Report to the Congress:

INCREASED PENALTIES FOR CYBER SECURITY OFFENSES

(As required by section 225(c) of the Homeland Security Act of 2002, Public Law 107-296)

UNITED STATES SENTENCING COMMISSION

May 2003

DIANA E. MURPHY
Chair

RUBEN CASTILLO
Vice Chair

WILLIAM K. SESSIONS, III
Vice Chair

JOHN R. STEER
Vice Chair

MICHAEL E. O'NEILL
Commissioner

ERIC H. JASO
(Ex Officio)

EDWARD F. REILLY, JR.
(Ex Officio)

I. Overview

This report is submitted pursuant to section 225(c) of the Homeland Security Act of 2002, Pub. L. 107–296. That section requires the United States Sentencing Commission ("the Commission") to submit a report not later than May 1, 2003 explaining actions taken in response to the Cyber Security Enhancement Act of 2002, Sec. 225 of Pub. L. 107–296, and offering any policy recommendations regarding statutory penalties.

In developing its response to the Act, the Commission analyzed sentencing data, reviewed relevant case law and legislative history, and solicited and considered commentary from the Department of Justice, defense attorneys, probation officers, academics and other experts in the field of computer crime. The Commission specifically considered the eight factors enumerated in the directive, detailed below, and considered the extent to which each was or was not accounted for by existing sentencing guidelines and policy statements. As a result of its study and analysis, the Commission promulgated a carefully tailored amendment designed to more fully account for specific factors relevant to computer offenses. This amendment, a copy of which is attached, was unanimously approved by the Commission on April 16, 2003. It is scheduled to become effective on November 1, 2003, subject to congressional review.

A. The Directive

The Cyber Security Enhancement Act directs the Commission to review and amend, if appropriate, guidelines and policy statements applicable to individuals convicted of offenses under 18 U.S.C. § 1030. The Act requires the Commission, in carrying out the directive, to ensure that the relevant guidelines and policy statements reflect the serious nature and growing incidence of section 1030 offenses and the need for an effective deterrent and appropriate punishment. It also requires the Commission to consider the extent to which the following eight factors are or are not accounted for by the relevant guidelines:

1. the potential and actual loss resulting from the offense;

2. the level of sophistication and planning involved in the offense;

3. whether the offense was committed for purposes of commercial advantage or private financial benefit;

4. whether the defendant acted with malicious intent to cause harm in committing the offense;

5. the extent to which the offense violated the privacy rights of individuals harmed;

6. whether the offense involved a computer used by the government in furtherance of national defense, national security, or the administration of justice;

7. whether the violation was intended to or had the effect of significantly interfering with or disrupting a critical infrastructure; and

8. whether the violation was intended to or had the effect of creating a threat to public health or safety, or injury to any person.

B. 18 U.S.C. § 1030 and the Applicable Guidelines

Section 1030 of title 18, United States Code, proscribes a wide range of criminal conduct involving computers. There are nine different offenses codified in section 1030, and they have statutory maximum penalties ranging from one year to life imprisonment.

Section 1030(a) violations are referred to four sentencing guidelines: §2B1.1 (Larceny, Embezzlement, and Other Forms of Theft; Offenses Involving Stolen Property; Property Damage or Destruction; Fraud and Deceit; Forgery; Offenses Involving Altered or Counterfeit Instruments Other than Counterfeit Bearer Obligations of the United States); §2B2.3 (Trespass); §2B3.2 (Extortion by Force or Threat of Injury or Serious Damage) and §2M3.2 (Gathering National Defense Information). Convictions under sections 1030(a)(2) (unauthorized access to a computer to obtain information from a financial institution, the United States government or a protected computer); 1030(a)(4) (unauthorized access to a protected computer in furtherance of fraud); 1030(a)(5) (transmission of a program or code or unauthorized access resulting in damage); and 1030(a)(6) (trafficking in computer passwords) are all referenced to §2B1.1. Convictions under section 1030(a)(1) (accessing and disseminating national defense or restricted information with reason to believe it could be used to the injury of the United States) are referred to §2M3.2; convictions under section 1030(a)(3) (misdemeanor trespass on a government computer) are referenced to §2B2.3; and convictions of section 1030(a)(7) (extortionate demand to damage protected computer) are referenced to §2B3.2. Finally, convictions under 18 U.S.C. § 1030(b) (attempts to commit violations of section 1030(a)) are referenced to §2X1.1 (Attempt, Solicitation, or Conspiracy).

C. Data

As part of its review of the guidelines applicable to computer crime, the Commission analyzed data for 116 cases with convictions under 18 U.S.C. § 1030 sentenced in fiscal years 2001 and 2002.[1] This review yielded valuable information about the backgrounds and

[1] Of the 126 cases with convictions under 18 U.S.C. § 1030 sentenced in fiscal years 2001 and 2002, 10 were excluded from the analysis due to incomplete or missing documentation.

motivations of computer crime offenders, the types of offenses committed and how such offenses are sentenced under the guidelines.

The data revealed that most violators of 18 U.S.C. § 1030 were well educated (66% had completed at least some college education) and had minimal or no criminal history (78% were sentenced using Criminal History Category I). Approximately half (48%) of offenders committed their crime for financial reasons. Most offenses (65%) involved a computer at the offender's current or former workplace.

The data showed that the overwhelming majority of cases with convictions under 18 U.S.C. § 1030 are sentenced under §2B1.1. For fiscal years 2001 and 2002, 116 cases were reviewed in which one of the counts of conviction was an offense under 18 U.S.C. § 1030. Of these, 89.6 percent (104) were sentenced using either §2B1.1 or another guideline that has since been consolidated with §2B1.1. Three cases were sentenced under §2B2.3, and no cases were sentenced under §2B3.2, §2M3.2, or §2X1.1.[2] The data showed that 20 percent of computer crime offenders in fiscal years 2001 and 2002 received the two level adjustment at §3B1.3 for abuse of trust or use of a special skill, which is higher than the annual rate of approximately 10 percent for all offenders sentenced under §2B1.1 (or a guideline consolidated with §2B1.1).

The Commission's findings with respect to recent computer crime cases build upon and mirror earlier findings of the Commission in this area. In 1996, the Commission conducted a review of cases under 18 U.S.C. §§ 1030(a)(4) and (a)(5) in response to the Antiterrorism and Effective Death Penalty Act of 1996, Pub. L 104–132. The report submitted to Congress documented findings similar to those described above, including that computer offenders tended to be well educated, tended to have little or no criminal history, frequently committed crimes through the use of a computer at the workplace, and often were motivated by financial reasons. Such offenders also received the enhancement for abuse of trust with greater than average frequency. *See Report to Congress: Adequacy of Federal Sentencing Guideline Penalties for Computer Fraud and Vandalism Offenses*, United States Sentencing Commission, June 1996.

II. The Amendment

The sentencing guideline amendment developed by the Commission makes modifications to three guidelines: §§2B1.1, 2B2.3 and 2B3.2, as well as to Appendix A (Statutory Index). This section summarizes and explains these changes.

---

[2] The remaining nine cases (7.8%) were sentenced under a variety of other guidelines due to other more serious counts of conviction.

A. Modifications to §2B1.1 (Theft, Property Destruction, and Fraud)

1. New Enhancement Targeting Offenses Involving Malicious Intent, Intent to Obtain Personal Information, Computer Systems Used in Furtherance of the Administration of Justice, National Defense, and National Security, and Interference with a Critical Infrastructure

The amendment specifically addresses four of the factors listed in the directive – malicious intent, invasions of privacy, computer systems used in furtherance of the administration of justice, national defense, and national security, and significant interference with a critical infrastructure – in one new specific offense characteristic in §2B1.1. The new specific offense characteristic provides a two level increase (corresponding to an approximate 25 percent increase in sentence) at §2B1.1(b)(13)(A)(i) for offenses under 18 U.S.C. § 1030 that involve either (a) 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 of justice, national defense, or national security; or (b) an intent to obtain personal information. It provides a four level increase (corresponding to an approximate 50 percent increase in sentence) at §2B1.1(b)(13)(A)(ii) for an offender convicted of violating 18 U.S.C. § 1030(a)(5)(A)(i), a crime that requires a heightened showing of intent to cause damage. It further provides a six level increase (roughly doubling the sentence) at §2B1.1(b)(13)(A)(iii) for those section 1030 offenses that cause a substantial disruption of a critical infrastructure. Because of the overlapping nature of these enhancements in terms of the conduct they punish, only the greatest applicable one will apply in a particular case. The graduated levels, however, ensure incremental punishment for increasingly serious conduct, and were chosen by the Commission in recognition of the fact that conduct supporting application of a more serious enhancement frequently will encompass behavior relevant to a lesser enhancement as well. With respect to the most serious enhancement, the six level increase for an offense resulting in a substantial disruption of a critical infrastructure, a minimum offense level of 24 (which corresponds to a range of 51 to 63 months in Criminal History Category I) is provided. This minimum offense level will ensure that offenders involved in the most serious offenses will face a substantial minimum guideline sentence.

Analysis of the Commission's data suggests that approximately 51 percent of section 1030 offenses sentenced under §2B1.1 likely will receive an adjustment under this new specific offense characteristic. Of the 104 cases reviewed that were sentenced under §2B1.1 (or a guideline consolidated with §2B1.1), 36.5 percent (38) would have qualified for the two level adjustment (the overwhelming majority of these (33) for having an intent to obtain personal information); an additional 14.4 percent (15) would have been eligible for the four level adjustment[3]; and none involved conduct meriting the six level adjustment.

---

[3] The cases that were calculated to be eligible for this adjustment were prosecuted under 18 U.S.C. § 1030(a)(5)(A), the predecessor to current section 1030(a)(5)(A)(i).

2. Expansion of Upward Departure Provision For Offenses That Result in Death

The amendment expands the upward departure provision in §2B1.1 addressing substantial non-monetary harms to account for violations of 18 U.S.C. § 1030 that result in death. Application Note 17(A)(ii) (to be redesignated Application Note 18(A)(ii)) provides a non-exhaustive list of factors that a court may consider in determining whether an upward departure would be warranted. One of the identified factors is whether the offense caused or risked substantial non-monetary harm, including physical harm. The amendment expands this provision to provide expressly that in the case of a section 1030 offense involving damage to a protected computer, an upward departure would be warranted if death resulted.

3. New Upward Departure Provision For Debilitating Impact on Critical Infrastructure

The amendment adds a new upward departure provision to §2B1.1 to address offenses in which the substantial disruption to a critical infrastructure is so severe as to have a debilitating impact on national security, national economic security, national public health or safety or any combination thereof. This provision, at Application Note 18(B) to §2B1.1, is an encouraged upward departure, stating that an upward departure "would be warranted" in such circumstances.

4. Clarification of Rule of Construction For Calculation of Loss

The amendment modifies the rule of construction relating to the calculation of loss in protected computer cases. Prior to this amendment, Application Note 2(A)(v)(III) (to be redesignated Application Note 3(A)(v)(III)) to §2B1.1 provided that in certain cases involving the unauthorized access, or access exceeding authorization, to a protected computer, certain pecuniary harms as described in the application note were to be considered "actual loss" regardless of whether such harms were reasonably foreseeable. In October 2001, as part of the USA PATRIOT Act of 2001, Pub. L. 107–56, Congress added a definition of loss to 18 U.S.C. § 1030, thus clarifying what types of expenses could be considered in calculating whether the $5,000 jurisdictional trigger applicable to certain section 1030(a)(5) cases was met. *See* 18 U.S.C. § 1030(e)(11). The guideline amendment modifies the rule of construction under §2B1.1 to more fully incorporate the statutory definition and to clarify its application to all offenses under 18 U.S.C. § 1030.

B. Modifications to §2B2.3 (Trespass) and §2B3.2 (Extortion by Force or Threat of Injury or Serious Damage) For Offenses Involving Computer Systems Used in Critical Infrastructure, Administration of Justice, National Defense and National Security

The amendment further accounts for offenses involving computer systems used to maintain or operate a critical infrastructure and used by or for a government entity in furtherance of the administration of justice, national defense, and national security by expanding the scope of

existing enhancements in §2B2.3 (Trespass), to which violations of 18 U.S.C. § 1030(a)(3) (misdemeanor trespass on a government computer) are referenced, and §2B3.2 (Extortion by Force or Threat of Injury or Serious Damage), to which violations of 18 U.S.C. § 1030(a)(7) (extortionate demand to damage protected computer) are referenced.

In the trespass guideline there is a two level enhancement at §2B2.3(b)(1) for trespasses that occur on particularly secure or sensitive areas, including a secured government facility, a nuclear energy facility, a vessel or aircraft of the United States, a secured area of an airport, and a residence. The amendment expands the scope of this enhancement so that it will also apply if the trespass occurred on a computer system used to operate or maintain a critical infrastructure or used by or for a government entity in furtherance of the administration of justice, national defense, or national security. Two of the three section 1030(a)(3) cases sentenced in fiscal years 2001 and 2002 under §2B2.3 involved national defense computers.

In the extortion guideline there is a three level enhancement at §2B3.2(b)(3) for offenses that involved preparation to carry out, or a demonstrated ability to carry out, certain serious types of threats, including threats of death, serious bodily injury, kidnapping, and product tampering. The amendment expands the scope of this enhancement so that it also will apply if an extortionate threat to damage a protected computer involved preparation to carry out, or a demonstrated ability to carry out, a threat to damage 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.

C. Reference of 18 U.S.C. § 2701 Offenses to §2B1.1 in Appendix A (Statutory Index)

Section 2701 of title 18, United States Code, prohibits unlawful access to stored communications such as e-mail. The amendment provides a reference for 18 U.S.C. § 2701 offenses in Appendix A (Statutory Index). Prior to the Homeland Security Act, an offense under section 2701 was punishable by a maximum term of imprisonment of six months, unless the offense involved one of the identified aggravated purposes, in which case the maximum term of imprisonment was one year for a first offense. Subsequent aggravated offenses were punishable by a maximum term of imprisonment of two years' imprisonment. The Homeland Security Act expanded the scope of section 2701 by adding an additional aggravated purpose to the statute and increased penalties for all violations of section 2701. A first offense under section 2701 is now punishable by a one year statutory maximum term of imprisonment, unless it was committed with one of the aggravated purposes, in which case the maximum term of imprisonment is five years. Subsequent offenses are punishable by a statutory maximum term of five years, and subsequent aggravated offenses are punishable by a statutory maximum term of 10 years' imprisonment.

Commission data indicate that 18 U.S.C. § 2701 has been used infrequently. For fiscal years 1997 through 2001, the Commission has data for only seven sentenced cases involving a

conviction under this statute.[4] All seven of these cases were related to fraud, and were sentenced using the fraud guideline. Given the newly enhanced statutory penalties, the number of prosecutions under this statute may increase, particularly in light of the widespread reliance on e-mail and other forms of wire or electronic communication. Accordingly, the Commission has provided a specific guideline reference for 18 U.S.C. § 2701 in Appendix A, rather than relying on the generally applicable rule that the most analogous guideline should be used for offenses not listed in the Statutory Index. *See* USSG §1B1.2(a). Section 2701 offenses are now referenced specifically to §2B1.1 because such offenses involve obtaining, altering or denial of authorized access to stored communications, conduct related to theft, property destruction, and fraud.

III. Implementation of the Directive

The amendment described above implements the directive to the Commission to ensure that the guidelines and policy statements applicable to persons convicted of an offense under 18 U.S.C. § 1030 reflect the serious nature and growing incidence of computer offenses and the need to provide an effective deterrent and appropriate punishment. The amendment provides enhanced penalties for computer offenses that involve increased risks to the public or government, or that involve a heightened level of intent. As described below, with the promulgation of this amendment, the guidelines and policy statements applicable to offenses under 18 U.S.C. § 1030 address each of the eight factors enumerated in the directive.

A. Loss

Loss is a primary component of the guidelines relevant to computer crime. The loss table at §2B1.1(b)(1) provides for substantial sentence increases in two level increments based on increasing loss amounts. Both §§2B2.3 and 2B3.2 also include enhancements for loss. *See* §§2B2.3(b)(3) and 2B3.2(b)(2). The potential harm, including loss, involved in violations of 18 U.S.C. § 1030(a)(1) (accessing and disseminating national defense or restricted information with reason to believe it could be used to the injury of the United States), which are referenced to §2M3.2 (Gathering National Defense Information), is accounted for by the high base offense levels in that guideline.

As described in Section II(A)(4) of this Report, the amendment makes a change in §2B1.1 relating to loss. The amendment modifies the existing rule of construction relating to loss in computer crimes cases to more fully incorporate the statutory definition of loss in 18

---

[4] The Commission only collects and records data for cases involving felony offenses or Class A misdemeanors. Prior to the Homeland Security Act, non-aggravated offenses under 18 U.S.C. § 2701 were Class B misdemeanors because they carried a maximum term of imprisonment of six months. *See* 18 U.S.C. § 3559(a)(7). Accordingly, no data on convictions for these offenses is available.

U.S.C. § 1030(e)(11), and to clarify its application to offenses under 18 U.S.C. § 1030.

B. Sophistication and Planning

The factor of sophistication and planning is addressed in the guidelines. Section 2B1.1 includes a two level enhancement, with a minimum offense level of 12, for use of "sophisticated means" at §2B1.1(b)(8)(C). This enhancement applies to "especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense." USSG §2B1.1 comment. (n.6(B)) (to be redesignated n.7(B)). The majority of section 1030 cases are sentenced under §2B1.1 and accordingly would be potentially eligible for this enhancement. Section 2B3.2, the guideline applicable to violations of section 1030(a)(7) involving extortionate demands to damage protected computers, also addresses sophistication and planning. In that guideline, there is a three level enhancement at §2B3.2(b)(3) for offenses that involved preparation to carry out, or a demonstrated ability to carry out, certain serious types of threats, including threats of death, serious bodily injury, kidnapping or product tampering. The amendment has expanded the scope of this enhancement so that it will also apply to offenses that involved preparation to carry out, or a demonstrated ability to carry out, an extortionate threat to damage 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. With respect to cases sentenced under §2M3.2, involving unauthorized access to and dissemination of national defense and restricted information, the high base offense levels in that guideline – level 35 if the offense involved top secret information and level 30 otherwise – take into account the sophistication and planning inherent in such offenses and punish such offenses at or near the statutory maximum.

The Commission's data analysis suggests that many 18 U.S.C. §1030 offenses are relatively unsophisticated. Of the 116 cases reviewed, only 7 (6%) involved sophisticated means.

C. Commercial Advantage and Private Financial Benefit

This factor is related to statutory sentencing enhancements for offenses under 18 U.S.C. § 1030(a)(2), which prohibits the unauthorized access to a computer to obtain information from a financial institution, the government, or a "protected computer," and 18 U.S.C. § 2701, which prohibits the unauthorized access to stored electronic communications. Both of these offenses are referenced to §2B1.1. Violations of both statutes are misdemeanors (other than subsequent offenses) unless committed with one of the statutory aggravating purposes. Among the aggravated purposes for § 1030(a)(2) violations are commercial advantage and private financial gain. *See* 18 U.S.C. § 1030(c)(2)(B)(i). Among the aggravated purposes for violations of section 2701 are commercial advantage and private commercial gain. *See* 18 U.S.C. § 2701(b)(1).

Commercial advantage and private financial benefit are typical motivations in offenses sentenced under §2B1.1, the principal economic crime guideline, and the structure of the

guideline takes this into account. An offender's intended or realized financial gain or commercial advantage typically will be addressed by proportional enhancements in the loss table. *See* §2B1.1(b)(1). The Commission's data showed that of the 104 18 U.S.C. § 1030 cases sentenced under §2B1.1 (or a guideline consolidated with §2B1.1) in fiscal years 2001 and 2002, financial gain and/or commercial advantage was a motivation in 49 percent (51), and 78.4 percent (40) of those received an enhancement for loss. The eleven remaining cases either did not result in loss or involved minimal loss amounts insufficient to trigger an enhancement.

D. Malicious Intent

The second enhancement of the new specific offense characteristic in §2B1.1 addresses the factor of malicious intent. Section 1030(a)(5)(A)(i) prohibits the transmission of a program, information, code, or command to a protected computer with the intent to cause damage. Proof of one of the five harms listed in the statute is required to sustain a violation. The other two subsections of section 1030(a)(5)(A) proscribe similar offenses resulting in damage to protected computers, but do not require the same showing of intent to cause damage. Violations of section 1030(a)(5)(A)(i) have recently been singled out by Congress as being of particular concern. In October 2001, the USA PATRIOT Act increased the maximum penalty for these violations from five to ten years' imprisonment. It also expanded the scope of the crime by including damage affecting computer systems used in furtherance of the administration of justice, national defense, or national security as one of the harms that may be proven to sustain a violation. In the Homeland Security Act, Congress again increased penalties for section 1030(a)(5)(A)(i) violations, this time adding provisions that provide for penalties of up to either twenty years' or life imprisonment, if the offender knowingly or recklessly caused or attempted to cause either serious bodily injury or death.

Until this amendment, the guidelines did not distinguish between violations of section 1030(a)(5)(A)(i), in which damage is caused intentionally, and violations of sections (a)(5)(A)(ii) or (iii), in which damage is caused recklessly, negligently, or accidentally. Given the increased statutory penalties that are now available for violations of section 1030(a)(5)(A)(i) and the heightened level of intent involved in such violations, the Commission concluded that an increased level of punishment would be appropriate for those convicted of a section 1030(a)(5)(A)(i) offense. Accordingly, the new enhancement at §2B1.1(b)(13)(A)(ii) provides for a four level increase if an offender is convicted of section 1030(a)(5)(A)(i), an approximate 50 percent increase in sentence.

Finally, violations of section 1030(a)(5)(A)(i) (except those in which the only statutory harm alleged is loss of $5,000 or more) that are related to terrorism will be potentially eligible for the terrorism enhancement in §3A1.4 (Terrorism). That guideline provides a 12 level enhancement, with a minimum offense level of 32, if the offense is a felony that involved, or was intended to promote, a federal crime of terrorism. Offenses under sections 1030(a)(5)(A)(i) (except those in which the only statutory harm alleged is loss of at least $5,000) and 1030(a)(1) qualify as predicate terrorism offenses under 18 U.S.C. § 2332b(g)(5) as a result of changes implemented by the USA PATRIOT Act.

E. Privacy

The first enhancement of the new specific offense characteristic in §2B1.1 provides a two level increase for a conviction under 18 U.S.C. § 1030 that involves an intent to obtain personal information. A definition of "personal information" is provided in the commentary. The definition makes clear that "personal information" means sensitive or private information, including information in the possession of a third party. Examples of personal information include medical records, wills, diaries, private correspondence and e-mail, financial information and photographs of a sensitive or private nature.

Prior to this amendment, the issue of privacy had only been addressed in §2B1.1 by way of an upward departure provision. Application Note 17 (to be redesignated Application Note 18) to §2B1.1 provides a non-exhaustive list of factors a court may consider in determining whether an upward departure is appropriate. One of the factors is whether the offense caused or risked a substantial non-monetary harm, such as a substantial invasion of a privacy interest. USSG §2B1.1, comment. (n.17(A)(ii)) (to be redesignated n.18(A)(ii)). Although §2B1.1 does address privacy invasions with this discretionary upward departure provision, the Commission concluded that because of the increasing amount of sensitive personal information stored on computers, a specific enhancement was the most appropriate way to account for harm resulting from computer offenses that compromise personal information.

Analysis of the Commission's data revealed that in the 104 cases under 18 U.S.C. § 1030 that were sentenced under §2B1.1 (or a guideline consolidated with §2B1.1), approximately one third involved an intent to obtain personal information.

F. Computers Used in Furtherance of the Administration of Justice, National Defense, and National Security

The first enhancement of the new specific offense characteristic in §2B1.1 also addresses the factor of computer systems used by or for a government entity in furtherance of the administration of justice, national defense, or national security. This factor is derived from the statute. Section 1030(a)(5) prohibits causing damage to a protected computer through either the transmission of a program, information, code or command, or as a result of unauthorized access, and requires proof of one of five harms listed in the statute: loss of at least $5,000; impairment of medical treatment; physical injury; threat to public health or safety; or damage affecting a computer system used in furtherance of the administration of justice, national defense, or national security. *See* 18 U.S.C. § 1030(a)(5)(B). The last harm, damage affecting a computer system used in furtherance of the administration of justice, national defense, or national security, was added to the statute as part of the USA PATRIOT Act. Previously, the guidelines did not distinguish between violations of section 1030 that involved one of these important government computer systems and those that did not. The Commission concluded that such a distinction is warranted because computers used in furtherance of national defense, national security, or the administration of justice are deserving of heightened protection. Computer offenses involving one of these important government computer systems may be more serious because of the

potential significance of the information compromised or the harm caused or risked to these systems. Because of the importance of these types of computers, the Commission did not limit application of this new enhancement to section 1030(a)(5) violations. Rather, the enhancement may apply to any conviction of 18 U.S.C. § 1030 sentenced under §2B1.1 that involves such computers.

In addition to the changes in §2B1.1, the amendment also modifies §2B2.3 (Trespass) and §2B3.2 (Extortion by Force or Threat of Injury or Serious Damage) to expand existing enhancements in those guidelines to provide increased punishment for trespass and extortion offenses involving computer systems used by or for a government entity in furtherance of the administration of justice, national defense, or national security.

G. Critical Infrastructure

Offenses involving interference with critical infrastructure are addressed by both the first and third enhancements of the new specific offense characteristic in §2B1.1, as well as by the new upward departure provision at Application Note 18(B) to §2B1.1. As noted in section II(A)(1) of this Report, an offender will receive a two level enhancement under §2B1.1(b)(13)(A)(i) if the offense involved a computer system used to maintain or operate a critical infrastructure, an approximate 25 percent increase in sentence. Alternatively, if the offense resulted in a substantial disruption to a critical infrastructure, the offender will receive a six level enhancement, roughly doubling the sentence, with a minimum offense level of 24. In addition, the amendment adds an upward departure provision at Application Note 18(B) to provide that an upward departure would be warranted for cases in which the substantial disruption to a critical infrastructure had a debilitating impact. Critical infrastructure is defined in the commentary at Application Note 12(A) as "systems and assets vital to national defense, national security, economic security, public health or safety, or any combination of those matters." This definition is derived in part from the definition provided by Congress in the USA PATRIOT Act, *see* Pub. L. 107–56, § 1016; 42 U.S.C. § 5195c(e), but was modified to ensure that the enhancement could apply to a substantial disruption of a critical infrastructure that was regional, rather than national, in scope. The application note also makes clear that a critical infrastructure can be publicly or privately owned and provides examples.

In addition to the changes in §2B1.1, the amendment also modifies §2B2.3 and §2B3.2 to expand existing enhancements in those guidelines to provide increased punishment for trespass and extortion offenses involving computer systems used to maintain or operate a critical infrastructure.

H. Threat to Public Health and Safety, Injury to Person

The guidelines address those relatively rare but significant cases in which a computer offense creates a threat to public health or safety, or injury to a person. Section 2B1.1(b)(11) provides a two level increase, with a minimum offense level of 14, for an offense that involved "the conscious or reckless risk of death or serious bodily injury." In addition, Application Note

17(A)(ii) (to be redesignated Application Note 18(A)(ii)) provides that an upward departure may be warranted if an offense caused or risked substantial non-monetary harm, including physical harm. The amendment has further addressed the issue of bodily harm by expanding the upward departure provision to account for computer cases that result in death. It now provides that "[a]n upward departure would be warranted, for example, in an 18 U.S.C. § 1030 offense involving damage to a protected computer, if, as a result of that offense, death resulted." §2B1.1 comment. (n.18(A)(ii)). Finally, cases involving threats to public health and safety or injury may be related to attacks on the critical infrastructure or terrorism. The significant enhancements applicable to such offenses, *see* §2B1.1(b)(13)(A)(iii) and §3A1.4, account for such threats.

IV. Recommendation For Increased Statutory Penalties

The Commission recommends that Congress consider increasing statutory maximum penalties for violations of 18 U.S.C. § 1030(a)(1), which proscribes the accessing and dissemination of national defense or restricted information with reason to believe that such information could be used to the injury of the United States or to the advantage of a foreign nation. Currently, section 1030(a)(1) violations are punishable by a statutory maximum term of imprisonment of ten years for a first offense and a statutory maximum term of imprisonment of twenty years for a subsequent offense. *See* 18 U.S.C. §§ 1030(c)(1)(A)-(B). The sentencing guidelines treat offenses under section 1030(a)(1) quite seriously. Under §2M3.2, the base offense level for a section 1030(a)(1) offense in which top secret information was gathered is level 35, which corresponds to a range of imprisonment of 168 to 210 months in Criminal History Category I. This range is significantly above the ten year statutory maximum. Even with a three level reduction for acceptance of responsibility, *see* §3E1.1, the range of imprisonment in such a case would be 121 to 151 months, still above the statutory maximum for a first offense. For section 1030(a)(1) offenses not involving top secret information, the base offense level under §2M3.2 is 30, which corresponds to a range of imprisonment of 97 to 121 months in Criminal History Category I.

As part of the USA PATRIOT Act, Congress added section 1030(a)(1) offenses to the list of terrorism predicates in 18 U.S.C. §2332b(g)(5)(B). As a result, a section 1030(a)(1) offense committed in furtherance of terrorism could be eligible for the terrorism enhancement in §3A1.4. That guideline provides a 12 level increase, with a minimum level of 32, for a felony that involved, or was intended to promote, a federal crime of terrorism. It also provides that the defendant's criminal history category will be Category VI. Because the guideline penalties already approach or exceed the statutory maximum term of ten years, the terrorism adjustment will have limited or no effect in section 1030(a)(1) cases involving terrorism. Accordingly, the Commission recommends that Congress increase statutory penalties for offenses under 18 U.S.C. § 1030(a)(1).

V. Conclusion

The Commission shares the concerns of Congress regarding the importance of deterring and appropriately punishing computer crimes. The amendment promulgated by the Commission reflects the serious and risky nature of many computer offenses. The Commission stands ready to provide any additional information Congress may require related to the further consideration of these important issues.