

fraud (*see* 18 U.S.C. 1030(a)(4)), the damaging of a protected computer resulting in certain types of specified harms (*see* 18 U.S.C. 1030(a)(5)), trafficking in passwords (*see* 18 U.S.C. 1030(a)(6)), and extortionate threats to cause damage to a "protected computer" (*see* 18 U.S.C. 1030(a)(7)). The statutory maximums for violations of section 1030 range from one year to life, depending upon the subsection violated and, in certain cases, whether certain aggravating factors are present. For example, although a violation of subsection (a)(2) generally carries a statutory maximum term of imprisonment of one year, if the offense was committed for purposes of commercial advantage or private financial gain (or one of the other aggravating conditions is met) the statutory maximum term of imprisonment is five years (*see* 18 U.S.C. 1030(c)(2)(B)). Section 1030 also provides heightened penalties for subsequent offenses. Currently Appendix A (Statutory Index) references convictions of section 1030 to §§ 2B1.1 (Theft, Fraud, and Property Destruction), 2B2.3 (Trespass), 2B3.2 (Extortion by Force or Threat of Injury or Serious Damage), and 2M3.2 (Gathering National Defense Information) depending on the conduct involved in the offense.

In response to the directive, the Commission is required to consider the eight identified factors and "the extent to which the guidelines may or may not account for them." Certain factors that the Commission must consider relate to, and in some instances mirror, either aggravating factors that result in higher statutory penalties under 18 U.S.C. 1030, or elements of certain offenses under 18 U.S.C. 1030. For example, the Commission has been directed to consider "whether the offense was committed for purposes of commercial advantage or private financial benefit." As noted above, this factor is specifically referenced in the statute as an aggravating factor with respect to violations of section 1030(a)(2). The current guidelines, however, do not provide for enhanced punishment for violations of section 1030(a)(2) that involve this aggravated purpose. Similarly, the Commission has been directed to consider "whether the offense involved a computer used by the government in furtherance of national defense, national security, or the administration of justice." Violations of section 1030(a)(5) require proof of one of five specified harms, one of which is "damage affecting a computer system used by or for a government entity in

furtherance of the administration of justice, national defense, or national security." (*see* 18 U.S.C. 1030(a)(5)(A) and (B)). The guidelines currently do not provide for an enhanced punishment when this type of harm results from a violation of section 1030(a)(5). Certain other factors that the Commission must consider already may be taken into account, in part or in whole, by the existing guidelines. For example, one factor that the Commission must consider is "the level of sophistication and planning involved in the offense." Currently, § 2B1.1(b)(8)(C) provides a two level increase and a minimum offense level of 12 for offenses that involve sophisticated means. This factor, therefore, may be at least partially accounted for by the existing guidelines.

The Commission requests comment regarding how it should address the directive and the extent to which the eight factors have or have not been accounted for by the guidelines. In addition, the Commission requests comment regarding whether it should provide enhancements in any of the guidelines that pertain to violations of 18 U.S.C. 1030 (*e.g.*, §§ 2B1.1, 2B2.3, 2B3.2, and 2M3.2) based on any of the factors listed in the directive? If so, which factors should be the bases for enhancements? What level enhancements (*e.g.*, [2] or [4] levels) would be appropriate and should the Commission provide a minimum offense level for any enhancement? Should any of the factors listed in the directive be identified in the guidelines as encouraged bases for upward departure? If so, for which violations of section 1030 and under which guidelines? Should any such enhancements or departure provisions be limited so as to apply only to specific violations of 18 U.S.C. 1030, and if so, which ones?

Alternatively, should the Commission structure an enhancement in any of the relevant guidelines to apply to convictions under 18 U.S.C. 1030, in general, or under certain subsections of section 1030 that the Commission may identify as warranting increased punishment? If any such enhancement is limited to certain subsections, what subsections should trigger that enhancement? Should the Commission provide an enhancement in the relevant guidelines that applies based on a combination of a conviction under section 1030 and certain serious conduct (*e.g.*, conduct relating to one of the eight factors contained in the directive, an aggravating factor resulting in an increased statutory maximum under the statute, or a particular

element of an offense under section 1030) that may be pertinent to the particular guideline under which the defendant is being sentenced? For any enhancement that the Commission may promulgate in response to this directive, what level enhancement would be appropriate (*e.g.*, [2] [4] levels)?

The Cyber Security Enhancement Act of 2002 also increased the statutory maximum term of imprisonment for convictions under 18 U.S.C. 1030(a)(5)(A)(i) (intentional damage to a protected computer) when certain aggravating conduct is present. The statute now provides a maximum term of imprisonment of twenty years' imprisonment if the offender knowingly or recklessly caused or attempted to cause serious bodily injury and provides a statutory maximum of life imprisonment if the offender knowingly or recklessly caused or attempted to cause death. The Commission requests comment regarding whether the current enhancement for an offense involving a conscious or reckless risk of death or serious bodily injury in § 2B1.1(b)(11), which provides a two level enhancement and a minimum offense level of 14, is sufficient in light of the increased statutory maximum terms of imprisonment for convictions with aggravating conduct under 18 U.S.C. 1030(a)(5)(A)(i). Alternatively, should the Commission provide an upward departure for such convictions? Should the Commission provide a cross reference in § 2B1.1 to the appropriate Chapter Two, Part A, Subpart 1 (Homicide) guideline in order to account for 18 U.S.C. 1030(a)(5)(A)(i) offenses that result in death?

Application Note 2(A)(v)(III) of § 2B1.1 provides a special rule of construction regarding offenses involving unlawful access to a protected computer. That rule states that for such offenses, actual loss includes the pecuniary harm of 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. This rule differs slightly from the statutory definition of loss provided in 18 U.S.C. 1030(e)(11), which was amended by the USA PATRIOT Act, Public Law 107-56, to include, in addition to the factors already included in the guidelines, the cost of responding to an offense, the cost of restoring the program or information to its condition prior to the offense, and any cost incurred or other consequential damages incurred because of interruption of service. Should the Commission modify the guidelines' rule to mirror the statutory definition of loss?