REVISED PROPOSED AMENDMENT: CYBERCRIME

Synopsis of Proposed Amendment: *This proposed amendment responds to the Cyber Security Enhancement Act of 2002, set forth in section 225 of the Homeland Security Act, Pub. L. 107–296. The Act directs the Commission to review and, if appropriate, amend the guidelines and policy statements applicable to persons convicted of an offense under 18 U.S.C. § 1030. In carrying out the directive, the Commission is required to ensure that the sentencing guidelines and policy statements reflect the serious nature and the growing incidence of computer offenses and the need to provide an effective deterrent and appropriate punishment. The Commission further is required to consider the following factors and the extent to which they are or are not accounted for by the 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 gain;

(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.

The proposed amendment addresses the directive by making several changes to §§2B1.1, 2B2.3 and 2B3.2, guidelines to which 18 U.S.C. § 1030 offenses are referred. These changes are designed to address certain factors that currently may not be adequately accounted for by the guidelines. In addition, the proposed amendment references 18 U.S.C. § 2701 to §2B1.1 in Appendix A.

First, the proposed amendment modifies §2B1.1 to address three of the directive factors in one, multi-pronged specific offense characteristic. The first prong provides a two level enhancement for convictions under 18 U.S.C. § 1030 that involve either a computer system used to maintain or operate a critical infrastructure or a computer system used in furtherance of the administration of justice, national defense or national security. Currently, the relevant guidelines do not distinguish between 18 U.S.C. § 1030 offenses that involve intrusions into these important computer systems and those that do not.

The second prong of the specific offense characteristic addresses convictions under 18 U.S.C. § 1030 that involve "malicious intent." Subsection (a)(5)(A)(i) of 18 U.S.C. § 1030 proscribes the knowing transmission of a program, information, code, or command, with the intent to cause damage to a protected computer. Proof of one of five harms identified in the statute is required to sustain a violation. In October 2001, the USA PATRIOT Act, Pub. L. 107–56, increased the statutory maximum penalty for violations of this subsection from five to ten years' imprisonment. The Homeland Security Act further

increased penalties for certain § 1030(a)(5)(A)(i) violations by providing 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. The significant statutory penalties provided for convictions of 18 U.S.C. § 1030(a)(5)(A)(i) reflect the serious nature of these crimes. Currently, the guidelines do not account for the heightened intent to cause damage involved in § 1030(a)(5)(A)(i) offenses. The proposed amendment would provide a four level enhancement for a defendant convicted of such an offense.

The third prong of the proposed specific offense characteristic addresses the factor relating to the significant interference with or disruption to a critical infrastructure. Section 2B1.1 currently does not account for this factor. The proposed amendment provides a six level enhancement and a minimum offense level of 24 for a conviction under 18 U.S.C. § 1030 that resulted in a substantial disruption of a critical infrastructure. The minimum offense level was chosen for two reasons. First, currently in §2B1.1 there is a floor of level 24 for an offense that substantially jeopardized a financial institution or that substantially endangered the solvency or financial security of a publicly traded company. See §2B1.1(b)(12)(B). The harm sought to be addressed by the proposed substantial disruption of a critical infrastructure enhancement is comparable to, and potentially more serious than, the harm addressed by the enhancement in §2B1.1(b)(12)(B). Accordingly, the Commission may wish to provide a comparable minimum offense level to ensure that offenses involving a substantial disruption of a critical infrastructure are treated at least as seriously. Second, level 24 is proposed in recognition of the fact that some offenders to whom the enhancement would apply will be subject to a statutory maximum of five years' imprisonment, which corresponds to a point at the top of the guideline range (51-63 months) for that level. (With acceptance of responsibility credit, the applicable guideline range could be much lower.)

The application note pertaining to the third prong of the enhancement provides a definition of critical infrastructure that is taken from the USA PATRIOT Act. That definition is relatively narrow, encompassing only those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on [national] security, national economic security, national public health or safety, or any combination of those matters." See Pub. L. 107-56, § 1016; 42 U.S.C. § 5195c(e). The note also explains that a critical infrastructure may be privately or publicly owned and provides examples of critical infrastructures. These examples are the eight categories of critical infrastructure identified by the National Infrastructure Protection Center. To ensure that the most egregious cases are addressed, the proposed amendment also provides an encouraged upward departure for cases in which the disruption of the critical infrastructure is so substantial as to have an actual debilitating impact on national security, national economic security, national public health or safety, or any combination of these matters.

The construct of the proposed three-pronged specific offense characteristic for §2B1.1 is worth a further mention. As described above, the proposed specific offense characteristic includes three enhancements, each based on factors in the directive. The enhancements are tiered based on offense seriousness and would not be applied cumulatively. The graduated levels ensure incremental punishment for increasingly serious conduct, and were chosen 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 is provided. This minimum offense level will ensure that offenders involved in the most serious offenses – even those with a statutory maximum of five years' imprisonment – will face a significant minimum guideline sentence.

Fourth, the proposed amendment modifies §2B2.3 (Trespass), to which 18 U.S.C. § 1030(a)(3) (misdemeanor trespass on a government computer) offenses are referenced, and §2B3.2 (Extortion), to which 18 U.S.C. § 1030(a)(7) (extortionate demand to damage protected computer) offenses are referenced, to provide enhancements relating to computer systems used (1) to maintain or operate a critical infrastructure; or (2) by a government entity in furtherance of administration of justice, national defense, or national security. In the trespass guideline, §2B2.3, there is currently a two level enhancement at §2B2.3(b)(1) for a trespass that occurred on a secured government facility, a nuclear energy facility, a vessel or aircraft of the United States, a secured area of an airport, or a residence. In the extortion guideline, §2B3.2, there is currently a three level enhancement at §2B3.2(b)(3) for an offense that involved preparation to carry out, or a demonstrated ability to carry out, a threat of death, serious bodily injury, kidnapping or product tampering. The proposed amendment expands the scope of these enhancements to cover offenses involving the types of computer systems described above.

Fifth, the proposed amendment modifies the rule of construction applicable to protected computer cases. Currently, Application Note 2(A)(v)(III) to §2B1.1 provides that in cases involving the unauthorized access, or access exceeding authorization, to a protected computer, certain pecuniary harms as described in the application note are to be considered "actual loss" regardless of whether such harms were reasonably foreseeable. In October 2001, as part of the USA PATRIOT Act, Congress added a definition of "loss" to 18 U.S.C. § 1030. See 18 U.S.C. § 1030(e)(11). This statutory definition is similar, but not quite identical, to the definition currently contained within the special rule of construction. The proposed amendment modifies the rule of construction to clarify its application to all 18 U.S.C. § 1030 cases and to more fully incorporate the statutory definition of loss.

Sixth, the proposed amendment expands the upward departure note in Application Note 17(A)(ii) of §2B1.1. Currently, that note provides that an upward departure may be warranted if an offense caused or risked substantial non-monetary harm. By way of examples, the application note cites physical harm, psychological harm, severe emotional trauma and substantial invasions of privacy. The proposed amendment expands this paragraph to provide that an upward departure would be warranted for an offense under 18 U.S.C. § 1030 involving damage to a protected computer that results in death.

Finally, the proposed amendment references offenses under 18 U.S.C. § 2701 (unlawful access to stored communications) to §2B1.1. Currently, these offenses are not referenced in Appendix A. Prior to the Homeland Security Act, an offense under section 2701 was punishable by a term of up to six months' imprisonment, unless the offense was committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, in which case the maximum term of imprisonment was one year, for a first offense. Subsequent aggravated offenses were punishable by a term of up to two years' imprisonment. The Act expanded the scope of section 2701 by adding an additional aggravated purpose to the statute (an offense committed in furtherance of a criminal or tortious act is now subject to heightened penalties), and increased penalties for all violations of section 2701. Now, a section 2701 offense is punishable by a term of one year imprisonment, unless the offense was committed with one of the aggravated purposes, in which case the maximum term of imprisonment is five years, for a first offense. Subsequent aggravated offenses are punishable by a term of 10 years, and other subsequent offenses are punishable by a term of five years' imprisonment. Given the increased penalties now available for 2701 offenses, the proposed amendment provides a reference for the statute in Appendix A. Section 2701 offenses would be referenced to §2B1.1 because offenses under that section involve the obtaining, altering or denial of authorized access to stored electronic communications, conduct that is related to fraud, theft, and property damage, which are covered by §2B1.1.

Proposed Amendment:

§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**

(b) Specific Offense Characteristics

* * *

(13) (A) (Apply the greatest): If the defendant was convicted of an offense under—

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

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

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

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

~~(13)~~(14) * * *

Commentary

Statutory Provisions: 7 U.S.C. §§ 6, 6b, 6c, 6h, 6o, 13, 23; 15 U.S.C. §§ 50, 77e, 77q, 77x, 78j, 78ff, 80b-6, 1644, 6821; 18 U.S.C. §§ 38, 225, 285-289, 471-473, 500, 510, 553(a)(1), 641, 656, 657, 659, 662, 664, 1001-1008, 1010-1014, 1016-1022, 1025, 1026, 1028, 1029, 1030(a)(4)-(5), 1031, 1341-1344, 1348, 1350, 1361, 1363, 1702, 1703 (if vandalism or malicious mischief, including destruction of mail, is involved), 1708, 1831, 1832, 1992, 1993(a)(1), (a)(4), 2113(b), 2312-2317, 2332b(a)(1); 2701; 29 U.S.C. § 501(c); 42 U.S.C. § 1011; 49 U.S.C. §§ 30170, 46317(a), 60123(b). For additional statutory provision(s), see Appendix A (Statutory Index).

Application Notes:

1. Definitions.—

"Protected computer" has the meaning given that term in 18 U.S.C. § 1030(e)(2).

* * *

2. *Loss Under Subsection (b)(1).—This application note applies to the determination of loss under subsection (b)(1).*

* * *

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

* * *

(III) ~~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.~~

Offenses Under 18 U.S.C. § 1030.—In the case of an offense under 18 U.S.C. § 1030, actual loss includes the following pecuniary harm, regardless of whether such pecuniary harm was reasonably foreseeable: 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 damages incurred because of interruption of service.

* * *

Application Notes 11 through 16 are redesignated as Application Notes 12 through 17, respectively.

11. Application of Subsection (b)(13).—

(A) Definitions.—For purposes of subsection (b)(13):

"Critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. A critical infrastructure may be publicly or privately owned. Examples of critical infrastructures include gas and oil production, storage, and delivery systems, water supply systems, telecommunications networks, electrical power delivery systems, financing and banking systems, emergency services (including medical, police, fire, and rescue services), transportation systems and services (including highways, mass transit, airlines, and airports), and government operations that provide essential services to the public. "United States" has the meaning given that term in Application Note 6(A) of this guideline.

"Government entity" has the meaning given that term in 18 U.S.C. § 1030(e)(9).

(B) Subsection (b)(13)(iii).—If the same conduct that forms the basis for an enhancement under subsection (b)(13)(iii) is the only conduct that forms the basis for an enhancement under subsection (b)(12)(B), do not apply the enhancement under subsection (b)(12)(B).

* * *

~~16.~~17. Departure Considerations.—

(A) Upward Departure Considerations.—*There may be cases in which the offense level determined under this guideline substantially understates the seriousness of the offense. In such cases, an upward departure may be warranted. The following is a non-exhaustive list of factors that the court may consider in determining whether an upward departure is warranted:*

(ii) The offense caused or risked substantial non-monetary harm. For example, the offense caused physical harm, psychological harm, or severe emotional trauma, or resulted in a substantial invasion of a privacy interest (through, for example, the theft of personal information such as medical, educational, or financial records). An 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.

* * *

(v) In a case involving stolen information from a "protected computer", ~~as defined in 18 U.S.C. § 1030(e)(2)~~, the defendant sought the stolen information to further a broader criminal purpose.

* * *

(B) Upward Departure for Debilitating Impact on a Critical Infrastructure.—An upward departure would be warranted in a case in which subsection (b)(13)(iii) applies and the disruption to the critical infrastructure(s) is so substantial as to have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters.

~~(B)~~(C) * * *

Background: (Technical and conforming amendments to background commentary to be made.)

* * *

Subsections (b)(13) implements the directive in section 225(b) of Public Law 107–296. The minimum offense level of 24 provided in subsection (b)(13)(B) for an offense that resulted in a substantial disruption of a critical infrastructure reflects the serious impact such an offense could have on national security, national economic security, national public health or safety, or a combination of any of these matters.

* * *

§2B2.3. Trespass

(a) Base Offense Level: **4**

(b) Specific Offense Characteristics

(1) If the trespass occurred (A) at a secured government facility; (B) at a nuclear energy facility; (C) on a vessel or aircraft of the United States; (D) in a secured area of an airport; ~~or~~ (E) at a residence; (F) on a computer system used (i) to maintain or operate a critical infrastructure; or (ii) by or for a government entity in furtherance of the administration of justice, national defense, or national security, increase by **2** levels.

* * *

Commentary

Statutory Provisions: 18 U.S.C. §§ 1030(a)(3), 1036; 42 U.S.C. § 7270b. For additional statutory provision(s), see Appendix A (Statutory Index).

Application Notes:

1. Definitions.—For purposes of this guideline:

"Airport" has the meaning given that term in section 47102 of title 49, United States Code.

"Critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. A critical infrastructure may be publicly or privately owned. Examples of critical infrastructures include gas and oil production, storage, and delivery systems, water supply systems, telecommunications networks, electrical power delivery systems, financing and banking systems, emergency services (including medical, police, fire, and rescue services), transportation systems and services (including highways, mass transit, airlines, and airports), and government operations that provide essential services to the public. "United States" has the meaning given that term in Application Note 6(A) of the Commentary to §2B1.1 (Theft, Property Destruction, and Fraud).

* * *

§2B3.2. Extortion by Force or Threat of Injury or Serious Damage

* * *

(b) Specific Offense Characteristics

(3) * * *

(B) If the offense involved preparation to carry out a threat of (i) death; (ii) serious bodily injury; (iii) kidnapping; ~~or~~ (iv) product tampering;

(v) damage to a computer system used (I) to maintain or operate a critical infrastructure; or (II) by or for a government entity in furtherance of the administration of justice, national defense, or national security; or if the participant(s) otherwise demonstrated the ability to carry out such threat, increase by **3** levels.

Commentary

* * *

Application Notes:

1. ~~*"Firearm," "dangerous weapon," "otherwise used," "brandished," "bodily injury," "serious bodily injury," "permanent or life-threatening bodily injury," "abducted," and "physically restrained" are defined in the Commentary to §1B1.1 (Application Instructions).*~~ *Definitions.—For purposes of this guideline:*

"Abducted," "bodily injury," "brandished," "dangerous weapon," "firearm," "otherwise used," "permanent or life-threatening bodily injury," "physically restrained" and "serious bodily injury," have the meaning given those terms in Application Note 1 of §1B1.1 (Application Instructions).

"Critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. A critical infrastructure may be publicly or privately owned. Examples of critical infrastructures include gas and oil production, storage, and delivery systems, water supply systems, telecommunications networks, electrical power delivery systems, financing and banking systems, emergency services (including medical, police, fire, and rescue services), transportation systems and services (including highways, mass transit, airlines, and airports), and government operations that provide essential services to the public. "United States" has the meaning given that term in Application Note 6(A) of the Commentary to §2B1.1 (Theft, Property Destruction, and Fraud).

"Government entity" has the meaning given that term in 18 U.S.C. § 1030(e)(9).

* * *

§2M3.2. Gathering National Defense Information

(a) Base Offense Level:

(1) **35**, if top secret information was gathered; or

(2) **30**, otherwise.

Commentary

Statutory Provisions: 18 U.S.C. §§ 793(a), (b), (c), (d), (e), (g), 1030(a)(1). For additional statutory provision(s), see Appendix A (Statutory Index).

* * *

APPENDIX A - STATUTORY INDEX

18 U.S.C. § 2512	2H3.2
18 U.S.C. § 2701	2B1.1