimes often cause egregious non-monetary harms. We believe that several specific amendments to the guidelines are appropriate to address these issues.

Congress amended 18 U.S.C. § 1030 expressly to account for some non-monetary harm (for instance, damage to a computer used in furtherance of the administration of justice, national defense, or national security, added by the USA PATRIOT Act as 18 U.S.C. § 1030(a)(5)(B)(v)) and directed the Commission to consider other specific factors that reflect the non-monetary harm that may be caused by computer crimes (such as harms to privacy, critical infrastructures, and public safety). Unlike most economic crimes, computer intrusions sometimes cause relatively little monetary loss, in part because computer offenders may act out of a variety of non-financial motives, including the challenge of penetrating a network, the ability to access private or confidential information, and the desire for "bragging rights" within the online community. Nevertheless, the consequences of computer crimes may be dire – egregious violations of privacy; damage to the computer systems that support national defense, national security, and the administration of justice; impairment of critical infrastructures; and even serious bodily injury or death. These crimes must be effectively deterred and severely punished.

Based on the substantial experience of the Criminal Division in preventing, investigating, and prosecuting computer crimes, we feel these amendments constitute an effective, measured implementation of Congress's intent to "ensure that the sentencing guidelines and policy statements reflect the serious nature of [computer crimes], the growing incidence of such offenses, and the need for an effective deterrent and effective punishment to prevent such offenses."

⁴The annual CSI/FBI Computer Crime Security surveys indicate that in 2000, 70 percent of the companies surveyed indicated that they had been the target of computer crime within the past 12 months; by 2002, that figure had risen to 90 percent. Both the 2000 and the 2002 surveys indicate that only about 40 percent of such victims feel that the harm resulting from the attacks may readily be expressed as "financial loss." In 2000, the total financial loss of the 273 responding companies that felt that they could quantify their loss was more than \$265 million; in 2002, the total financial loss of the 223 companies that quantified their loss was more than \$455 million. See "2000 CSI/FBI Computer Crime and Security Survey," in *Computer Security Issues & Trends*, Vol. VI, No. 1 (Richard Power ed. 2000); "2002 CSI/FBI Computer Crime and Security Survey," in *Computer Security Issues & Trends*, Vol. VIII, No. 1 (Richard Power ed. 2002).

⁵Statement of the Hon. Lamar Smith (R-TX), Chairman, Crime Subcommittee, House Judiciary Committee, hearing on H.R. 3482, the "Cyber Security Act of 2001," February 12, 2002.

II. The Statutory Scheme and Recent Amendments

Three portions of the criminal code proscribe unauthorized access to or interference with computers, networked communications, and electronic information. Section 1030 generally prohibits intentionally accessing a protected computer without, or in excess of, authorization, *see* 18 U.S.C. § 1030(a)(1)-(4); knowingly transmitting a computer command, code or program with intent to cause damage to a protected computer, *see* 18 U.S.C. § 1030(a)(5); knowingly trafficking in devices that facilitate unauthorized access to computers, *see* 18 U.S.C. § 1030(a)(6); and threatening to damage a protected computer, *see* 18 U.S.C. § 1030(a)(7). Section 2511(1) prohibits intentionally intercepting any wire, oral or electronic communication. And section 2701(a) proscribes obtaining, altering, or preventing access to undelivered e-mail by intentionally accessing without, or in excess of, authorization a facility through which an electronic communication service is provided.

The USA-PATRIOT Act, Pub. L. No. 107-56 (2001), included several important amendments of Section 1030. Three of those amendments may have implications for the sentencing guidelines. First, Congress increased the statutory maximum sentence for intentionally damaging a protected computer from five years to 10 years for first time offenders and from 10 years to 20 years for repeat offenders. *See* 18 U.S.C. § 1030(c)(4). Second, Congress prohibited damaging a computer system used by the government in furtherance of the administration of justice, national defense, or national security even if the aggregate damage falls short of \$5,000. *See* 18 U.S.C. § 1030(a)(5)(B)(i). Third, Congress included a new, broad definition of "loss:"

the term 'loss' means any reasonable cost to any victim, including 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 consequential damages incurred because of interruption of service.

18 U.S.C. § 1030(e)(11). In sum, the USA-PATRIOT Act strengthened some of the statutory penalties for computer crimes, brought new destructive conduct within the purview of the federal criminal code, and expanded the definition of loss suffered by a computer crime victim.

Roughly a year after the USA-PATRIOT Act became law, Congress passed the Homeland Security Act of 2002, Pub. L. 107-296 (Nov. 25, 2002), again strengthening the penalties for many computer crimes. Congress increased the statutory maximum to 20 years for attacks on computer systems in which the defendant knowingly or recklessly causes or attempts to cause serious bodily injury. *See* 18 U.S.C. § 1030(c)(5)(A). Congress increased the statutory maximum sentence to life in prison if the defendant knowingly or recklessly causes or attempts to cause death. *See* 18 U.S.C. § 1030(c)(5)(B).

Congress also increased the statutory maximum penalty for obtaining, altering or preventing authorized access to a wire or electronic communication in electronic storage by accessing an electronic communication service without, or in excess of, authorization. *See* 18 U.S.C. § 2701(a). An offender convicted of such conduct for the first time now faces a one-year maximum sentence, and an offender with a prior conviction faces a five-year maximum sentence as opposed to the six-month sentence provided for before the Homeland Security Act. *See* 18 U.S.C. § 2701(b)(2). Moreover, if such an offender is motivated by commercial advantage, malice, or private gain, Congress increased the maximum sentence from one year to five years for a first-time offender and from two years to ten years for a repeat offender. *See* 18 U.S.C. 2701(b)(1).

III. The Guidelines' Current Treatment of Sections 1030 and 2701

With a few notable exceptions, the guidelines currently treat 18 U.S.C. § 1030 violations as basic economic offenses for which §2B1.1 determines a defendant's sentence.⁶ Section 2M3.2 determines the sentence for obtaining national defense information by accessing a protected computer in violation of 18 U.S.C. § 1030(a)(1). Section 2B2.3, the trespass section, determines the sentence for accessing without, or in excess of, authorization a computer of a department or agency of the United States. Section 2B3.2, the extortion guideline, determines the sentence for transmitting with intent to extort a threat to damage a protected computer in violation of 18 U.S.C. § 1030(a)(7). The guidelines currently provide no specific instruction as to how to sentence violations of 18 U.S.C. § 2701.

IV. Comments & Recommendations

Consistent with Congress's instruction to strengthen the penalties for computer crimes and to take into account non-monetary harm caused by such crimes, we recommend several specific Guidelines amendments. We address each of the enumerated factors set forth in the directive to the Commission in the Homeland Security Act and each of the questions posed by the Commission's solicitation for public comment.

A. Loss

The USA-PATRIOT Act amended 18 U.S.C. § 1030 to include a new definition of loss (see above). Application Note 2(A)(v)(III) of §2B1.1 currently instructs courts to include in a loss calculation "reasonable costs to the victim of conducting a damage assessment, and restoring the system and data to their condition prior to the offense, and any lost revenue due to interruption of service." To avoid confusion and promote consistency, we believe the guideline loss definition should be amended to mirror the definition now contained in 18 U.S.C. § 1030.

⁶Guideline §2X1.1 determines the sentence for an attempt to violate any subsection of 18 U.S.C. § 1030(a). It generally instructs courts to apply the appropriate guideline for the substantive offense and then decrease the offense level by 3. *See* U.S.S.G. § 2X1.1(a), (b)(1).

As amended, the definition of loss will be sufficiently broad to capture the monetary harm caused by computer crimes (it does *not*, however, adequately address non-monetary harms such as invasion of privacy, damage to critical infrastructures, and bodily injury or death, which are addressed specifically later in these comments). We thus recommend that §2B1.1, note 2(A)(v)(III) be amended as follows:

Protected Computer Cases.—In the case of an offense involving unlawfully accessing, or exceeding authorized access to, a “protected computer” as defined in 18 U.S.C. § 1030(e)(2), actual loss includes the following pecuniary harm, regardless of whether such pecuniary harm was reasonably foreseeable: ~~reasonable costs to the victim of conducting a damage assessment, and restoring the system and data to their condition prior to the offense, and any lost revenue due to interruption of service; any reasonable cost to any victim, including 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 consequential damages incurred because of interruption of service.~~

B. Level of Sophistication

The guidelines currently account for the level of sophistication of an offense in §2B1.1(b)(8). We believe this offense level increase is adequate and that no further amendment is needed.

C. Commercial Advantage or Private Financial Benefit

Congress directed the Commission to consider whether the guidelines should treat differently a violation of § 1030 that was motivated by commercial advantage or private financial benefit. Congress has expressly treated more severely computer crimes committed with these purposes. An offender who violates 18 U.S.C. § 1030(a)(2) by intruding into a protected computer and obtaining information generally faces a statutory maximum sentence of one year, *see* 18 U.S.C. § 1030(c)(2)(A); if, however, that same offender is motivated by the prospect of commercial advantage or private financial gain he faces a statutory maximum sentence of five years, *see* 18 U.S.C. § 1030(c)(2)(B)(i). In the Homeland Security Act, Congress established a similar increase in the statutory maximum penalty faced by an offender who violates 18 U.S.C. § 2701 with such motives. *See* 18 U.S.C. § 2701(b)(1) (establishing a statutory maximum sentence for offenses committed “for purposes of commercial advantage . . . or private commercial gain” of one year for first offenders and two years for repeat offenders); *cf.* 18 U.S.C. § 2701(b)(2) (establishing a statutory maximum sentence of six months where such motives are absent).

As a general matter, §2B1.1’s loss table addresses monetary motives and harms by punishing an offense in proportion to the loss it causes or is intended to cause. However, in light of Congress’s clearly expressed intent that crimes committed for such purposes be sentenced

more severely, we believe a minimum offense level floor of 12 for such offenses is appropriate (with no provision for any generally applicable penalty enhancement). Such a minimum would place an offender in Zone C of the sentencing table, absent the effect of other mitigating or extenuating specific offense characteristics. A short prison term is the appropriate penalty for these offenses, and, we believe, should be an effective deterrent for an offender who accesses without or in excess of authorization the computer of another in order to obtain commercial advantage or personal financial benefit.

We thus propose adding the following specific offense characteristic to §2B1.1(b):

() If the offense involves violation of 18 U.S.C. §§ 1030 or 2701 and was committed for purposes of commercial advantage or private financial gain and the offense level is less than 12, increase to 12.

D. Intent to Cause Harm

Section 1030 violations committed with intent to cause harm are relatively commonplace; the disgruntled former employee who exacts revenge by attacking his former employer's network, for example, is a figure familiar to prosecutors. Punishing more severely offenders who intend to cause harm than offenders who cause harm unintentionally serves three of the four penological purposes recognized by federal law. Congress provided in the USA-PATRIOT Act for higher statutory maximum sentences for violations of 18 U.S.C. § 1030(a)(5)(A)(i), which applies to computer criminals who act with intent to cause damage. For a first offense, Congress raised the maximum sentence to 10 years, *see* 18 U.S.C. 1030(c)(4)(A); for any subsequent offense, Congress raised the maximum sentence to 20 years, *see* 18 U.S.C. 1030(c)(4)(C).

We believe the Commission should amend §2B1.1 to include a significant offense level increase and an offense level floor that reflects both the purposes of sentencing and Congress's unequivocal intent that the sentences for such crimes be increased. Individuals who violate the law with the intent to harm the life and livelihood of others are a threat to public safety and economic security. We recommend that the guidelines increase the offense level of such offenders by 4, to not less than 14, placing them in Zone D and assuring that, absent a departure, their sentence will include a term of imprisonment.

We suggest that the following specific offense characteristic to § 2B1.1:

() If the offense involved intentionally causing or attempting to cause damage to a protected computer in violation of 18 U.S.C. § 1030(a)(5)(A)(i), increase by 4 levels; if the resulting offense level is less than 14, increase to 14.

E. Violations of Privacy

Personal information such as medical and financial records, diaries and personal correspondence, and other confidential information is increasingly stored on network-accessible digital media, either on networked personal computers or in the custody of third parties such as Internet service providers, credit reporting services, or data storage services. One objective of many computer intruders is to obtain such information. Given computer networks' roles as repositories for private and confidential information, computer intrusions have unprecedented potential to expose the personal information of hundreds or thousands of users at once. A computer intrusion in which the offender obtains personal information causes non-monetary harm that is difficult to capture in the loss table or elsewhere in the current guideline.

For instance, accessing without authorization a hospital's medical records in violation of 18 U.S.C. § 1030 and posting on the web a list of HIV-positive patients may be extremely harmful to both the hospital and the patients even though it may cause little or no measurable economic loss. In fact, at least one hospital has suffered such an intrusion. Several years ago, a hacker accessed a Pittsburgh hospital to obtain the medical records of a popular country western singer. Similarly, accessing a Hotmail web server in violation of 18 U.S.C. § 2701⁷ and reading the personal correspondence of several of Hotmail's subscribers harms each subscriber, although that harm is difficult to quantify. We believe the guidelines should reflect the serious harm that such offenses cause.

Currently, §2B1.1 accounts for violations of privacy by including among a "non-exhaustive list of factors the court may consider" in making an upward departure from a defendant's sentencing range whether "[t]he offense . . . resulted in a substantial invasion of a privacy interest." §2B1.1, note 15(A)(ii). In practice, however, courts seldom depart upward from the guidelines. As a result privacy violations are left unpunished and under-deterred. In cases such as the intrusion into the hospital computer described above, the invasion of privacy is not a footnote to the monetary loss, it is the most significant harm caused by the intrusion. Moreover, even where an intrusion does involve a monetary loss (*e.g.*, where it results in the theft of financial records), the invasion of privacy is a separate and significant harm. In fact, it may be the harm regarded as most egregious by the individual victim.

We recommend increasing by two the offense level of offenders who obtain important private information. In addition, because a violation of the privacy of 50 people causes more harm than a violation of the privacy of a single person, we recommend amending the application note for section 2B1.1(b)(2) to clarify that every individual about whom such information is obtained as a result of a computer intrusion is a "victim" for the purposes of the guidelines.

⁷The guidelines do not currently reference violations of 18 U.S.C. § 2701 to a specific guideline. Section 2701, like section 1030, prohibits unauthorized access to certain computer systems. We believe Appendix A should be amended to reference violations of 18 U.S.C. § 2701 to §2B1.1.

Thus, if a hacker accesses a medical records database and steals 100 people's records, the number of victims would include these 100, not just the computer owner.

We propose (1) adding the following specific offense characteristic:

() (A) If the offense involved knowingly accessing a computer without authorization or exceeding authorized access in violation of 18 U.S.C. §§ 1030 or 2701 and obtaining personal information as a result, increase by 2 levels.

(2) adding the following Application Note to the Commentary:

1. Definitions.—For the purposes of this guideline:

* * *

“Personal information” means sensitive or private information, including but not limited to medical records, financial records, social security numbers, wills, diaries, private correspondence including email, photographs of a sensitive or private nature, or similar information, including such information in the possession of a third party.

(3) amending application note 3(A)(ii) as follows:

(ii) *“Victim” means (I) any person who sustained any part of the actual loss determined under subsection (b)(1); or (II) any individual who sustained bodily injury as a result of the offense; or (III) any individual whose personal information was accessed during a violation of 18 U.S.C. §§ 1030 or 2701. “Person” includes individuals, corporations, companies, associations, firms, partnerships, societies, and joint stock companies.*

F. Computers Used by the Government in Furtherance of National Defense, National Security, or the Administration of Justice & Disruptions of Critical Infrastructures⁸

Computer networks are 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 a critical role in ensuring that the justice system performs effectively and efficiently and that dangerous criminals are kept off the streets. In one notable case, a convicted felon hacked into the computer network of a United States District Court in an effort to modify his sentence. Intrusion into networks used in

⁸Although Congress listed these as two separate factors, we believe they are so closely related that they are best addressed by a single amendment to the guidelines.

furtherance of the administration of justice should be appropriately accounted for in the guidelines. Accordingly, we believe a four level increase should be provided for intruding into such networks.

Computer networks are also used to maintain and operate the critical infrastructures upon which our society and economy rely. Such critical infrastructures, whether publicly or privately held,⁹ include the provision of health care, the production and distribution of energy, public transportation, emergency response, national defense and national security, and the administration of justice. The prospect of attacks on, or intrusions into, these networks raises harrowing possibilities. For instance, in March 1997, a computer intrusion into a telephone company serving Worcester, Massachusetts disabled the night landing lights and communications with airport emergency services at Worcester's airport for six hours. Luckily, no one was injured.

In 1998, a young hacker broke into the computer system that runs Arizona's Roosevelt Dam, attaining complete command of the system controlling its massive floodgates. If the 1.5 million acre-feet of water restrained by the dam had been released, experts indicate that the consequences could have been disastrous for Mesa and Tempe Arizona, two communities with a population totaling nearly one million people that rest on the flood plain below the dam. Again, in 2000, in Australia, a computer hacker obtained complete control over the waste- and fresh-water system that served a large community, leaking hundreds of thousands of gallons of sludge that killed marine life, destroyed a riparian area, and subjected residents to an insufferable stench. The chief executive of the water station indicated that the consequences could have been much worse, stating, "He could have done anything he liked to the fresh water." Only two months ago, in January 2003, a computer virus disrupted operations for the Seattle-area 911 operations center that serves two suburban police departments and at least 14 fire departments.

Other dire scenarios are not hard to imagine:¹⁰ attacks on, for instance, the computer systems that regulate and operate nuclear power plants, that control the orbit of telecommunications satellites, or that route calls to 911 operators could have truly disastrous

⁹Since many critical infrastructures in the United States are owned and operated by private companies, it is essential that the definition of critical infrastructures include such private concerns and not merely public or governmental entities.

¹⁰Computer attacks striking at the heart of the United States' critical infrastructures have fortunately been few in number. However, we agree with the statement of Senator Hatch that "[t]errorists and others who wish to harm our country recognize that cyber attacks on our vital computer and related technological systems can have a devastating impact on our country, our economy and the lives of our people." 148 Cong. Rec. S8901 (daily ed. Sept. 19, 2002) (statement of Sen. Hatch). In light of this threat, we believe it is essential for the guidelines to provide severe punishment for such cyber attacks to effectively deter and appropriately punish them.

consequences. For instance, a computer intrusion that compromised the integrity of databases reflecting troop and equipment locations could gravely harm national security. Computer intrusions that impede, or risk impeding, such critical infrastructures should be sentenced severely to deter effectively and punish appropriately conduct that risks such formidable consequences.

We do not believe these harms can be adequately quantified in monetary terms and therefore are not adequately accounted for by the section 2B1.1 loss table. Congress's concern with such attacks is evidence. The USA-PATRIOT Act added to the list of specific computer conduct prohibited by 18 U.S.C. § 1030 a computer intrusion or the transmission of a code or program that causes damage to "a computer system used by the government in furtherance of the administration of justice, national defense, or national security." 18 U.S.C. §§ 1030(a)(5)(A) & (a)(5)(B)(v). Such computer systems are integral to the proper functioning of government, and conduct that exposes them to damage should be strongly deterred and severely punished. We therefore propose a specific offense characteristics with a two-tiered offense level increase and a minimum offense level floor for the second tier. This structure provides for increased punishment for computer intrusions that risk harm to the computers that maintain and operate critical infrastructures, reflecting the notion that hacking into such computers is serious, risky conduct even if no harm results. The second tier punishes extremely severely computer intrusions that substantially disrupts critical infrastructures themselves.

The proposed amendment would apply cumulatively where appropriate with the specific offense characteristic for creating a risk of death or serious bodily injury and the specific offense characteristic for causing injury or death. The Commission may also want to consider including as a ground for upward departure violations disrupting so severely a critical infrastructure as to incapacitate the economy, public health, or national defense or security.

We propose adding the following specific offense characteristic:

() (A) If the offense violated 18 U.S.C. § 1030 and involved a computer system used to maintain or operate a critical infrastructure or a computer system used by or for a government entity in furtherance of the administration justice, national defense, or national security, increase by 4 levels.

(B) If the offense violated 18 U.S.C. § 1030(a)(5)(A)(i) caused a substantial disruption of a critical infrastructure, increase by 6 levels. If the resulting offense level is less than level 28, increase to level 28.

We also suggest adding the following Application Notes to the Commentary:

1. Definitions.—For the purposes of this guideline:

* * *

“Critical infrastructure” means systems and assets vital to the national defense, national security, economic security, public health or safety, or any combination of those matters.

... Critical Infrastructures under Subsection (b)(16). – *Examples of critical infrastructures to which subsection (b)(16) applies are systems and facilities, whether publicly or privately held, that provide essential services in support of the economy and national defense and national security. Such infrastructures include, but are not limited to, water supply systems, telecommunications networks, electrical power delivery systems, financing and banking systems, emergency services, medical care, and transportation links such as interstate highways, airlines, and rail systems. Substantial disruptions in the services provided by such infrastructures jeopardizes the health, safety, security, or economic welfare of a substantial number of people. The enhancement provided for in subsection (b)(16) reflects the seriousness of substantially disrupting a critical infrastructure such as by impairing 9-1-1 phone service to a town or city for several hours or by eliminating electrical power to a county for a similar period of time. Subsection (b)(16) should be applied cumulatively with subsections (b)(11) and (b)(17).*

H. Threat to Public Health & Safety; Risk of Bodily Injury, and Death

Both 18 U.S.C. § 1030 and the guidelines should take into account the potential that a computer intrusion may cause serious bodily injury or death.¹¹ Congress has recognized this potential by significantly increasing the maximum penalties for conduct that involves the risk of such consequences. The USA-PATRIOT Act doubled the maximum sentences for intentionally damaging a computer and, as a result, causing physical injury to any person or a threat to public health or safety. See 18 U.S.C. § 1030(c)(3)-(4). Congress further strengthened these penalties in the Homeland Security Act of 2002, increasing the statutory maximum to 20 years for an offender who knowingly or recklessly causes serious bodily injury and to life in prison for an offender who knowingly or recklessly causes death. Thus, Congress has unequivocally expressed its intent to punish and deter computer intrusions that cause death or serious bodily injury.

Section 2B1.1(b)(11) currently addresses conduct that *creates a risk* of death or serious bodily injury. It provides: “If the offense involved (A) the conscious or reckless risk of death or serious bodily injury . . . increase by 2 levels. If the resulting offense level is less than level 14, increase to level 14.” For a first time offender, an offense level of 14 results in a sentencing range of 15 to 21 months; even an offender with the highest possible criminal history points faces only a 46-month sentence, absent discretionary departure from the guidelines by the sentencing

¹¹See 148 Cong. Rec. S8901 (daily ed. Sept. 19, 2002) (statement of Sen. Hatch) (“[I]t is not difficult to imagine an assault on a computer system which might cause death or serious bodily injury.”).

court. Section 2B1.1 does not, however, provide guidance to a court confronted by a computer intrusion or the transmission of a computer virus that *actually causes* serious bodily injury or death. For example, a computer intrusion that disabled even for a moment the 911 emergency response system could easily deprive a medical patient of emergency treatment or a crime victim of timely protection.

We believe §2B1.1 should be amended to reflect both the wider scope of section 1030 violations that Congress intended to punish more severely, and the stronger penalties Congress intended for offenders whose conduct has such dire consequences. We recommend including a specific offense characteristic in section 2B1.1 that reflects the physical harm caused by the offense.

We suggest adding the following specific offense characteristic:

() If the offense resulted in: (A) bodily injury, add 2 levels; (B) serious bodily injury, add 4 levels; (C) permanent or life-threatening bodily injury, add 6 levels; and (D) death, add 8 levels.¹²

And adding the following cross reference:

() If the offense involved a violation of 18 U.S.C. § 1030 and any person was killed under circumstances that would constitute homicide, apply the appropriate homicide guideline from Chapter Two, Part A, Subpart 1, if the application of that section results in a higher offense level than application of this section.

1. Number of Victims

The current guidelines treat the same a computer attack that damages one computer and a computer attack that damages 100 computers, so long as there is only one victim of the statutory violation. It is undeniable, however, that even if a computer intrusion victimizes only one government agency (e.g., the armed forces), the intrusion is more egregious if it damages 100 of that agencies computers than if it damages only one of them. We believe the definition of "victim" should be amended to reflect that each computer damaged by a computer intrusion constitutes a victim for the purposes of subsection (b)(2).

¹²The offense level increases in this recommended amendment are drawn from §2L1.1 (Smuggling, Transporting, or Harboring an Unlawful Alien) and other similar provisions.

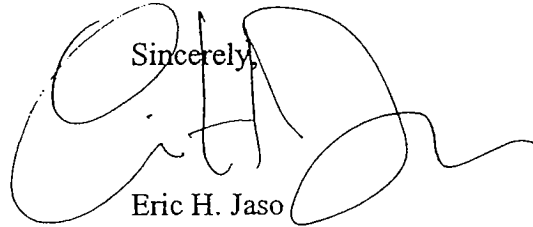
We suggest amending Application Note 3.(A)(ii) as follows:

- (ii) *"Victim" means (I) any person or computer that who sustained any part of the actual loss determined under subsection (b)(1); or (II) any individual who sustained bodily injury as a result of the offense; or (III) any individual whose personal information was accessed during a violation of 18 U.S.C. §§ 1030 or 2701. "Person" includes individuals, corporations, companies, associations, firms, partnerships, societies, and joint stock companies.*¹³

* * * * *

We appreciate the opportunity to provide the Commission with our views, comments, and suggestions. We look forward to working further with you and the other Commissioners to refine the sentencing guidelines and to develop effective, efficient, and fair sentencing policy.

Sincerely,

A handwritten signature in black ink, appearing to read 'Eric H. Jaso', written over the word 'Sincerely,'.

Eric H. Jaso
Counselor to the
Assistant Attorney General

¹³This amended application note incorporates the amendment recommended in Part IV.E., *supra*.