

The Commentary to § 2B2.3 captioned "Application Notes" is amended in Note 1 by inserting after "United States Code." the following paragraph:

"'Critical infrastructure' means systems and assets vital to national defense, national security, economic security, public health or safety, or any combination of those matters. A critical infrastructure may be publicly or privately owned. Examples of critical infrastructures include gas and oil production, storage, and delivery systems, water supply systems, telecommunications networks, electrical power delivery systems, financing and banking systems, emergency services (including medical, police, fire, and rescue services), transportation systems and services (including highways, mass transit, airlines, and airports), and government operations that provide essential services to the public.";

and by inserting after "Instructions)." the following paragraph:

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

Section 2B3.2(b)(3)(B) is amended to read as follows:

"(B) If (i) the offense involved preparation to carry out a threat of (I) death; (II) serious bodily injury; (III) kidnapping; (IV) product tampering; or (V) damage to a computer system used to maintain or operate a critical infrastructure, or by or for a government entity in furtherance of the administration of justice, national defense, or national security; or (ii) the participant(s) otherwise demonstrated the ability to carry out a threat described in any of subdivisions (i)(I) through (i)(V), increase by 3 levels."

The Commentary to § 2B3.2 captioned "Application Notes" is amended by striking Note 1 and inserting the following:

"1. 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 the Commentary to § 1B1.1 (Application Instructions).

'Critical infrastructure' means systems and assets vital to national defense, national security, economic security, public health or safety, or any combination of those matters. A critical infrastructure may be publicly or privately owned. Examples of critical infrastructures include gas and oil production, storage, and delivery

systems, water supply systems, telecommunications networks, electrical power delivery systems, financing and banking systems, emergency services (including medical, police, fire, and rescue services), transportation systems and services (including highways, mass transit, airlines, and airports), and government operations that provide essential services to the public.

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

The Commentary to § 2M3.2 captioned "Statutory Provisions" is amended by inserting "\$" before "793(a)"; and by inserting ", 1030(a)(1)" after "(g)".

Appendix A (Statutory Index) is amended by inserting after the line referenced to 18 U.S.C. 2512 the following:

"18 U.S.C. 2701 2B1.1".

Reason for Amendment: This amendment addresses the serious harm and invasion of privacy that can result from offenses involving the misuse of, or damage to, computers. It implements the directive in section 225(b) of the Homeland Security Act of 2002, Pub. L. 107–296, which required the Commission to review, and if appropriate amend, the guidelines and policy statements applicable to persons convicted of offenses under 18 U.S.C. 1030 (fraud and related activity in connection with computers) to ensure that the guidelines and policy statements reflect the serious nature and growing incidence of such offenses and the need for an effective deterrent and appropriate punishment. The directive further requires the Commission to consider the extent to which eight specific factors were or were not accounted for by the guidelines. The amendment responds to the directive by making several changes to §§ 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), and 2B3.2 (Extortion by Force or Threat of Injury or Serious Damage). These changes are designed to supplement existing guidelines and policy statements and thereby ensure that offenses under 18 U.S.C. 1030 are adequately addressed and punished.

First, the amendment adds a new specific offense characteristic at § 2B1.1(b)(13) with three alternative enhancements of two, four, and six levels. The first enhancement provides a two level increase for convictions

under 18 U.S.C. 1030 that involve either (1) a computer system used to maintain or operate a critical infrastructure or used in furtherance of the administration of justice, national defense, or national security; or (2) an intent to obtain private personal information. The second enhancement provides a four level increase for a conviction under 18 U.S.C.

1030(a)(5)(A)(i), which requires a heightened showing of intent to cause damage. The third enhancement provides a six level increase, with a minimum offense level of level 24, for a conviction under 18 U.S.C. 1030 that resulted in a substantial disruption of a critical infrastructure. 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. Accordingly, the most serious applicable enhancement will apply in any particular case.

The minimum offense level of level 24 applicable to the third such enhancement was chosen to maintain parity with the minimum offense level that applies to an offense that substantially jeopardized the safety and soundness of a financial institution, substantially endangered the solvency or financial security of a publicly traded company or an organization of at least 1,000 employees, or substantially endangered the solvency or financial security of 100 or more victims. See § 2B1.1(b)(12)(B). Because of the potential overlap in certain cases, the commentary provides that the enhancement at § 2B1.1(b)(12)(B) will not apply in a case in which the conduct supporting the six level critical infrastructure enhancement is the only conduct that forms the basis for the § 2B1.1(b)(12)(B) enhancement.

The minimum offense level of level 24 applicable to the third enhancement also reflects the fact that some offenders to whom the enhancement may apply will be subject to a statutory maximum penalty of five years' imprisonment, *i.e.*, those convicted of an offense under 18 U.S.C. 1030(a)(5)(A)(ii). To ensure that the most egregious cases involving critical infrastructure are adequately addressed, the amendment also provides an encouraged upward departure for cases in which the disruption of the critical infrastructure has a debilitating impact on national security, national economic security, national public health or safety, or any combination of these matters.