alternative minimum levels between 25 to 30, but would suggest that they should be commensurate to other guidelines where underlying criminal conduct results in death.[20]

We also support the amendment to treat multiple deaths occurring in a single incident as if the case involved multiple counts. It would bring §2L1.1 in conformity with other similar guideline provisions such as §§2D2.3(b)(1), 2G2.1(c)(1), 2M6.1(d)(1), 2N1.1(d)(1) and 2Q1.4(d)(1). In recent years, we have seen a number of alien smuggling cases involving multiple deaths. This provision would, we believe, result in an appropriate increase in the sentence imposed.

C. Number of Illegal Aliens

We support the Commission's proposal to expand the specific offense characteristic that increases the offense levels depending upon the number of unlawful aliens smuggled, transported, or harbored, adding groupings of "200 to 299", and of "300 or more" with a corresponding increase in levels of either 11 or 12, for the first set and either 13,15 or 18 for the second.

We believe increases in offense levels of 12 and 15 for the two new groups would be an appropriate extension of the enhancements already assigned to the lower levels. This would result in increases of three, six, nine, 12, and 15 levels for the entire specific offense characteristic. It would provide a six level enhancement for the first 99 aliens smuggled and then three level increases for each additional 100 illegal aliens. Sentencing courts would still be able to depart upward in those cases involving substantially more than 300 aliens, pursuant to Application Note 4.

II. Document Fraud

People entering into this country using false documents are a serious national security threat. The recent hearings of the National Commission on Terrorists Attacks Upon the United States ("the 9-11 Commission") revealed that many of the terrorists involved in the airline highjackings of September 11th entered the country using fraudulent passports and/or made false statements to gain entry.[21] Although we recognize that most who enter the country illegally are not terrorists, ensuring the security of our borders is critical to protecting the safety of all Americans, and maintaining the integrity of U.S. passports and other immigration documents is absolutely necessary to securing the borders. We strongly support the proposed amendments

---

[20]See for example, §2D2.3(a)(1) (base offense level 26, if death resulted from operating or directing the operation of a common carrier under the influence of alcohol or drugs).

[21]*Entry of the 9/11 Highjackers in the United States*, Staff Statement No. 1, January 26, 2004, http://www.9-11commission.gov/hearings/hearing7/staff_statement_1.pdf.

here (with some suggested revisions, see infra), which would increase penalties for fraudulently acquiring or misusing a passport or other immigration documents and strike the right balance of just punishment for all offenses.

We especially support the proposed increases for fraud related to the acquisition and use of U.S. passports. The U.S. passport is the most respected travel document in the world and is the most widely accepted and versatile identity document. Whereas visas allow a person to enter the United States, holders of U.S. passports are granted all of the privileges of U.S. citizens both in the United States and throughout the world. A U.S. passport is the "gold standard" of all passports and identity documents and is used not only as a travel document but also to open bank and credit card accounts, obtain a driver's license, obtain government benefits, cash checks, and obtain a host of other privileges of U.S. citizenship. The proposed amendment properly recognizes the unique nature of U.S. passports with significant penalties when a defendant fraudulently obtains or uses such a document. As a whole, we think the proposed amendments are critical to the nation's homeland security efforts, and we thank the Commission for considering them now.

A. Base Offense Level

We support the proposed revision of the base offense level under §2L2.2. Stricter penalties for document fraud offenses are needed to help stem the growing number of instances in which such fraud is used as a means to enter the country or obtain purported United States citizenship. We also believe an increase is necessary simply to bring the guideline into parity with §2B1.1, which provides enhanced penalties for "the unauthorized transfer or use of any means of identification to produce or obtain any other means of identification." See §2B1.1(b)((9)(C)(i). In any monetary crime, e.g., a credit card fraud involving a small dollar loss, a two level increase applies if the case involved the unauthorized use of a social security number or other means of identification to obtain the credit card with a minimum offense level of 12. Although the same circumstance arises in nearly all passport or document fraud cases, where an applicant unlawfully submits a false or stolen name, birth certificate and/or social security number in support of a passport application, these crimes yield a base offense level of eight under

§2L2.2.[22] We strongly urge the Commission to provide a base offense level of 12 for these offenses.

B. Specific Offense Characteristics

The proposed amendment also includes two new specific offense characteristics: when the defendant is a fugitive and when the case involves a U.S. Passport. We support these proposed enhancements. As for fugitive status, we recommend that the enhancement be accompanied by an explanatory note about the type of evidence necessary to prove the fugitive status. Obtaining complete foreign court records to prove that a defendant is a fugitive in a foreign country can be very difficult. It might involve the Mutual Legal Assistance Treaty process, which usually takes many months, and may depend upon the cooperativeness of the foreign responding authority. We believe an explanatory note in the guideline stating that prima facie proof is sufficient if a foreign government has notified the United States of the defendant's foreign fugitive status or if the defendant's foreign fugitive status has been entered in an international organization's data base (such as Interpol) would be helpful. In addition, we believe the enhancement should not apply to defendants who are being prosecuted for offenses that would not be recognized as criminal in the United States, either because of First Amendment or other civil rights concerns, to avoid the appearance of the United States' complicity in another country's political persecution.

The second enhancement would apply in any case where "the defendant fraudulently obtained or used a United States passport". We think the proposed enhancement properly distinguishes cases involving U.S. passports from cases involving visa fraud or foreign passports and visas. As we mention above, the U.S. passport is the most respected travel document in the world, and its integrity must be maintained. Whereas visas only allow a person to enter the United States, holders of U.S. passports are granted the privileges of U.S. citizens both in the United States and around the world. The enhancement also recognizes that non-citizens who

---

[22]The guideline in its current form also frustrates efforts to seek detention at bail hearings in passport fraud cases. Despite the fact that these cases often present compelling flight risk indicators, many U.S. Magistrate Judges will not order detention if the defendant is charged with passport fraud, because the sentence that follows a finding of guilt almost never involves a period of incarceration. The worst scenario occurs when a passport fraud defendant would remain in administrative custody pending deportation by ICE in the absence of criminal proceedings, but is ordered released by a Magistrate Judge upon transfer to the court's jurisdiction. In this situation prosecution actually works to the defendant's benefit. The low sentence range results in pretrial release, and provides the defendant an opportunity to flee and thereby avoid both prosecution and deportation.

obtain passports by fraud engage in a host of collateral criminal activity each time the passport is used for any domestic or travel purposes.

We support the enhancement's limited scope – it would apply only if a United States passport was "fraudulently obtained or used." The majority of passport fraud cases arise when the crimes are detected by the State Department at the application stage, before the passport is actually issued, and thus would not be subject to the enhancement. For those defendants whose crime results in actually obtaining the fraudulent passport, a much more severe penalty is warranted. First of all, a criminal's success in moving an application past the approval stage is usually attributable to the sophistication of the fraudulent application. The defendant may have obtained a high quality counterfeit birth certificate or stolen the true birth certificate and social security number of a real victim/citizen. Furthermore, many who have obtained fraudulent passports have enjoyed the benefits of citizenship and passport ownership for many years. Some of these offenders are now being detected for the first time as they send in the unlawfully obtained passports for renewal. This is a class of offenders to which the enhanced penalties are surely appropriate.[23]

Overall, we believe in order to maintain the integrity of U.S. passports, the repercussions of someone fraudulently obtaining a U.S. passport must be significantly increased from current policy. We support the adoption of the proposed specific offense characteristic but recommend a slightly revised tiered enhancement: four levels if the defendant fraudulently obtained or used a United States passport, and eight levels if the defendant fraudulently obtained or used a United States passport, intending to enter the United States to engage in terrorist activity.

Unlike the proposed amendment for alien smuggling, where a defendant who smuggles an alien into the United States to engage in terrorist activity would receive a notably greater increase in sentence than one who smuggles an alien into the United States to engage in other crime, the proposed amendment as published by the Commission, makes no distinction between terrorism related activities and others. As such, a terrorist who fraudulently applied for and obtained a United States passport would receive exactly the same level increase as any nonviolent offender who also fraudulently applied for and obtained a United States passport. We think some distinction should be made in the guideline.[24] This bifurcated approach is also

---

[23]We believe this specific offense characteristic should be accompanied by an application note which makes clear that the "use" of a passport includes the attempted renewal of the previously-issued passport. This would allow the application of §2L2.2(b)(4) to all cases involving fraudulent applications for renewal of U.S. passports (Form DSP-82).

[24]We also recommend the inclusion of the following proposed Application Note for this version of proposed §2L2.2(b)(4):

Application of Subsection (b)(4). The first sentence of Subsection (b)(4)

consistent with the approach followed in the general identity theft statute, 18 U.S.C. § 1028(a)(7). Under § 1028(a)(7), the maximum term of imprisonment for identity theft is (1) 15 years imprisonment, if as a result of the offense anyone committing the offense obtained anything of value aggregating $1,000 or more during a one year period; (2) 20 years imprisonment, if the offense is committed to facilitate a drug trafficking offense or in connection with a crime of violence; or (3) 25 years imprisonment, if the offense is committed to facilitate an act of international terrorism. See 18 U.S.C. § 1028(b)(1)(D), (b)(3)-(4).

IMPLEMENTATION OF THE CAN-SPAM ACT OF 2003

The Commission has published a number of issues for comment in response to section four of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act of 2003"), Pub. L. 108–187, which directs the Commission to review and, as appropriate, amend the sentencing guidelines and policy statements to establish appropriate penalties for the criminal offenses created the act – i.e. 18 U.S.C. § 1037 – and other offenses that may be facilitated by the sending of a large volume of unsolicited e-mail. Section four further directs the Commission to consider providing sentencing enhancements for several listed factors.

I. Statutory Reference for § 1037 Offenses

We recommend that the Commission reference in the Statutory Index all five sections of 18 U.S.C. §1037 to §2B1.1. The "hacking spam" provision in §1037(a)(1) prohibits one from

---

would establish a four-level increase in any case (other than the special circumstance set forth in the second sentence of that subsection) in which the defendant fraudulently obtained or used a United States passport. As the Department of State has noted, "The U.S. passport is the most valuable identity document in the world as it establishes American citizenship and allows its bearer unlimited access to virtually every country in the world." [Source: http://www.state.gov/m/ds/investigat/] In addition, United States passports – especially if they are legitimate passports obtained by fraud – are likely to be given greater credence, as proof of identity by financial institutions and other businesses, than many other types of identifying documents than can be more easily forged or counterfeited. The second sentence of Subsection (b)(4) would establish an eight-level increase in any case where the defendant fraudulently obtained or used a United States passport intending to enter the United States to engage in terrorist activity. The defendant need not have actually entered the United States or actually engaged in terrorist activity within the United States for this latter increase to apply.

knowingly accessing a protected computer without authorization and intentionally initiating the transmission of multiple commercial electronic mail messages from or through that computer. This provision is intended for the prosecution of those who break into computer systems of others, set up an e-mail server, and start sending out electronic mail messages. It is intended to fill a perceived gap in § 1030 when the resulting damage from the hacking offense does not meet the $5,000.00 threshold or is otherwise the type of damage established under § 1030(a)(5)(B). Given that §2B1.1 already encompasses similar conduct, we believe the same guideline section should apply to violations of §1037(a)(1).

The "open relay" provision of §1037(a)(2) prohibits one from knowingly using a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of those messages. This subsection is intended for the prosecution of people who send spam through mail servers that are configured to accept mail from any source and forward it to mail servers on other networks. Such mail servers, or "open relays," are often otherwise available to the public, but not necessarily intended for the use of spam. Consequently, the use is not necessarily "without authorization," but is nonetheless an abuse of the servers, especially when the origin of the spam is disguised. This fills a perceived gap in § 1030(a)(5) when a computer is intentionally accessed, but not necessarily without authorization, and where the type of damage under § 1030(a)(5)(B) cannot be proven. Again, §2B1.1 already encompasses similar conduct, and as such is the logical reference to violations of §1037(a)(2).

The "false header" provision in § 1037(a)(3) prohibits one from knowingly and materially falsifying header information in multiple commercial electronic mail messages and intentionally initiating the transmission of those messages. This subsection is intended for the prosecution of persons who create false e-mail headers to frustrate efforts by recipients, Internet Service Providers ("ISP"), or investigating agencies in determining the true sender of the electronic mail. Since this is a type of fraud, to the extent it is criminalized, we believe it can also be adequately addressed by §2B1.1.

The "false registration" provision in §1037(a)(4) prohibits one from registering for five or more e-mail addresses or online user accounts, or two or more domain names, knowingly using information that materially falsifies the identity of the registrant, and then initiating the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names. This is a companion provision to § 1037(a)(3), and prohibits persons from sending out commercial electronic mail that reflects a true electronic mail address, but which address points to an account that has been registered with bogus information. Again, as a type of fraud, it can be adequately addressed by § 2B1.1.

Finally, the "false IP address" provision of the statute, covered by § 1037(a)(5) prohibits one from falsely representing oneself to be the registrant or legitimate successor in interest to the

registrant of five or more Internet Protocol addresses, and intentionally initiating the transmission of multiple commercial electronic mail messages from those addresses. This subsection is intended for the prosecution of those involved in the developing problem of "zombie spam," where spammers attempt to get around IP-level blocking software by falsely assuming the identity of a legitimate domain name and convincing the appropriate IP-block administrator to re-establish routing to the spammer's ISP, effectively hijacking legitimate IP blocks for spam-sending purposes. Once again, it is a type of fraud which can be addressed by §2B1.1.

II. Base Offense Level and Enhancements

We believe that the present base offense level under §2B1.1 is appropriate for all provisions of §1037. At the current base offense level of six, a misdemeanor violator would receive a penalty of 0-6 months in Criminal History Category I through to a penalty of 12 months in Criminal History Category VI (since the applicable 12-18 month range would be capped by the statutory maximum). Additional levels could be added for the more serious conduct described in § 1037(b)(2).

In keeping with the statutory directive, however, we believe additional enhancements should be triggered by the amount of loss to victims, the amount of gain to the defendant,[25] quantity of electronic mail sent, number of false domain and address registrations, unauthorized access to a computer system in the course of the offense, and role as an organizer or leader.[26] We believe that an enhancement of at least four levels is necessary to appropriately capture the increased statutory penalty enacted by Congress where these aggravating factors are present.

We recommend against applying the multiple victim enhancement and mass-marketing enhancement to simple misdemeanor violations of the statute. Since the offense described in 18 U.S.C. § 1037 inherently involves mass-marketing, adding an enhancement on top of the base offense level would effectively establish a higher base offense level because the enhancement would apply to every case. Because we believe that the present base offense level of six is an appropriate starting point for the guideline calculation, we would not seek an automatic enhancement to level eight.

However, we believe the "multiple victim" enhancement should apply if, for example, a defendant accessed more than ten protected computers to send out commercial electronic mail

---

[25]Specifically, we believe that the sentencing guidelines should, at least in the spam context, treat gain more affirmatively than they do at present – in which gain can only be considered as a measure when loss to the victim cannot be reasonably calculated. See §2B1.1 Commentary (n. 3(B)).

[26]We believe that the leadership role can be appropriately applied through the existing §3B1.1 enhancements.

messages in violation of § 1037(a)(1). Furthermore, in cases where the conduct is widespread or significant, such as cases where the amount of electronic mail initiated significantly exceeds the minimum thresholds of § 1037(b)(2)(C), a mass-marketing enhancement would be appropriate. Major financial institutions and other online businesses, for example, are being increasingly targeted for "phishing" – i.e., the use of unsolicited e-mail, designed to appear that it is being sent by those institutions or businesses, that seeks to deceive multiple Internet users into disclosing their personal financial or identifying data, which the phishing scheme can then use to gain access to Internet or financial accounts and commit identity theft and fraud. During 2003 and early 2004, several dozen phishing schemes have used the names and corporate logos of leading U.S. financial institutions and financial services-related businesses such as Bank One, Bank of America, Citibank, eBay, PayPal, and U.S. Bank.

Therefore, we recommend revising Application Note 4 in §2B1.1 relating to the mass-marketing enhancement to address the use of spam in furtherance of schemes to conduct online identity theft and fraud to read as follows (changes in bold):

> For purposes of subsection (b)(2), "mass-marketing" means a plan, program, promotion or campaign that is conducted through solicitation by telephone, mail, the Internet, or other means to induce a large number of persons to (i) purchase goods or services; (ii) participate in a contest or sweepstakes; **(iii)** invest for financial profit**; or (iv) disclose personal financial or identifying data.** "Mass-marketing" includes, for example, a telemarketing campaign that solicits a large number of individuals to purchase life insurance policies**, or a campaign of unsolicited e-mail that solicits a large number of people to assist in transfers of funds or to disclose personal financial or identifying data.**

Inclusion of the proposed language would also serve as a suitable alternative to creating a new and separate enhancement for the sending of a large volume of unsolicited e-mail in cases that would be governed by §2B1.1 (e.g., fraud and identity theft cases).

Although to some extent, a level of sophistication is inherent in all spam, we believe there are circumstances under which an offense under § 1037 could be considered to involve sophisticated means which should trigger the application of an additional enhancement. For example, if an offender created or distributed a virus or trojan horse program to assist in accessing the computers of a number of innocent users to facilitate the sending of unsolicited commercial email, or if an offender routed his communications overseas to frustrate investigation or prosecution of a spam offense, the sophisticated means enhancement should apply. Accordingly, we do not believe that commentary discouraging application of the enhancement should be included.

We also recommend an enhancement for defendants who obtain e-mail addresses through improper means such as harvesting of e-mail addresses or who knowingly send or advertise an internet domain registered with false information, in keeping with the directive in section 4(b)(2)(A) of the Act. Such e-mails are more pernicious because the threat of being spammed creates a disincentive for legitimate users to use the Internet – these users will be less likely to purchase merchandise online or engage in other beneficial activities if they believe that their e-mail address might be misused or misappropriated by an Internet vendor. In addition, when the receipt of spam e-mail that relates to a false domain name, it is harder to report those violations to the Federal Trade Commission or the Department of Justice. Therefore, such an enhancement should be at least two and possibly four levels, to adequately reflect the additional culpability reflected by this behavior.

Finally, we recommend an additional enhancement for sending large quantities of electronic mail in the course of commission of crimes involving fraud, obscenity, child pornography, and sexual exploitation of children, among others. We believe, however, that rather than amending a number of individual guidelines sections to add this enhancement, a more generally applicable role/means enhancement in Chapter Three of the guidelines should be considered. If, however, the Commission believes that amending a number of individual guidelines provisions is more appropriate, then the fraud, obscenity, child pornography and sexual exploitation of children guidelines should be covered comprehensively, in order to best effectuate the express intent of Congress.

III. Other Issues

In response to one of a the Commission's question, we believe the term "large quantities of electronic mail" as used in the CAN-SPAM Act should at least include such quantities that would trigger the felony provisions of § 1037(b)(3) – i.e., 2,500 messages within a 24-hour period, 25,000 within 30 days, or 250,000 within one year. The Commission could also appropriately choose to set the guidelines lower than that, to the point that would trigger misdemeanor violations of § 1037. This would be particularly appropriate in cases involving child pornography and sexual exploitation of children, in which a few hundred messages might permit a defendant to find potential child victims.

In regards to violations of 15 U.S.C. § 7704, we recommend they be referenced to §2G3.1. Where the offense does not involve the transmission of child pornography, § 7704 violations are roughly analogous to offenses under 18 U.S.C. § 2252B and should be sentenced accordingly. In cases where the offense involves the transmission of child pornography, offenders would almost certainly be charged under one of the statutes sentenced at §2G2.2 and the existing cross-reference in §2G3.1 would nonetheless direct the court to §2G2.2. For offenses not involving the transmission of child pornography, the enhancements at §2G3.1 are generally sufficient, with one exception. Currently, proposed §2G3.1(b)(2) is written to cover "use of a misleading domain name on the Internet with the intent to deceive a [minor][person]

into viewing material that is harmful to minors." This enhancement should be expanded to cover "a violation of 15 U.S.C. Section 7704(d)."

* * * * *

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,

Deborah J. Rhodes
Counselor to the Assistant Attorney General

PRACTITIONERS' ADVISORY GROUP
CO-CHAIRS BARRY BOSS & JIM FELMAN
C/O ASBILL MOFFITT & BOSS, CHARTERED
1615 NEW HAMPSHIRE AVENUE, N.W.
WASHINGTON, DC 20009
(202) 234-9000 - BARRY BOSS
(813) 229-1118 - JIM FELMAN

February 27, 2004

VIA HAND DELIVERY

United States Sentencing Commission
One Columbus Circle, N.E.
Suite 2-500, South Lobby
Washington, D.C. 20002-8002

Re: 2004 Proposed Amendments and Issues for Comment

Dear Commissioners:

We write on behalf of the Practitioners Advisory Group to address the notice of proposed amendments and issues for comment published in the Federal Register notices of January 14, 2004. As always, we view our primary role as assisting the Commission by drawing on our expertise as defense attorneys to respond to the issues for comment and specific amendments proposed by the Commission.

I. Proposed Amendments to Chapter 8 (Amendment #2)[1]

Initially, the PAG applauds the Commission for the formation of this Ad Hoc Advisory Group. From our perspective, this is sentencing policy-making at its best, and it stands in unfortunate contrast to the process that has led to many of the recent amendments that have resulted from Congressional directive. We also wish to compliment the Ad Hoc Advisory Group on its excellent work product. It is refreshing to see sentencing policy formulated through a process that brings together experienced individuals from different backgrounds and ideological perspectives. Although we do not necessarily agree with all of the Group's recommendations, we hope that the Group's success can serve as a model for future policy-making in this arena. We do wish to provide input on the four issues for comment:

[1] The PAG expresses its appreciation to Eugene Illovsky and Greg Smith for their assistance in preparing this portion of our submission.

A. Eliminate the Automatic Preclusion for Unreasonable Delay.

Under U.S.S.G. § 8C2.5(f), an organization cannot receive the three point culpability score reduction if it "unreasonably delayed reporting the offense to appropriate governmental authorities." The proposed amendment retains that prohibition in subsection (f)(2), even though the clear thrust of amended § 8C2.5(f) is the adequacy of the organization's compliance program.

The prohibition should be removed. An organization's delay in reporting is sufficiently considered in the guideline's subsection explicitly addressed to such self-reporting. U.S.S.G. § 8C2.5(g). Under that section, an organization cannot get the five point culpability score reduction for self-reporting and acceptance of responsibility if it does not "report[] the offense to appropriate government authorities" within a "reasonably prompt time."

An organization with an excellent compliance program may, for some reason, delay its self-reporting of the violation. That decision, if later deemed unreasonable, may not necessarily reflect on inefficacy of the organization's program to "prevent and detect violations of law." It is proper to have reporting delay be the subject of subsection (g) and remove it from subsection (f).

B. High-Level Personnel Involvement Should Create a Rebuttable Presumption.

If certain high-level personnel participated in, condoned, or were willfully blind to the offense, § 8C2.5(f) automatically precludes the three-point culpability score reduction for an effective compliance program. The proposed amendment changes the automatic preclusion to a rebuttable presumption that the organization's compliance program was not effective.

The PAG believes the proposed amendment, reflected in subsection(f)(3), correctly treats the issue of high-level employee involvement. The PAG believes the Commission should not try to distinguish further between 'large' and 'small' organizations for the purpose of leaving some version of the automatic preclusion in place. An "automatic" rule will invariably lead to unjust results in some cases.

An automatic preclusion also unnecessarily restricts judicial discretion. Removing it gives judges the discretion to consider each organization's circumstances, and the particulars of the higher-level employee involvement, on a case-by-case basis. The organization should have the opportunity to present its case to the judge as to how it can rebut the presumption in those particular circumstances. Judges will no doubt exercise that discretion in light of precisely those factors recognized to be important, such as the organization's size and the number and type of high-level employees involved in the offense.

C. Increase The Culpability Score Point Reduction.

The PAG supports increasing the culpability score reduction from three to four points. Awarding more points for an effective compliance program would not only appropriately reflect the heightened requirements of U.S.S.G. § 8B2.1, but would also create an incentive for organizations to examine the adequacy of their current programs.

D. Factors Relating to Small and Mid Size Organizations.

Chapter Eight's impact on small and mid-size companies requires further study. Historically, the great majority of sentenced companies are small, closely-held entities. And, as the Advisory Group's Report notes, since 1991 an overwhelming number of convicted organizations failed to receive effective compliance program sentencing credit for reasons related to their smaller size. The PAG seconds the Advisory Group's recommendation that the Commission devote resources to reaching and training small and mid-size companies about corporate compliance.

The PAG believes that many factors or considerations could be incorporated into Chapter Eight to encourage small and mid size organizations to develop and maintain compliance programs. There is likely, however, to be some spirited disagreement among business interests, the defense bar, and the Department of Justice as to which factors or considerations will likely be most effective or important. And, to say the issue is a difficult one may understate things. The Advisory Group Report noted the difficulties it had in getting feedback on the matter.

The PAG therefore proposes that the Commission convene a working group dedicated solely to the study of the specific issue of the guidelines' application to small and mid size companies. This working group will no doubt have the first, difficult task of even defining the best methodology for studying this issue. The PAG envisions that the working group would reflect the usual affected constituencies (e.g., business, defense bar, prosecutors), but also that it might fruitfully be broadened to include an economist and/or other academics who have studied these issues from a broader perspective. The interdisciplinary approach may be the most effective way to give the Commission the help it needs to tackle this complex yet exceedingly important guidelines matter.

II. Proposed Amendments relating to Public Corruption (Amendment #4)

The PAG is unaware of any data or even anecdotal examples suggesting a need for increased penalties under these guidelines. No such basis or justification is included in the materials accompanying the proposed amendments. Although the Synopsis of the proposed amendment states that it "aims at moving away from a guideline structure that relies heavily on monetary harm to determine the severity of the offense," it does not appear that the proposed amendment in fact does so (assuming there are policy reasons for such a change, which are not explained in the published materials). The new guidelines incorporate the §2B1.1 loss table in precisely the same fashion as the existing guidelines. Accordingly, the PAG does not believe any

increase to the base offense levels for bribery and gratuity cases has been demonstrated to be warranted. Indeed, these base offense levels could instead be *reduced* to achieve proportionality with 2B1.1, the guideline governing other similar economic crimes.

The PAG agrees that Guidelines 2C1.1 and 2C1.7 may readily be consolidated, but the 2-level enhancement for multiple incidents should be limited to those cases currently sentenced under 2C1.1 to avoid even further unwarranted disparity between cases involving intangible rather than tangible harm. Similarly, if guidelines 2C1.2 and 2C1.6 are consolidated, the 2-level enhancement for multiple incidents should be limited to cases currently sentenced under 2C1.2 to avoid unwarranted disparity between cases involving mere gratuities rather than actual theft.

Briberies and gratuities are purely economic crimes. While the acceptance of a bribe or gratuity by a public or bank official is a serious offense because it serves to undermine the public's confidence in government and banks, there is little reason to believe it does so to any greater degree than outright theft or embezzlement by such officials, particularly where the official's position does not involve high-level decision-making or other sensitive matters, and is not an elected office. Because the base offense level for economic crimes is either 6 or 7, depending on the statutory maximum sentence, the current base offense level of 10 for bribery offenses results in unwarranted disparity. Increasing the base offense level from 10 to 12 would exacerbate this unwarranted disparity rather than cure it, and result in sentences that are unjust.

Consider, for example, a typical bribery case in which a low-level public official accepts two $5,000 bribes to award a $100,000 contract on which the contractor makes a $20,000 profit.[2] Under the current version of 2C1.1, the base offense level would be 10, increased by 2 levels for multiple incidents, plus 4 levels under the 2B1.1 table reflecting the $20,000 "benefit received," resulting in an adjusted offense level of 16. If the base offense level is increased by two levels as proposed in the amendment, the adjusted offense level would be 18.

Contrast this $10,000 bribery scenario with a case in which a public official simply steals $10,000 outright from the public fisc. Assuming some use of the mails or wires, the base offense level would be 7, plus 4 levels for the loss, plus 2 levels for abuse of trust, resulting in an adjusted offense level of 13. Why should a low-level public official be sentenced 3 levels higher for accepting a $10,000 bribe from a third party than stealing the $10,000 directly from the public fisc? And if the proposed amendment were adopted, the disparity would be *5* levels. This means that the minor official who accepts the $10,000 bribe would be sentenced 1 level *higher* (18) than an official who outright steals up to $120,000 – *more than the entire value of the contract* (7+8+2=17).

The unwarranted disparity noted above would be further exacerbated by the consolidation of 2C1.7 with 2C1.1 if the 2-level increase for multiple incidents is applied across the board.

---

[2] Obviously the numbers used in hypotheticals such as this are important. We believe the numbers above are quite reasonable, and further believe our overall point would be amplified by having the Commission Staff apply and contrast the fraud and bribery guidelines to randomly selected actual bribery cases.