

ADDITIONAL FEDERAL STATUTES, GUIDELINES & REGULATIONS

Homeland Security Act of 2002 (Amendments)

http://www.usdoj.gov/criminal/cybercrime/homeland_CSEA.htm

**Provisions of Section 225 (“The Cyber Security Enhancement Act”)
of the
Homeland Security Act of 2002, H.R. 5710
That Amend Title 18 of the United States Code**

SEC. 225. CYBER SECURITY ENHANCEMENT ACT OF 2002.

(a) SHORT TITLE.—This section may be cited as the “Cyber Security Enhancement Act of 2002”.

(b) AMENDMENT OF SENTENCING GUIDELINES RELATING TO CERTAIN COMPUTER CRIMES.—

(1) DIRECTIVE TO THE UNITED STATES SENTENCING COMMISSION.—Pursuant to its authority under section 994(p) of title 28, United States Code, and in accordance with this subsection, the United States Sentencing Commission shall review and, if appropriate, amend its guidelines and its policy statements applicable to persons convicted of an offense under section 1030 of title 18, United States Code.

(2) REQUIREMENTS.—In carrying out this subsection, the Sentencing Commission shall— (A) ensure that the sentencing guidelines and policy statements reflect the serious nature of the offenses described in paragraph (1), the growing incidence of such offenses, and the need for an effective deterrent and appropriate punishment to prevent such offenses;

(B) consider the following factors and the extent to which the guidelines may or may not account for them—

(i) the potential and actual loss resulting from the offense;

(ii) the level of sophistication and planning involved in the offense;

(iii) whether the offense was committed for purposes of commercial advantage or private financial benefit;

(iv) whether the defendant acted with malicious intent to cause harm in committing the offense;

(v) the extent to which the offense violated the privacy rights of individuals harmed;

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

(vii) whether the violation was intended to or had the effect of significantly interfering with or disrupting a critical infrastructure; and

(viii) whether the violation was intended to or had the effect of creating a threat to public health or safety, or injury to any person;

(C) assure reasonable consistency with other relevant directives and with other sentencing guidelines;

(D) account for any additional aggravating or mitigating circumstances that might justify exceptions to the generally applicable sentencing ranges;

(E) make any necessary conforming changes to the sentencing guidelines; and

(F) assure that the guidelines adequately meet the purposes of sentencing as set forth in section 3553(a)(2) of title 18, United States Code.

(c) **STUDY AND REPORT ON COMPUTER CRIMES.**— Not later than May 1, 2003, the United States Sentencing Commission shall submit a brief report to Congress that explains any actions taken by the Sentencing Commission in response to this section and includes any recommendations the Commission may have regarding statutory penalties for offenses under section 1030 of title 18, United States Code.

(d) **EMERGENCY DISCLOSURE EXCEPTION.**—

(1) **IN GENERAL.**—Section 2702(b) of title 18, United States Code, is amended—

(A) in paragraph (5), by striking “or” at the end;

(B) in paragraph (6)(A), by inserting “or” at the end;

(C) by striking paragraph (6)(C); and

(D) by adding at the end the following: “(7) to a Federal, State, or local governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.”

(2) **REPORTING OF DISCLOSURES.**—A government entity that receives a disclosure under section 2702(b) of title 18, United States Code,

shall file, not later than 90 days after such disclosure, a report to the Attorney General stating the paragraph of that section under which the disclosure was made, the date of the disclosure, the entity to which the disclosure was made, the number of customers or subscribers to whom the information disclosed pertained, and the number of communications, if any, that were disclosed. The Attorney General shall publish all such reports into a single report to be submitted to Congress 1 year after the date of enactment of this Act.

(e) GOOD FAITH EXCEPTION.—Section 2520(d)(3) of title 18, United States Code, is amended by inserting “or 2511(2)(i)” after “2511(3)”.

(f) INTERNET ADVERTISING OF ILLEGAL DEVICES.—Section 2512(1)(c) of title 18, United States Code, is amended—

(1) by inserting “or disseminates by electronic means” after “or other publication”; and

(2) by inserting “knowing the content of the advertisement and” before “knowing or having reason to know”.

(g) STRENGTHENING PENALTIES.—Section 1030(c) of title 18, United States Code, is amended—

(1) by striking “and” at the end of paragraph (3);

(2) in each of subparagraphs (A) and (C) of paragraph (4), by inserting “except as provided in paragraph (5),” before “a fine under this title”;

(3) in paragraph (4)(C), by striking the period at the end and inserting “; and”;

(4) by adding at the end the following:

“(5)(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection

(a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and

“(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.”.

(h) PROVIDER ASSISTANCE.—

(1) SECTION 2703.—Section 2703(e) of title 18, United States Code, is amended by inserting “, statutory authorization” after “subpoena”.

(2) SECTION 2511.—Section 2511(2)(a)(ii) of title 18, United States Code, is amended by inserting “, statutory authorization,” after “court order” the last place it appears.

(i) EMERGENCIES.—Section 3125(a)(1) of title 18, United States Code, is amended—

(1) in subparagraph (A), by striking “or” at the end;

(2) in subparagraph (B), by striking the comma at the end and inserting a semicolon; and

(3) by adding at the end the following:

“(C) an immediate threat to a national security interest; or

“(D) an ongoing attack on a protected computer (as defined in section 1030) that constitutes a crime punishable by a term of imprisonment greater than one year;”.

USA Patriot Act

<http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03162:%5D>

Section 202 Authority to Intercept Voice Communications in Computer Hacking Investigations

Section 2516(1)(c) of title 18, United States Code, is amended by striking `and section 1341 (relating to mail fraud),' and inserting `section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse),'.

Section 209 Obtaining Voice-mail and Other Stored Voice Communications

Title 18, United States Code, is amended--

(1) in section 2510--

(A) in paragraph (1), by striking beginning with `and such' and all that follows through `communication'; and

(B) in paragraph (14), by inserting `wire or' after `transmission of'; and

(2) in subsections (a) and (b) of section 2703--

(A) by striking `CONTENTS OF ELECTRONIC' and inserting `CONTENTS OF WIRE OR ELECTRONIC' each place it appears;

(B) by striking `contents of an electronic' and inserting `contents of a wire or electronic' each place it appears; and

(C) by striking `any electronic' and inserting `any wire or electronic' each place it appears.

Section 210 Scope of Subpoenas for Electronic Evidence

Section 2703(c)(2) of title 18, United States Code, as redesignated by section 212, is amended--

(1) by striking `entity the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber' and inserting the following: `entity the--

`(A) name;

`(B) address;

`(C) local and long distance telephone connection records, or records of session times and durations;

`(D) length of service (including start date) and types of service utilized;

`(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

`(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber'; and

(2) by striking `and the types of services the subscriber or customer utilized,'.

Section 211 Clarifying the Scope of the Cable Act

Section 631 of the Communications Act of 1934 (47 U.S.C. 551) is amended--

(1) in subsection (c)(2)--

(A) in subparagraph (B), by striking `or';

(B) in subparagraph (C), by striking the period at the end and inserting `; or'; and

(C) by inserting at the end the following:

`(D) to a government entity as authorized under chapters 119, 121, or 206 of title 18, United States Code, except that such disclosure shall not include records revealing cable subscriber selection of video programming from a cable operator.'; and

(2) in subsection (h), by striking `A governmental entity' and inserting `Except as provided in subsection (c)(2)(D), a governmental entity'.

Section 212 Emergency Disclosures by Communications Providers

(a) DISCLOSURE OF CONTENTS-

(1) IN GENERAL- Section 2702 of title 18, United States Code, is amended--

(A) by striking the section heading and inserting the following:

`Sec. 2702. Voluntary disclosure of customer communications or records';

(B) in subsection (a)--

(i) in paragraph (2)(A), by striking `and' at the end;

(ii) in paragraph (2)(B), by striking the period and inserting `; and'; and

(iii) by inserting after paragraph (2) the following:

`(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.';

(C) in subsection (b), by striking `EXCEPTIONS- A person or entity' and inserting `EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS- A provider described in subsection (a)';

(D) in subsection (b)(6)--

(i) in subparagraph (A)(ii), by striking `or';

(ii) in subparagraph (B), by striking the period and inserting `; or'; and

(iii) by adding after subparagraph (B) the following:

`(C) if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay.'; and

(E) by inserting after subsection (b) the following:

`(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS- A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--

`(1) as otherwise authorized in section 2703;

`(2) with the lawful consent of the customer or subscriber;

`(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

`(4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information; or

`(5) to any person other than a governmental entity.'

(2) TECHNICAL AND CONFORMING AMENDMENT- The table of sections for chapter 121 of title 18, United States Code, is amended by striking the item relating to section 2702 and inserting the following:

`2702. Voluntary disclosure of customer communications or records.'

(b) REQUIREMENTS FOR GOVERNMENT ACCESS-

(1) IN GENERAL- Section 2703 of title 18, United States Code, is amended--

(A) by striking the section heading and inserting the following:

`Sec. 2703. Required disclosure of customer communications or records';

(B) in subsection (c) by redesignating paragraph (2) as paragraph (3);

(C) in subsection (c)(1)--

(i) by striking `(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may' and inserting `A governmental entity may require a provider of electronic communication service or remote computing service to';

(ii) by striking `covered by subsection (a) or (b) of this section) to any person other than a governmental entity.

`(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity' and inserting `)';

(iii) by redesignating subparagraph (C) as paragraph (2);

(iv) by redesignating clauses (i), (ii), (iii), and (iv) as subparagraphs (A), (B), (C), and (D), respectively;

(v) in subparagraph (D) (as redesignated) by striking the period and inserting `; or'; and

(vi) by inserting after subparagraph (D) (as redesignated) the following:

`(E) seeks information under paragraph (2).'; and

(D) in paragraph (2) (as redesignated) by striking `subparagraph (B)' and insert `paragraph (1)'.

(2) TECHNICAL AND CONFORMING AMENDMENT- The table of sections for chapter 121 of title 18, United States Code, is amended by striking the item relating to section 2703 and inserting the following:

`2703. Required disclosure of customer communications or records.'

Section 216 Pen Register and Trap and Trace Statute

(a) GENERAL LIMITATIONS- Section 3121(c) of title 18, United States Code, is amended--

(1) by inserting `or trap and trace device' after `pen register';

(2) by inserting `, routing, addressing,' after `dialing'; and

(3) by striking `call processing' and inserting `the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications'.

(b) ISSUANCE OF ORDERS-

(1) IN GENERAL- Section 3123(a) of title 18, United States Code, is amended to read as follows:

`(a) IN GENERAL-

`(1) ATTORNEY FOR THE GOVERNMENT- Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.

`(2) STATE INVESTIGATIVE OR LAW ENFORCEMENT OFFICER- Upon an application made under section 3122(a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

`(3)(A) Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication

service to the public, the agency shall ensure that a record will be maintained which will identify--

`(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;

`(ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;

`(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and

`(iv) any information which has been collected by the device.

To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device.

`(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).'

(2) CONTENTS OF ORDER- Section 3123(b)(1) of title 18, United States Code, is amended--

(A) in subparagraph (A)--

(i) by inserting `or other facility' after `telephone line'; and

(ii) by inserting before the semicolon at the end `or applied'; and

(B) by striking subparagraph (C) and inserting the following:

`(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and'.

(3) NONDISCLOSURE REQUIREMENTS- Section 3123(d)(2) of title 18, United States Code, is amended--

(A) by inserting `or other facility' after `the line'; and

(B) by striking `, or who has been ordered by the court' and inserting `or applied, or who is obligated by the order'.

(c) DEFINITIONS-

(1) COURT OF COMPETENT JURISDICTION- Section 3127(2) of title 18, United States Code, is amended by striking subparagraph (A) and inserting the following:

`(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated; or'.

(2) PEN REGISTER- Section 3127(3) of title 18, United States Code, is amended--

(A) by striking `electronic or other impulses' and all that follows through `is attached' and inserting `dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted,

provided, however, that such information shall not include the contents of any communication'; and

(B) by inserting `or process' after `device' each place it appears.

(3) TRAP AND TRACE DEVICE- Section 3127(4) of title 18, United States Code, is amended--

(A) by striking `of an instrument' and all that follows through the semicolon and inserting `or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;'; and

(B) by inserting `or process' after `a device'.

(4) CONFORMING AMENDMENT- Section 3127(1) of title 18, United States Code, is amended--

(A) by striking `and'; and

(B) by inserting `, and `contents' after `electronic communication service'.

(5) TECHNICAL AMENDMENT- Section 3124(d) of title 18, United States Code, is amended by striking `the terms of'.

(6) CONFORMING AMENDMENT- Section 3124(b) of title 18, United States Code, is amended by inserting `or other facility' after `the appropriate line'.

Section 217 Intercepting the Communications of Computer Trespassers

Chapter 119 of title 18, United States Code, is amended--

(1) in section 2510--

(A) in paragraph (18), by striking `and' at the end;

(B) in paragraph (19), by striking the period and inserting a semicolon; and

(C) by inserting after paragraph (19) the following:

`(20) `protected computer' has the meaning set forth in section 1030; and

`(21) `computer trespasser'--

`(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

`(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.'; and

(2) in section 2511(2), by inserting at the end the following:

`(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if--

`(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

`(II) the person acting under color of law is lawfully engaged in an investigation;

`(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and
` (IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.'

Section 220 Nationwide Search Warrants for E-mail

(a) IN GENERAL- Chapter 121 of title 18, United States Code, is amended--

(1) in section 2703, by striking `under the Federal Rules of Criminal Procedure' every place it appears and inserting `using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation'; and

(2) in section 2711--

(A) in paragraph (1), by striking `and';

(B) in paragraph (2), by striking the period and inserting `; and'; and

(C) by inserting at the end the following:

`(3) the term `court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation.'

(b) CONFORMING AMENDMENT- Section 2703(d) of title 18, United States Code, is amended by striking `described in section 3127(2)(A)'

Section 814 Deterrence and Prevention of Cyberterrorism

(a) CLARIFICATION OF PROTECTION OF PROTECTED COMPUTERS- Section 1030(a)(5) of title 18, United States Code, is amended--

(1) by inserting `(i)' after `(A)';

(2) by redesignating subparagraphs (B) and (C) as clauses (ii) and (iii), respectively;

(3) by adding `and' at the end of clause (iii), as so redesignated; and

(4) by adding at the end the following:

`(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--

`(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;

`(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

`(iii) physical injury to any person;

`(iv) a threat to public health or safety; or

`(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;'

(b) PROTECTION FROM EXTORTION- Section 1030(a)(7) of title 18, United States Code, is amended by striking `, firm, association, educational institution, financial institution, government entity, or other legal entity,'.

(c) PENALTIES- Section 1030(c) of title 18, United States Code, is amended--

(1) in paragraph (2)--

(A) in subparagraph (A) --

(i) by inserting `except as provided in subparagraph (B),' before `a fine';

(ii) by striking `(a)(5)(C)' and inserting `(a)(5)(A)(iii)'; and

(iii) by striking `and' at the end;

(B) in subparagraph (B), by inserting `or an attempt to commit an offense punishable under this subparagraph,' after `subsection (a)(2),' in the matter preceding clause (i); and

(C) in subparagraph (C), by striking `and' at the end;

(2) in paragraph (3)--

(A) by striking `, (a)(5)(A), (a)(5)(B),' both places it appears; and

(B) by striking `(a)(5)(C)' and inserting `(a)(5)(A)(iii)'; and

(3) by adding at the end the following:

`(4)(A) a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

`(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

`(C) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section.'

(d) DEFINITIONS- Section 1030(e) of title 18, United States Code is amended--

(1) in paragraph (2)(B), by inserting `, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States' before the semicolon;

(2) in paragraph (7), by striking `and' at the end;

(3) by striking paragraph (8) and inserting the following:

`(8) the term `damage' means any impairment to the integrity or availability of data, a program, a system, or information;';

(4) in paragraph (9), by striking the period at the end and inserting a semicolon; and

(5) by adding at the end the following:

`(10) the term `conviction' shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

`(11) the term `loss' means 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 consequential damages incurred because of interruption of service; and

`(12) the term `person' means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.'

(e) DAMAGES IN CIVIL ACTIONS- Section 1030(g) of title 18, United States Code is amended--

(1) by striking the second sentence and inserting the following: `A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages.'; and

(2) by adding at the end the following: `No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.'

(f) AMENDMENT OF SENTENCING GUIDELINES RELATING TO CERTAIN COMPUTER FRAUD AND ABUSE- Pursuant to its authority under section 994(p) of title 28, United States Code, the United States Sentencing Commission shall amend the Federal sentencing guidelines to ensure that any individual convicted of a violation of section 1030 of title 18, United States Code, can be subjected to appropriate penalties, without regard to any mandatory minimum term of imprisonment.

Section 815 Additional Defense to Civil Actions Relating to Preserving Records in Response to government Requests

Section 2707(e)(1) of title 18, United States Code, is amended by inserting after `or statutory authorization' the following: `(including a request of a governmental entity under section 2703(f) of this title)'

Section 816 Development and Support of Cybersecurity Forensic Capabilities

(a) IN GENERAL- The Attorney General shall establish such regional computer forensic laboratories as the Attorney General considers appropriate, and provide support to existing computer forensic laboratories, in order that all such computer forensic laboratories have the capability--

- (1) to provide forensic examinations with respect to seized or intercepted computer evidence relating to criminal activity (including cyberterrorism);
- (2) to provide training and education for Federal, State, and local law enforcement personnel and prosecutors regarding investigations, forensic analyses, and prosecutions of computer-related crime (including cyberterrorism);
- (3) to assist Federal, State, and local law enforcement in enforcing Federal, State, and local criminal laws relating to computer-related crime;
- (4) to facilitate and promote the sharing of Federal law enforcement expertise and information about the investigation, analysis, and prosecution of computer-related crime with State and local law enforcement personnel and prosecutors, including the use of multijurisdictional task forces; and
- (5) to carry out such other activities as the Attorney General considers appropriate.

(b) AUTHORIZATION OF APPROPRIATIONS-

- (1) AUTHORIZATION- There is hereby authorized to be appropriated in each fiscal year \$50,000,000 for purposes of carrying out this section.
- (2) AVAILABILITY- Amounts appropriated pursuant to the authorization of appropriations in paragraph (1) shall remain available until expended.

[Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001](#)

Section 202 Authority to Intercept Voice Communications in Computer Hacking Investigations

Previous law: Under previous law, investigators could not obtain a wiretap order to intercept wire communications (those involving the human voice) for violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030). For example, in several investigations, hackers have stolen teleconferencing services from a telephone company and used this mode of communication to plan and execute hacking attacks.

Amendment: Section 202 amends 18 U.S.C. § 2516(1) – the subsection that lists those crimes for which investigators may obtain a wiretap order for wire communications – by adding felony violations of 18 U.S.C. § 1030 to the list of predicate offenses.¹ This provision will sunset December 31, 2005.

Section 209 Obtaining Voice-mail and Other Stored Voice Communications

Previous law: Under previous law, the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2703 et seq., governed law enforcement access to stored electronic communications (such as e-mail), but not stored wire communications (such as voice-mail). Instead, the wiretap statute governed such access because the definition of "wire communication" (18 U.S.C. § 2510(1)) included stored communications, arguably requiring law enforcement to use a wiretap order (rather than a search warrant) to obtain

unopened voice communications. Thus, law enforcement authorities used a wiretap order to obtain voice communications stored with a third party provider but could use a search warrant if that same information were stored on an answering machine inside a criminal's home.

Regulating stored wire communications through section 2510(1) created large and unnecessary burdens for criminal investigations. Stored voice communications possess few of the sensitivities associated with the real-time interception of telephones, making the extremely burdensome process of obtaining a wiretap order unreasonable.

Moreover, in large part, the statutory framework envisions a world in which technology-mediated voice communications (such as telephone calls) are conceptually distinct from non-voice communications (such as faxes, pager messages, and e-mail). To the limited extent that Congress acknowledged that data and voice might co-exist in a single transaction, it did not anticipate the convergence of these two kinds of communications typical of today's telecommunications networks. With the advent of MIME — Multipurpose Internet Mail Extensions — and similar features, an e-mail may include one or more "attachments" consisting of any type of data, including voice recordings. As a result, a law enforcement officer seeking to obtain a suspect's unopened e-mail from an ISP by means of a search warrant (as required under 18 U.S.C. § 2703(a)) had no way of knowing whether the inbox messages include voice attachments (i.e., wire communications) which could not be compelled using a search warrant.

Amendment: Section 209 of the Act alters the way in which the wiretap statute and ECPA apply to stored voice communications.² The amendments delete "electronic storage" of wire communications from the definition of "wire communication" in section 2510 and insert language in section 2703 to ensure that stored wire communications are covered under the same rules as stored electronic communications. Thus, law enforcement can now obtain such communications using the procedures set out in section 2703 (such as a search warrant), rather than those in the wiretap statute (such as a wiretap order).

This provision will sunset December 31, 2005.

Section 210 Scope of Subpoenas for Electronic Evidence

Previous law: Subsection 2703(c) allows the government to use a subpoena to compel a limited class of information, such as the customer's name, address, length of service, and means of payment. Prior to the amendments in Section 210 of the Act, however, the list of records that investigators could obtain with a subpoena did not include certain records (such as credit card number or other form of payment for the communication service) relevant to determining a customer's true identity. In many cases, users register with Internet service providers using false names. In order to hold these individuals responsible for criminal acts committed online, the method of payment is an essential means of determining true identity.

Moreover, many of the definitions in section 2703(c) were technology-specific, relating primarily to telephone communications. For example, the list included "local and long distance telephone toll billing records," but did not include parallel terms for communications on computer networks, such as "records of session times and durations." Similarly, the previous list allowed the government to use a subpoena to obtain the customer's "telephone number or other subscriber number or identity," but did not define what that phrase meant in the context of Internet communications.

Amendment: Amendments to section 2703(c) update and expand the narrow list of records that law enforcement authorities may obtain with a subpoena. The new subsection 2703(c)(2) includes "records of session times and durations," as well as "any temporarily assigned network address." In the Internet context, such records include the Internet Protocol (IP) address assigned by the provider to the customer or subscriber for a particular session, as well as the remote IP address from which a customer connects to the provider. Obtaining such records will make the process of identifying computer criminals and tracing their Internet communications faster and easier.

Moreover, the amendments clarify that investigators may use a subpoena to obtain the "means and source of payment" that a customer uses to pay for his or her account with a communications provider, "including any credit card or bank account number." 18 U.S.C. §2703(c)(2)(F). While generally helpful, this information will prove particularly valuable in identifying the users of Internet services where a company does not verify its users' biographical information. (This section is not subject to the sunset provision in section 224 of the Act).

Section 211 Clarifying the Scope of the Cable Act

Previous law: The law contains two different sets of rules regarding privacy protection of communications and their disclosure to law enforcement: one governing cable service (the "Cable Act") (47 U.S.C. § 551), and the other applying to the use of telephone service and Internet access (the wiretap statute, 18 U.S.C. § 2510 et seq.; ECPA, 18 U.S.C. § 2701 et seq.; and the pen register and trap and trace statute (the "pen/trap" statute), 18 U.S.C. § 3121 et seq.).

Prior to the amendments in Section 211 of the Act, the Cable Act set out an extremely restrictive system of rules governing law enforcement access to most records possessed by a cable company. For example, the Cable Act did not allow the use of subpoenas or even search warrants to obtain such records. Instead, the cable company had to provide prior notice to the customer (even if he or she were the target of the investigation), and the government had to allow the customer to appear in court with an attorney and then justify to the court the investigative need to obtain the records. The court could then order disclosure of the records only if it found by "clear and convincing evidence" – a standard greater than probable cause or even a preponderance of the evidence – that the subscriber was "reasonably suspected" of engaging in criminal activity. This procedure was completely unworkable for virtually any criminal investigation.

The legal regime created by the Cable Act caused grave difficulties in criminal investigations because today, unlike in 1984 when Congress passed the Cable Act, many cable companies offer not only traditional cable programming services but also Internet access and telephone service. In recent years, some cable companies have refused to accept subpoenas and court orders pursuant to the pen/trap statute and ECPA, noting the seeming inconsistency of these statutes with the Cable Act's harsh restrictions. See *In re Application of United States*, 36 F. Supp. 2d 430 (D. Mass. Feb. 9, 1999) (noting apparent statutory conflict and ultimately granting application for order under 18 U.S.C. 2703(d) for records from cable company providing Internet service). Treating identical records differently depending on the technology used to access the Internet made little sense. Moreover, these complications at times delayed or ended important investigations.

Amendment: Section 211 of the Act amends title 47, section 551(c)(2)(D), to clarify that ECPA, the wiretap statute, and the trap and trace statute govern disclosures by cable companies that relate to the provision of communication services – such as telephone and Internet services. The amendment preserves, however, the Cable Act's primacy with respect to records revealing what ordinary cable television programming a customer chooses to purchase, such as particular premium channels or "pay per view" shows. Thus, in a case where a customer receives both Internet access and conventional cable television service from a single cable provider, a government entity can use legal process under ECPA to compel the provider to disclose only those customer records relating to Internet service. (This section is not subject to the sunset provision in Section 224 of the Act).

Section 212 Emergency Disclosures by Communications Providers

Previous law: Previous law relating to voluntary disclosures by communication service providers was inadequate in two respects. First, it contained no special provision allowing providers to disclose customer records or communications in emergencies. If, for example, an Internet service provider ("ISP") independently learned that one of its customers was part of a conspiracy to commit an imminent terrorist attack, prompt disclosure of the account information to law enforcement could save lives. Since providing this information did not fall within one of the statutory exceptions, however, an ISP making such a disclosure could be sued civilly.

Second, prior to the Act, the law did not expressly permit a provider to voluntarily disclose non-content records (such as a subscriber's login records) to law enforcement for purposes of self-protection, even though providers could disclose the content of communications for this reason. See 18 U.S.C. § 2702(b)(5), 2703(c)(1)(B). Yet the right to disclose the content of communications necessarily implies the less intrusive ability to disclose non-content records. Cf. *United States v. Auler*, 539 F.2d 642, 646 n.9 (7th Cir. 1976) (phone company's authority to monitor and disclose conversations to protect against fraud necessarily implies right to commit lesser invasion of using, and disclosing fruits of, pen register device) (citing *United States v. Freeman*, 524 F.2d 337, 341 (7th Cir. 1975)). Moreover, as a practical matter, providers must have the right to disclose to law enforcement the facts surrounding attacks on their systems. For example, when an

ISP's customer hacks into the ISP's network, gains complete control over an e-mail server, and reads or modifies the e-mail of other customers, the provider must have the legal ability to report the complete details of the crime to law enforcement.

Amendment: Section 212 corrects both of these inadequacies in previous law. Section 212 amends subsection 2702(b)(6) to permit, but not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. This voluntary disclosure, however, does not create an affirmative obligation to review customer communications in search of such imminent dangers.

The amendments in Section 212 of the Act also change ECPA to allow providers to disclose information to protect their rights and property. It accomplishes this change by two related sets of amendments. First, amendments to sections 2702 and 2703 of title 18 simplify the treatment of voluntary disclosures by providers by moving all such provisions to 2702. Thus, section 2702 now regulates all permissive disclosures (of content and non-content records alike), while section 2703 covers only compulsory disclosures by providers. Second, an amendment to new subsection 2702(c)(3) clarifies that service providers do have the statutory authority to disclose non-content records to protect their rights and property. All of these changes will sunset December 31, 2005.

Section 216 Pen Register and Trap and Trace Statute

The pen register and trap and trace statute (the "pen/trap" statute) governs the prospective collection of non-content traffic information associated with communications, such as the phone numbers dialed by a particular telephone. Section 216 updates the pen/trap statute in three important ways: (1) the amendments clarify that law enforcement may use pen/trap orders to trace communications on the Internet and other computer networks; (2) pen/trap orders issued by federal courts now have nationwide effect; and (3) law enforcement authorities must file a special report with the court whenever they use a pen/trap order to install their own monitoring device (such as the FBI's DCS1000) on computers belonging to a public provider. The following sections discuss these provisions in greater detail. (This section is not subject to the sunset provision in Section 224 of the Act).

A. Using pen/trap orders to trace communications on computer networks

Previous law: When Congress enacted the pen/trap statute in 1986, it could not anticipate the dramatic expansion in electronic communications that would occur in the following fifteen years. Thus, the statute contained certain language that appeared to apply to telephone communications and that did not unambiguously encompass communications over computer networks.³ Although numerous courts across the country have applied the pen/trap statute to communications on computer networks, no federal district or appellate court has explicitly ruled on its propriety. Moreover, certain private litigants have challenged the application of the pen/trap statute to such electronic communications based on the statute's telephone-specific language.

Amendment: Section 216 of the Act amends sections 3121, 3123, 3124, and 3127 of title 18 to clarify that the pen/trap statute applies to a broad variety of communications technologies. References to the target "line," for example, are revised to encompass a "line or other facility." Such a facility might include, for example, a cellular telephone number; a specific cellular telephone identified by its electronic serial number; an Internet user account or e-mail address; or an Internet Protocol address, port number, or similar computer network address or range of addresses. In addition, because the statute takes into account a wide variety of such facilities, amendments to section 3123(b)(1)(C) now allow applicants for pen/trap orders to submit a description of the communications to be traced using any of these or other identifiers.

Moreover, the amendments clarify that orders for the installation of pen register and trap and trace devices may obtain any non-content information – all "dialing, routing, addressing, and signaling information" – utilized in the processing and transmitting of wire and electronic communications. Such information includes IP addresses and port numbers, as well as the "To" and "From" information contained in an e-mail header. Pen/trap orders cannot, however, authorize the interception of the content of a communication, such as words in the "subject line" or the body of an e-mail. Agents and prosecutors with questions about whether a particular type of information constitutes content should contact the Office of Enforcement Operations in the telephone context (202-514-6809) or the Computer Crime and Intellectual Property Section in the computer context (202-514-1026).

Further, because the pen register or trap and trace "device" often cannot be physically "attached" to the target facility, Section 216 makes two other related changes. First, in recognition of the fact that such functions are commonly performed today by software instead of physical mechanisms, the amended statute allows the pen register or trap and trace device to be "attached or applied" to the target facility. Likewise, Section 216 revises the definitions of "pen register" and "trap and trace device" in section 3127 to include an intangible "process" (such as a software routine) which collects the same information as a physical device.

B. Nationwide effect of pen/trap orders

Previous law: Under previous law, a court could only authorize the installation of a pen/trap device "within the jurisdiction of the court." Because of deregulation in the telecommunications industry, however, a single communication may be carried by many providers. For example, a telephone call may be carried by a competitive local exchange carrier, which passes it to a local Bell Operating Company, which passes it to a long distance carrier, which hands it to a local exchange carrier elsewhere in the U.S., which in turn may finally hand it to a cellular carrier. If these carriers do not pass source information with each call, identifying that source may require compelling information from a string of providers located throughout the country – each requiring a separate order.

Moreover, since, under previous law, a court could only authorize the installation of a pen/trap device within its own jurisdiction, when one provider indicated that the source of a communication was a different carrier in another district, a second order in the new district became necessary. This order had to be acquired by a supporting prosecutor in the new district from a local federal judge – neither of whom had any other interest in the case. Indeed, in one case investigators needed three separate orders to trace a hacker’s communications. This duplicative process of obtaining a separate order for each link in the communications chain has delayed or — given the difficulty of real-time tracing — completely thwarted important investigations.

Amendment: Section 216 of the Act divides section 3123 of title 18 into two separate provisions. New subsection (a)(1) gives federal courts the authority to compel assistance from any provider of communication services in the United States whose assistance is appropriate to effectuate the order.

For example, a federal prosecutor may obtain an order to trace calls made to a telephone within the prosecutor’s local district. The order applies not only to the local carrier serving that line, but also to other providers (such as long-distance carriers and regional carriers in other parts of the country) through whom calls are placed to the target telephone. In some circumstances, the investigators may have to serve the order on the first carrier in the chain and receive from that carrier information identifying the communication’s path to convey to the next carrier in the chain. The investigator would then serve the same court order on the next carrier, including the additional relevant connection information learned from the first carrier; the second carrier would then provide the connection information in its possession for the communication. The investigator would repeat this process until the order has been served on the originating carrier who is able to identify the source of the communication.

When prosecutors apply for a pen/trap order using this procedure, they generally will not know the name of the second or subsequent providers in the chain of communication covered by the order. Thus, the application and order will not necessarily name these providers. The amendments to section 3123 therefore specify that, if a provider requests it, law enforcement must provide a "written or electronic certification" that the order applies to that provider.

The amendments in Section 216 of the Act also empower courts to authorize the installation and use of pen/trap devices in other districts. Thus, for example, if a terrorism or other criminal investigation based in Virginia uncovers a conspirator using a phone or an Internet account in New York, the Virginia court can compel communications providers in New York to assist investigators in collecting information under a Virginia pen/trap order.

Consistent with the change above, Section 216 of the Act modifies section 3123(b)(1)(C) of title 18 to eliminate the requirement that federal pen/trap orders specify their geographic limits. However, because the new law gives nationwide effect for federal

pen/trap orders, an amendment to section 3127(2)(A) imposes a "nexus" requirement: the issuing court must have jurisdiction over the particular crime under investigation.

C. Reports for use of law enforcement pen/trap devices on computer networks

Section 216 of the Act also contains an additional requirement for the use of pen/trap devices in a narrow class of cases. Generally, when law enforcement serves a pen/trap order on a communication service provider that provides Internet access or other computing services to the public, the provider itself should be able to collect the needed information and provide it to law enforcement. In certain rare cases, however, the provider may be unable to carry out the court order, necessitating installation of a device (such as Etherpeek or the FBI's DCS1000) to collect the information. In these infrequent cases, the amendments in section 216 require the law enforcement agency to provide the following information to the court under seal within thirty days: (1) the identity of the officers who installed or accessed the device; (2) the date and time the device was installed, accessed, and uninstalled; (3) the configuration of the device at installation and any modifications to that configuration; and (4) the information collected by the device. 18 U.S.C. § 3123(a)(3).

Section 217 Intercepting the Communications of Computer Trespassers

Prior law: Although the wiretap statute allows computer owners to monitor the activity on their machines to protect their rights and property, until Section 217 of the Act was enacted it was unclear whether computer owners could obtain the assistance of law enforcement in conducting such monitoring. This lack of clarity prevented law enforcement from assisting victims to take the natural and reasonable steps in their own defense that would be entirely legal in the physical world. In the physical world, burglary victims may invite the police into their homes to help them catch burglars in the act of committing their crimes. The wiretap statute should not block investigators from responding to similar requests in the computer context simply because the means of committing the burglary happen to fall within the definition of a "wire or electronic communication" according to the wiretap statute. Indeed, because providers often lack the expertise, equipment, or financial resources required to monitor attacks themselves, they commonly have no effective way to exercise their rights to protect themselves from unauthorized attackers. This anomaly in the law created, as one commentator has noted, a "bizarre result," in which a "computer hacker's undeserved statutory privacy right trumps the legitimate privacy rights of the hacker's victims." Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 Wash. & Lee L. Rev. 1287, 1300 (2000).

Amendment: To correct this problem, the amendments in Section 217 of the Act allow victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer systems. Under new section 2511(2)(i), law enforcement may intercept the communications of a computer trespasser transmitted to, through, or from a protected computer. Before monitoring can occur, however, four requirements must be met. First, section 2511(2)(i)(I) requires that the owner or operator of the

protected computer must authorize the interception of the trespasser's communications. Second, section 2511(2)(i)(II) requires that the person who intercepts the communication be lawfully engaged in an ongoing investigation. Both criminal and intelligence investigations qualify, but the authority to intercept ceases at the conclusion of the investigation.

Third, section 2511(2)(i)(III) requires that the person acting under color of law have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation. Fourth, section 2511(2)(i)(IV) requires that investigators intercept only the communications sent or received by trespassers. Thus, this section would only apply where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of non-consenting users authorized to use the computer.

Finally, section 217 of the Act amends section 2510 of title 18 to create a definition of "computer trespasser." Such trespassers include any person who accesses a protected computer (as defined in section 1030 of title 18)⁴ without authorization. In addition, the definition explicitly excludes any person "known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator for access to all or part of the computer." 18 U.S.C. § 2510(21). For example, certain Internet service providers do not allow their customers to send bulk unsolicited e-mails (or "spam"). Customers who send spam would be in violation of the provider's terms of service, but would not qualify as trespassers – both because they are authorized users and because they have an existing contractual relationship with the provider. These provisions will sunset December 31, 2005.

Section 220 Nationwide Search Warrants for E-mail

Previous law: Section 2703(a) requires the government to use a search warrant to compel a provider to disclose unopened e-mail less than six months old. Because Rule 41 of the Federal Rules of Criminal Procedure requires that the "property" to be obtained be "within the district" of the issuing court, however, some courts have declined to issue section 2703(a) warrants for e-mail located in other districts. Unfortunately, this refusal has placed an enormous administrative burden on those districts in which major ISPs are located, such as the Eastern District of Virginia and the Northern District of California, even though these districts may have no relationship with the criminal acts under investigation. In addition, requiring investigators to obtain warrants in distant jurisdictions has slowed time-sensitive investigations.

Amendment: Section 220 of the Act amends section 2703(a) of title 18 (and parallel provisions elsewhere in section 2703) to allow investigators to use section 2703(a) warrants to compel records outside of the district in which the court is located, just as they use federal grand jury subpoenas and orders under section 2703(d). This change enables courts with jurisdiction over investigations to compel evidence directly, without requiring the intervention of agents, prosecutors, and judges in the districts where major ISPs are located. This provision will sunset December 31, 2005.

Section 814 Deterrence and Prevention of Cyberterrorism

Section 814 makes a number of changes to improve 18 U.S.C. § 1030, the Computer Fraud and Abuse Act. This section increases penalties for hackers who damage protected computers (from a maximum of 10 years to a maximum of 20 years); clarifies the *mens rea* required for such offenses to make explicit that a hacker need only intend damage, not a particular *type* of damage; adds a new offense for damaging computers used for national security or criminal justice; expands the coverage of the statute to include computers in foreign countries so long as there is an effect on U.S. interstate or foreign commerce; counts state convictions as "prior offenses" for purpose of recidivist sentencing enhancements; and allows losses to several computers from a hacker's course of conduct to be aggregated for purposes of meeting the \$5,000 jurisdictional threshold.

The following discussion analyzes these and other provisions in more detail.

A. Section 1030(c) - Raising the maximum penalty for hackers that damage protected computers and eliminating mandatory minimums

Previous law: Under previous law, first-time offenders who violate section 1030(a)(5) could be punished by no more than five years' imprisonment, while repeat offenders could receive up to ten years. Certain offenders, however, can cause such severe damage to protected computers that this five-year maximum did not adequately take into account the seriousness of their crimes. For example, David Smith pled guilty to violating section 1030(a)(5) for releasing the "Melissa" virus that damaged thousands of computers across the Internet. Although Smith agreed, as part of his plea, that his conduct caused over \$80,000,000 worth of loss (the maximum dollar figure contained in the Sentencing Guidelines), experts estimate that the real loss was as much as ten times that amount.

In addition, previous law set a mandatory sentencing guidelines minimum of six months imprisonment for any violation of section 1030(a)(5), as well as for violations of section 1030(a)(4) (accessing a protected computer with the intent to defraud).

Amendment: Section 814 of the Act raises the maximum penalty for violations for damaging a protected computer to ten years for first offenders, and twenty years for repeat offenders. 18 U.S.C. § 1030(c)(4). Congress chose, however, to eliminate all mandatory minimum guidelines sentencing for section 1030 violations.

B. Subsection 1030(c)(2)(C) and (e)(8) - Hackers need only intend to cause damage, not a particular consequence or degree of damage

Previous law: Under previous law, in order to violate subsections (a)(5)(A), an offender had to "intentionally [cause] damage without authorization." Section 1030 defined "damage" as impairment to the integrity or availability of data, a program, a system, or information that (1) caused loss of at least \$5,000; (2) modified or impairs medical treatment; (3) caused physical injury; or (4) threatened public health or safety.

The question repeatedly arose, however, whether an offender must *intend* the \$5,000 loss or other special harm, or whether a violation occurs if the person only intends to damage the computer, *that in fact* ends up causing the \$5,000 loss or harming the individuals. It appears that Congress never intended that the language contained in the definition of "damage" would create additional elements of proof of the actor's mental state. Moreover, in most cases, it would be almost impossible to prove this additional intent.

Amendment: Section 814 of the Act restructures the statute to make clear that an individual need only intend to damage the computer or the information on it, and not a specific dollar amount of loss or other special harm. The amendments move these jurisdictional requirements to 1030(a)(5)(B), explicitly making them elements of the offense, and define "damage" to mean "any impairment to the integrity or availability of data, a program, a system or information." 18 U.S.C. § 1030(e)(8) (emphasis supplied). Under this clarified structure, in order for the government to prove a violation of 1030(a)(5), it must show that the actor caused damage to a protected computer (with one of the listed mental states), and that the actor's conduct caused either loss exceeding \$5,000, impairment of medical records, harm to a person, or threat to public safety. 18 U.S.C. § 1030(a)(5)(B).

C. Section 1030(c) - Aggregating the damage caused by a hacker's entire course of conduct

Previous law: Previous law was unclear about whether the government could aggregate the loss resulting from damage an individual caused to different protected computers in seeking to meet the jurisdictional threshold of \$5,000 in loss. For example, an individual could unlawfully access five computers on a network on ten different dates — as part of a related course of conduct — but cause only \$1,000 loss to each computer during each intrusion. If previous law were interpreted not to allow aggregation, then that person would not have committed a federal crime at all since he or she had not caused over \$5,000 to any particular computer.

Amendment: Under the amendments in Section 814 of the Act, the government may now aggregate "loss resulting from a related course of conduct affecting one or more other protected computers" that occurs within a one year period in proving the \$5,000 jurisdictional threshold for damaging a protected computer. 18 U.S.C. § 1030(a)(5)(B)(i).

D. 1030(c)(2)(C) - New offense for damaging computers used for national security and criminal justice

Previous law: Section 1030 previously had no special provision that would enhance punishment for hackers who damage computers used in furtherance of the administration of justice, national defense, or national security. Thus, federal investigators and prosecutors did not have jurisdiction over efforts to damage criminal justice and military computers where the attack did not cause over \$5,000 loss (or meet one of the other special requirements). Yet these systems serve critical functions and merit felony prosecutions even where the damage is relatively slight. Indeed, attacks on computers

used in the national defense that occur during periods of active military engagement are particularly serious — even if they do not cause extensive damage or disrupt the war-fighting capabilities of the military — because they divert time and attention away from the military's proper objectives. Similarly, disruption of court computer systems and data could seriously impair the integrity of the criminal justice system.

Amendment: Amendments in Section 814 of the Act create section 1030(a)(5)(B)(v) to solve this inadequacy. Under this provision, a hacker violates federal law by damaging a computer "used by or for a government entity in furtherance of the administration of justice, national defense, or national security," even if that damage does not result in provable loss over \$5,000.

E. Subsection 1030(e)(2) - expanding the definition of "protected computer" to include computers in foreign countries

Previous law: Before the amendments in Section 814 of the Act, section 1030 of title 18 defined "protected computer" as a computer used by the federal government or a financial institution, or one "which is used in interstate or foreign commerce." 18 U.S.C. § 1030(e)(2). The definition did not explicitly include computers outside the United States.

Because of the interdependency and availability of global computer networks, hackers from within the United States are increasingly targeting systems located entirely outside of this country. The statute did not explicitly allow for prosecution of such hackers. In addition, individuals in foreign countries frequently route communications through the United States, even as they hack from one foreign country to another. In such cases, their hope may be that the lack of any U.S. victim would either prevent or discourage U.S. law enforcement agencies from assisting in any foreign investigation or prosecution.

Amendment: Section 814 of the Act amends the definition of "protected computer" to make clear that this term includes computers outside of the United States so long as they affect "interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B). By clarifying the fact that a domestic offense exists, the United States can now use speedier domestic procedures to join in international hacker investigations. As these crimes often involve investigators and victims in more than one country, fostering international law enforcement cooperation is essential.

In addition, the amendment creates the option, where appropriate, of prosecuting such criminals in the United States. Since the U.S. is urging other countries to ensure that they can vindicate the interests of U.S. victims for computer crimes that originate in their nations, this provision will allow the U.S. to provide reciprocal coverage.

F. Subsection 1030(e)(10) - counting state convictions as "prior offenses"

Previous law: Under previous law, the court at sentencing could, of course, consider the offender's prior convictions for State computer crime offenses. State convictions,

however, did not trigger the recidivist sentencing provisions of section 1030, which double the maximum penalties available under the statute.

Amendment: Section 814 of the Act alters the definition of "conviction" so that it includes convictions for serious computer hacking crimes under State law – i.e., State felonies where an element of the offense is "unauthorized access, or exceeding authorized access, to a computer." 18 U.S.C. § 1030(e)(10).

G. Subsection 1030(e)(11) -- Definition of "loss"

Previous law: Calculating "loss" is important where the government seeks to prove that an individual caused over \$5,000 loss in order to meet the jurisdictional requirements found in 1030(a)(5)(B)(i). Yet prior to the amendments in Section 814 of the Act, section 1030 of title 18 had no definition of "loss." The only court to address the scope of the definition of loss adopted an inclusive reading of what costs the government may include. In *United States v. Middleton*, 231 F.3d 1207, 1210-11 (9th Cir. 2000), the court held that the definition of loss includes a wide range of harms typically suffered by the victims of computer crimes, including costs of responding to the offense, conducting a damage assessment, restoring the system and data to their condition prior to the offense, and any lost revenue or costs incurred because of interruption of service.

Amendments: Amendments in Section 814 codify the appropriately broad definition of loss adopted in *Middleton*. 18 U.S.C. § 1030(e)(11).

Section 815 Additional Defense to Civil Actions Relating to Preserving Records in Response to government Requests

Section 815 added to an existing defense to a cause for damages for violations of the Electronic Communications Privacy Act, Chapter 121 of Title 18. Under prior law it was a defense to such a cause of action to rely in good faith on a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization. This amendment makes clear that the "statutory authorization" defense includes good-faith reliance on a government request to preserve evidence under 18 U.S.C. § 2703(f).

Section 816 Development and Support of Cybersecurity Forensic Capabilities

Section 816 requires the Attorney General to establish such regional computer forensic laboratories as he considers appropriate, and to provide support for existing computer forensic laboratories, to enable them to provide certain forensic and training capabilities. The provision also authorizes the spending of money to support those laboratories.

###

Sentencing Guidelines that Relate to Computer Intrusions

U.S. Sentencing Guidelines that Relate to Computer Intrusions

§ 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

(a) Base Offense Level: 6

(b) Specific Offense Characteristics

(1) If the loss exceeded \$5,000, increase the offense level as follows:

Loss	(Apply the Greatest)	<u>Increase in Level</u>
(A)	\$5,000 or less	no increase
(B)	More than \$5,000	add 2
(C)	More than \$10,000	add 4
(D)	More than \$30,000	add 6
(E)	More than \$70,000	add 8
(F)	More than \$120,000	add 10
(G)	More than \$200,000	add 12
(H)	More than \$400,000	add 14
(I)	More than \$1,000,000	add 16
(K)	More than \$2,500,000	add 18
(L)	More than	add 20

- \$7,000,000
- (M) More than \$20,000,000 add 22
- (N) More than \$50,000,000 add 24
- (O) More than \$100,000,000 add 26

(2) (Apply the greater) If the offense--

(A) (i) involved more than 10, but less than 50, victims; or (ii) was committed through mass-marketing, increase by 2 levels; or

(B) involved 50 or more victims, increase by 4 levels.

(3) If the offense involved a theft from the person of another, increase by 2 levels.

(4) If the offense involved receiving stolen property, and the defendant was a person in the business of receiving and selling stolen property, increase by 2 levels.

(5) If the offense involved misappropriation of a trade secret and the defendant knew or intended that the offense would benefit a foreign government, foreign instrumentality, or foreign agent, increase by 2 levels.

(6) If the offense involved theft of, damage to, or destruction of, property from a national cemetery, increase by 2 levels.

(7) If the offense involved (A) a misrepresentation that the defendant was acting on behalf of a charitable, educational, religious, or political organization, or a government agency; (B) a misrepresentation or other fraudulent action during the course of a bankruptcy proceeding; (C) a violation of any prior, specific judicial or administrative order, injunction, decree, or process not addressed elsewhere in the guidelines; or (D) a misrepresentation to a consumer in connection with obtaining, providing, or furnishing financial assistance for an institution of higher

education, increase by 2 levels. If the resulting offense level is less than level 10, increase to level 10.

(8) If (A) the defendant relocated, or participated in relocating, a fraudulent scheme to another jurisdiction to evade law enforcement or regulatory officials; (B) a substantial part of a fraudulent scheme was committed from outside the United States; or (C) the offense otherwise involved sophisticated means, increase by 2 levels. If the resulting offense level is less than level 12, increase to level 12.

(9) If the offense involved (A) the possession or use of any device-making equipment; (B) the production or trafficking of any unauthorized access device or counterfeit access device; or (C)(i) the unauthorized transfer or use of any means of identification unlawfully to produce or obtain any other means of identification; or (ii) the possession of 5 or more means of identification that unlawfully were produced from, or obtained by the use of, another means of identification, increase by 2 levels. If the resulting offense level is less than level 12, increase to level 12.

(10) If the offense involved an organized scheme to steal vehicles or vehicle parts, and the offense level is less than level 14, increase to level 14.

(11) If the offense involved (A) the conscious or reckless risk of death or serious bodily injury; or (B) possession of a dangerous weapon (including a firearm) in connection with the offense, increase by 2 levels. If the resulting offense level is less than level 14, increase to level 14.

(12) (Apply the greater) If--

(A) the defendant derived more than \$1,000,000 in gross receipts from one or more financial institutions as a result of the offense, increase by 2 levels; or

(B) the offense substantially jeopardized the safety and soundness of a financial institution, increase by 4 levels.

If the resulting offense level determined under subdivision (A) or (B) is less than level 24, increase to level 24.

(c) Cross References

(1) If (A) a firearm, destructive device, explosive material, or controlled substance was taken, or the taking of any such item was an object of the offense; or (B) the stolen property received, transported, transferred, transmitted, or possessed was a firearm, destructive device, explosive material, or controlled substance, apply § 2D1.1 (Unlawful Manufacturing, Importing, Exporting, or Trafficking (Including Possession with Intent to Commit These Offenses); Attempt or Conspiracy), § 2D2.1 (Unlawful Possession; Attempt or Conspiracy), § 2K1.3 (Unlawful Receipt, Possession, or Transportation of Explosive Materials; Prohibited Transactions Involving Explosive Materials), or § 2K2.1 (Unlawful Receipt, Possession, or Transportation of Firearms or Ammunition; Prohibited Transactions Involving Firearms or Ammunition), as appropriate.

(2) If the offense involved arson, or property damage by use of explosives, apply § 2K1.4 (Arson; Property Damage by Use of Explosives), if the resulting offense level is greater than that determined above.

(3) If (A) neither subdivision (1) nor (2) of this subsection applies; (B) the defendant was convicted under a statute proscribing false, fictitious, or fraudulent statements or representations generally (e.g., [18 U.S.C. § 1001](#), [§ 1341](#), [§ 1342](#), or §

[1343](#)); and (C) the conduct set forth in the count of conviction establishes an offense specifically covered by another guideline in Chapter Two (Offense Conduct), apply that other guideline.

(4) If the offense involved a cultural heritage resource, apply § 2B1.5 (Theft of, Damage to, or Destruction of, Cultural Heritage Resources; Unlawful Sale, Purchase, Exchange, Transportation, or Receipt of Cultural Heritage Resources), if the resulting offense level is greater than that determined above.

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, 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); [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.--For purposes of this guideline:

"Cultural heritage resource" has the meaning given that term in Application Note 1 of the Commentary to § 2B1.5 (Theft of, Damage to, or Destruction of, Cultural Heritage Resources; Unlawful Sale, Purchase, Exchange, Transportation, or Receipt of Cultural Heritage Resources).

"Financial institution" includes any institution described in [18 U.S.C. § 20](#), [§ 656](#), [§ 657](#), [§ 1005](#), [§ 1006](#), [§ 1007](#), or [§ 1014](#); any state or foreign bank, trust company, credit union, insurance company, investment company, mutual fund, savings (building and loan) association, union or employee pension fund; any health, medical, or hospital insurance association; brokers and dealers registered, or required to be registered, with the Securities and Exchange Commission; futures commodity merchants and commodity pool operators registered, or required to be registered, with the Commodity Futures Trading Commission; and any similar entity, whether or not insured by the federal government. "Union or employee pension fund" and "any health, medical, or hospital insurance association," primarily include large pension funds that serve many persons (e.g., pension funds of large national and international organizations, unions, and corporations doing substantial interstate business), and associations that undertake to provide pension, disability, or other benefits (e.g., medical or hospitalization insurance) to large numbers of persons.

"Firearm" and "destructive device" have the meaning given those terms in the Commentary to § 1B1.1 (Application Instructions).

"Foreign instrumentality" and "foreign agent" have the meaning given those terms in [18 U.S.C. § 1839\(1\) and \(2\)](#), respectively.

"National cemetery" means a cemetery (A) established under [section 2400 of title 38, United States Code](#); or (B) under the jurisdiction of the Secretary of the Army, the Secretary of the Navy, the Secretary of the Air Force, or the Secretary of the Interior.

"Theft from the person of another" means theft, without the use of force, of property that was being held by another person or was within arms' reach. Examples include pick-pocketing and non-forcible purse-snatching, such as the theft of a purse from a shopping cart.

"Trade secret" has the meaning given that term in [18 U.S.C. § 1839\(3\)](#).

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

(A) General Rule.--Subject to the exclusions in subdivision (D), loss is the greater of actual loss or intended loss.

(i) Actual Loss.--"Actual loss" means the reasonably foreseeable pecuniary harm that resulted from the offense.

(ii) Intended Loss.--"Intended loss" (I) means the pecuniary harm that was intended to result from the offense; and (II) includes intended pecuniary harm that would have been impossible or unlikely to occur (e.g., as in a government sting operation, or an insurance fraud in which the claim exceeded the insured value).

(iii) Pecuniary Harm.--"Pecuniary harm" means harm that is monetary or that otherwise is readily measurable in money. Accordingly, pecuniary harm does not include emotional distress, harm to reputation, or other non-economic harm.

(iv) Reasonably Foreseeable Pecuniary Harm.--For purposes of this guideline, "reasonably foreseeable pecuniary harm" means pecuniary harm that the defendant knew or, under the circumstances, reasonably should have known, was a potential result of the offense.

(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:

(I) Product Substitution Cases.--In the case of a product substitution offense, the reasonably foreseeable pecuniary harm includes the reasonably foreseeable costs of making substitute transactions and handling or disposing of the product delivered, or of retrofitting the product so that it can be used for its intended purpose, and the reasonably foreseeable costs of rectifying the actual or potential disruption to the victim's business operations caused by the product substitution.

(II) Procurement Fraud Cases.--In the case of a procurement fraud, such as a fraud affecting a defense contract award, reasonably foreseeable pecuniary harm includes the reasonably foreseeable administrative costs to the government and other participants of repeating or correcting the procurement action affected, plus any increased costs to procure the product or service involved that was reasonably foreseeable.

(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.

(B) Gain.--The court shall use the gain that resulted from the offense as an alternative measure of loss only if there is a loss but it reasonably cannot be determined.

(C) Estimation of Loss.--The court need only make a reasonable estimate of the loss. The sentencing judge is in a unique position to assess the evidence and estimate the loss based upon that evidence. For this reason, the court's loss determination is entitled to appropriate deference. See [18 U.S.C. § 3742\(e\) and \(f\)](#).

The estimate of the loss shall be based on available information, taking into account, as appropriate and practicable under the circumstances, factors such as the following:

- (i) The fair market value of the property unlawfully taken or destroyed; or, if the fair market value is impracticable to determine or inadequately measures the harm, the cost to the victim of replacing that property.
- (ii) The cost of repairs to damaged property.
- (iii) The approximate number of victims multiplied by the average loss to each victim.

(iv) More general factors, such as the scope and duration of the offense and revenues generated by similar operations.

(D) Exclusions from Loss.--Loss shall not include the following:

(i) Interest of any kind, finance charges, late fees, penalties, amounts based on an agreed-upon return or rate of return, or other similar costs.

(ii) Costs to the government of, and costs incurred by victims primarily to aid the government in, the prosecution and criminal investigation of an offense.

(E) Credits Against Loss.--Loss shall be reduced by the following:

(i) The money returned, and the fair market value of the property returned and the services rendered, by the defendant or other persons acting jointly with the defendant, to the victim before the offense was detected. The time of detection of the offense is the earlier of (I) the time the offense was discovered by a victim or government agency; or (II) the time the defendant knew or reasonably should have known that the offense was detected or about to be detected by a victim or government agency.

(ii) In a case involving collateral pledged or otherwise provided by the defendant, the amount the victim has recovered at the time of sentencing from disposition of the collateral, or if the collateral has not been disposed of by that time, the fair market value of the collateral at the time of sentencing.

(F) Special Rules.--Notwithstanding subdivision (A), the following special rules shall be used to assist in determining loss in the cases indicated:

(i) Stolen or Counterfeit Credit Cards and Access Devices; Purloined Numbers and Codes.--In a case involving any counterfeit access device or unauthorized access device, loss includes any unauthorized charges made with the counterfeit access device or unauthorized access device and shall be not less than \$500 per access device. However, if the unauthorized access device is a means of telecommunications access that identifies a specific telecommunications instrument or telecommunications account (including an electronic serial number/mobile identification number (ESN/MIN) pair), and that means was only possessed, and not used, during the commission of the offense, loss shall be not less than \$100 per unused means. For purposes of this subdivision, "counterfeit access device" and "unauthorized access device" have the meaning given those terms in Application Note 7(A).

(ii) Government Benefits.--In a case involving government benefits (e.g., grants, loans, entitlement program payments), loss shall be considered to be not less than the value of the benefits obtained by unintended recipients or diverted to

unintended uses, as the case may be. For example, if the defendant was the intended recipient of food stamps having a value of \$100 but fraudulently received food stamps having a value of \$150, loss is \$50.

(iii) Davis-Bacon Act Violations.--In a case involving a Davis-Bacon Act violation (i.e., a violation of [40 U.S.C. § 276a](#), criminally prosecuted under [18 U.S.C. § 1001](#)), the value of the benefits shall be considered to be not less than the difference between the legally required wages and actual wages paid.

(iv) Ponzi and Other Fraudulent Investment Schemes.--In a case involving a fraudulent investment scheme, such as a Ponzi scheme, loss shall not be reduced by the money or the value of the property transferred to any individual investor in the scheme in excess of that investor's principal investment (i.e., the gain to an individual investor in the scheme shall not be used to offset the loss to another individual investor in the scheme).

(v) Certain Other Unlawful Misrepresentation Schemes.--In a case involving a scheme in which (I) services were fraudulently rendered to the victim by persons falsely posing as licensed professionals; (II) goods were falsely represented as approved by a governmental regulatory agency; or (III) goods for which regulatory approval by a government agency was required but not obtained, or was obtained by fraud, loss shall include the amount paid for the property, services or goods transferred, rendered, or misrepresented, with no credit provided for the value of those items or services.

(vi) Value of Controlled Substances.--In a case involving controlled substances, loss is the estimated street value of the controlled substances.

(vii) Value of Cultural Heritage Resources.--In a case involving a cultural heritage resource, loss attributable to that cultural heritage resource shall be determined in accordance with the rules for determining the "value of the cultural heritage resource" set forth in Application Note 2 of the Commentary to § 2B1.5.

3. Victim and Mass-Marketing Enhancement under Subsection (b)(2).--

(A) Definitions.-- For purposes of subsection (b)(2):

(i) "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; or (III) invest for financial profit. "Mass-marketing" includes, for example, a telemarketing campaign that solicits a large number of individuals to purchase fraudulent life insurance policies.

(ii) "Victim" means (I) any person who sustained any part of the actual loss determined under subsection (b)(1); or (II) any individual who sustained bodily

injury as a result of the offense. "Person" includes individuals, corporations, companies, associations, firms, partnerships, societies, and joint stock companies.

(B) Undelivered United States Mail.--

(i) In General.--In a case in which undelivered United States mail was taken, or the taking of such item was an object of the offense, or in a case in which the stolen property received, transported, transferred, transmitted, or possessed was undelivered United States mail, "victim" means any person (I) described in subdivision (A)(ii) of this note; or (II) who was the intended recipient, or addressee, of the undelivered United States mail.

(ii) Special Rule.--A case described in subdivision (B)(i) of this note that involved a Postal Service (I) relay box; (II) collection box; (III) delivery vehicle; or (IV) satchel or cart, shall be considered to have involved 50 or more victims.

(iii) Definition.--"Undelivered United States mail" means mail that has not actually been received by the addressee or his agent (e.g., mail taken from the addressee's mail box).

(C) Vulnerable Victims.--If subsection (b)(2)(B) applies, an enhancement under § 3A1.1(b)(2) shall not apply.

4. Enhancement for Business of Receiving and Selling Stolen Property under Subsection (b)(4).--For purposes of subsection (b)(4), the court shall consider the following non-exhaustive list of factors in determining whether the defendant was in the business of receiving and selling stolen property:

(A) The regularity and sophistication of the defendant's activities.

(B) The value and size of the inventory of stolen property maintained by the defendant.

(C) The extent to which the defendant's activities encouraged or facilitated other crimes.

(D) The defendant's past activities involving stolen property.

5. Application of Subsection (b)(7).--

(A) In General.--The adjustments in subsection (b)(7) are alternative rather than cumulative. If, in a particular case, however,

more than one of the enumerated factors applied, an upward departure may be warranted.

(B) Misrepresentations Regarding Charitable and Other Institutions.-- Subsection (b)(7)(A) applies in any case in which the defendant represented that the defendant was acting to obtain a benefit on behalf of a charitable, educational, religious, or political organization, or a government agency (regardless of whether the defendant actually was associated with the organization or government agency) when, in fact, the defendant intended to divert all or part of that benefit (e.g., for the defendant's personal gain). Subsection (b)(7)(A) applies, for example, to the following:

- (i) A defendant who solicited contributions for a non-existent famine relief organization.
- (ii) A defendant who solicited donations from church members by falsely claiming to be a fundraiser for a religiously affiliated school.
- (iii) A defendant, chief of a local fire department, who conducted a public fundraiser representing that the purpose of the fundraiser was to procure sufficient funds for a new fire engine when, in fact, the defendant intended to divert some of the funds for the defendant's personal benefit.

(C) Fraud in Contravention of Prior Judicial Order.--Subsection (b)(7)(C) provides an enhancement if the defendant commits a fraud in contravention of a prior, official judicial or administrative warning, in the form of an order, injunction, decree, or process, to take or not to take a specified action. A defendant who does not comply with such a prior, official judicial or administrative warning demonstrates aggravated criminal intent and deserves additional punishment. If it is established that an entity the defendant controlled was a party to the prior proceeding that resulted in the official judicial or administrative action, and the defendant had knowledge of that prior decree or order, this enhancement applies even if the defendant was not a specifically named party in that prior case. For example, a defendant whose business previously was enjoined from selling a dangerous product, but who nonetheless engaged in fraudulent conduct to sell the product, is subject to this enhancement. This enhancement does not apply if the same conduct resulted in an enhancement pursuant to a provision found elsewhere in the guidelines (e.g., a violation of a condition of release addressed in § 2J1.7 (Commission of Offense While on Release) or a violation of probation addressed in § 4A1.1 (Criminal History Category)).

(D) College Scholarship Fraud.--For purposes of subsection (b)(7)(D):

"Financial assistance" means any scholarship, grant, loan, tuition, discount, award, or other financial assistance for the purpose of financing an education.

"Institution of higher education" has the meaning given that term in section 101 of the Higher Education Act of 1954 ([20 U.S.C. § 1001](#)).

(E) Non-Applicability of Enhancements.--

(i) Subsection (b)(7)(A).--If the conduct that forms the basis for an enhancement under subsection (b)(7)(A) is the only conduct that forms the basis for an adjustment under § 3B1.3 (Abuse of Position of Trust or Use of Special Skill), do not apply that adjustment under § 3B1.3.

(ii) Subsection (b)(7)(B) and (C).--If the conduct that forms the basis for an enhancement under subsection (b)(7)(B) or (C) is the only conduct that forms the basis for an adjustment under § 3C1.1 (Obstructing or Impeding the Administration of Justice), do not apply that adjustment under § 3C1.1.

6. Sophisticated Means Enhancement under Subsection (b)(8).--

(A) Definition of United States.--For purposes of subsection (b)(8)(B), "United States" means each of the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, Guam, the Northern Mariana Islands, and American Samoa.

(B) Sophisticated Means Enhancement.--For purposes of subsection (b)(8)(C), "sophisticated means" means especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense. For example, in a telemarketing scheme, locating the main office of the scheme in one jurisdiction but locating soliciting operations in another jurisdiction ordinarily indicates sophisticated means. Conduct such as hiding assets or transactions, or both, through the use of fictitious entities, corporate shells, or offshore financial accounts also ordinarily indicates sophisticated means.

(C) Non-Applicability of Enhancement.--If the conduct that forms the basis for an enhancement under subsection (b)(8) is the only conduct that forms the basis for an adjustment under § 3C1.1, do not apply that adjustment under § 3C1.1.

7. Application of Subsection (b)(9).--

(A) Definitions.--For purposes of subsection (b)(9):

"Counterfeit access device" (i) has the meaning given that term in [18 U.S.C. § 1029\(e\)\(2\)](#); and (ii) includes a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications service. "Telecommunications service" has the meaning given that term in [18 U.S.C. § 1029\(e\)\(9\)](#).

"Device-making equipment" (i) has the meaning given that term in [18 U.S.C. § 1029\(e\)\(6\)](#); and (ii) includes (I) any hardware or software that has been configured as described in [18 U.S.C. § 1029\(a\)\(9\)](#); and (II) a scanning receiver referred to in [18 U.S.C. § 1029\(a\)\(8\)](#). "Scanning receiver" has the meaning given that term in [18 U.S.C. § 1029\(e\)\(8\)](#).

"Means of identification" has the meaning given that term in [18 U.S.C. § 1028\(d\)\(4\)](#), except that such means of identification shall be of an actual (i.e., not fictitious) individual, other than the defendant or a person for whose conduct the defendant is accountable under § 1B1.3 (Relevant Conduct).

"Produce" includes manufacture, design, alter, authenticate, duplicate, or assemble. "Production" includes manufacture, design, alteration, authentication, duplication, or assembly.

"Unauthorized access device" has the meaning given that term in [18 U.S.C. § 1029\(e\)\(3\)](#).

(B) Identification Documents.--Offenses involving identification documents, false identification documents, and means of identification, in violation of [18 U.S.C. § 1028](#), also are covered by this guideline. If the primary purpose of the offense, under [18 U.S.C. § 1028](#), was to violate, or assist another to violate, the law

pertaining to naturalization, citizenship, or legal resident status, apply § 2L2.1 (Trafficking in a Document Relating to Naturalization) or § 2L2.2 (Fraudulently Acquiring Documents Relating to Naturalization), as appropriate, rather than this guideline.

(C) Application of Subsection (b)(9)(C)(i).--

(i) In General.--Subsection (b)(9)(C)(i) applies in a case in which a means of identification of an individual other than the defendant (or a person for whose conduct the defendant is accountable under § 1B1.3 (Relevant Conduct)) is used without that individual's authorization unlawfully to produce or obtain another means of identification.

(ii) Examples.--Examples of conduct to which subsection (b)(9)(C)(i) applies are as follows:

(I) A defendant obtains an individual's name and social security number from a source (e.g., from a piece of mail taken from the individual's mailbox) and obtains a bank loan in that individual's name. In this example, the account number of the bank loan is the other means of identification that has been obtained unlawfully.

(II) A defendant obtains an individual's name and address from a source (e.g., from a driver's license in a stolen wallet) and applies for, obtains, and subsequently uses a credit card in that individual's name. In this example, the credit card is the other means of identification that has been obtained unlawfully.

(iii) Nonapplicability of Subsection (b)(9)(C)(i): --Examples of conduct to which subsection (b)(9)(C)(i) does not apply are as follows:

(I) A defendant uses a credit card from a stolen wallet only to make a purchase. In such a case, the defendant has not used the stolen credit card to obtain another means of identification.

(II) A defendant forges another individual's signature to cash a stolen check. Forging another individual's signature is not producing another means of identification.

(D) Application of Subsection (b)(9)(C)(ii).--Subsection (b)(9)(C)(ii) applies in any case in which the offense involved the possession of 5 or more means of identification that unlawfully were produced or obtained, regardless of the number of individuals in whose name (or other identifying information) the means of identification were so produced or so obtained.

8. Chop Shop Enhancement under Subsection (b)(10).--Subsection (b)(10) provides a minimum offense level in the case of an ongoing, sophisticated operation (such as an auto theft ring or "chop shop") to steal vehicles or vehicle parts, or to receive stolen vehicles or vehicle parts. "Vehicles" refers to all forms of vehicles, including aircraft and watercraft.

9. Gross Receipts Enhancement under Subsection (b)(12)(A).--

(A) In General.--For purposes of subsection (b)(12)(A), the defendant shall be considered to have derived more than \$1,000,000 in gross receipts if the gross receipts to the defendant individually, rather than to all participants, exceeded \$1,000,000.

(B) Definition.--"Gross receipts from the offense" includes all property, real or personal, tangible or intangible, which is obtained directly or indirectly as a result of such offense. See [18 U.S.C. § 982\(a\)\(4\)](#).

10. Enhancement for Substantially Jeopardizing the Safety and Soundness of a Financial Institution under Subsection (b)(12)(B).--For purposes of subsection (b)(12)(B), an offense shall be considered to have substantially jeopardized the safety and soundness of a financial institution if, as a consequence of the offense, the institution (A) became insolvent; (B) substantially reduced benefits to pensioners or insureds; (C) was unable on demand to refund fully any deposit, payment, or investment; (D) was so depleted of its assets as to be forced to merge with another institution in order to continue active operations; or (E) was placed in substantial jeopardy of any of subdivisions (A) through (D) of this note.

11. Cross Reference in Subsection (c)(3).--Subsection (c)(3) provides a cross reference to another guideline in Chapter Two (Offense Conduct) in cases in which the defendant is convicted of a general fraud statute, and the count of conviction establishes an offense more aptly covered by another guideline. Sometimes, offenses involving fraudulent statements are prosecuted under [18 U.S.C. § 1001](#), or a similarly general statute, although the offense is also covered by a more specific statute. Examples include false entries regarding currency transactions, for which § 2S1.3 (Structuring Transactions to Evade Reporting Requirements) likely would be more apt, and false statements to a customs officer, for which § 2T3.1 (Evading Import Duties or Restrictions (Smuggling); Receiving or Trafficking in Smuggled Property) likely would be more apt. In certain other cases, the mail or wire fraud statutes, or other relatively broad statutes, are used primarily as jurisdictional bases for the prosecution of other offenses.

12. Continuing Financial Crimes Enterprise.--If the defendant is convicted under [18 U.S.C. § 225](#) (relating to a continuing financial crimes enterprise), the offense

level is that applicable to the underlying series of offenses comprising the "continuing financial crimes enterprise".

13. Partially Completed Offenses.--In the case of a partially completed offense (e.g., an offense involving a completed theft or fraud that is part of a larger, attempted theft or fraud), the offense level is to be determined in accordance with the provisions of § 2X1.1 (Attempt, Solicitation, or Conspiracy) whether the conviction is for the substantive offense, the inchoate offense (attempt, solicitation, or conspiracy), or both. See Application Note 4 of the Commentary to § 2X1.1.

14. Multiple-Count Indictments.--Some fraudulent schemes may result in multiple-count indictments, depending on the technical elements of the offense. The cumulative loss produced by a common scheme or course of conduct should be used in determining the offense level, regardless of the number of counts of conviction. See Chapter Three, Part D (Multiple Counts).

15. 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:

(i) A primary objective of the offense was an aggravating, non-monetary objective. For example, a primary objective of the offense was to inflict emotional harm.

(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).

(iii) The offense involved a substantial amount of interest of any kind, finance charges, late fees, penalties, amounts based on an agreed-upon return or rate of return, or other similar costs, not included in the determination of loss for purposes of subsection (b)(1).

(iv) The offense created a risk of substantial loss beyond the loss determined for purposes of subsection (b)(1).

(v) The offense endangered the solvency or financial security of one or more victims.

(vi) 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.

(vii) In a case involving access devices or unlawfully produced or unlawfully obtained means of identification:

(I) The offense caused substantial harm to the victim's reputation or credit record, or the victim suffered a substantial inconvenience related to repairing the victim's reputation or a damaged credit record.

(II) An individual whose means of identification the defendant used to obtain unlawful means of identification is erroneously arrested or denied a job because an arrest record has been made in that individual's name.

(III) The defendant produced or obtained numerous means of identification with respect to one individual and essentially assumed that individual's identity.

(B) Downward Departure Consideration.--There may be cases in which the offense level determined under this guideline substantially overstates the seriousness of the offense. In such cases, a downward departure may be warranted.

Background: This guideline covers offenses involving theft, stolen property, property damage or destruction, fraud, forgery, and counterfeiting (other than offenses involving altered or counterfeit bearer obligations of the United States). It also covers offenses involving altering or removing motor vehicle identification numbers, trafficking in automobiles or automobile parts with altered or obliterated identification numbers, odometer laws and regulations, obstructing correspondence, the falsification of documents or records relating to a benefit plan covered by the Employment Retirement Income Security Act, and the failure to maintain, or falsification of, documents required by the Labor Management Reporting and Disclosure Act.

Because federal fraud statutes often are broadly written, a single pattern of offense conduct usually can be prosecuted under several code sections, as a result of which the offense of conviction may be somewhat arbitrary. Furthermore, most fraud statutes cover a broad range of conduct with extreme variation in severity. The specific offense characteristics and cross references contained in this guideline are designed with these considerations in mind.

The Commission has determined that, ordinarily, the sentences of defendants convicted of federal offenses should reflect the nature and magnitude of the loss caused or intended by their crimes. Accordingly, along with other relevant factors under the guidelines, loss serves as a measure of the seriousness of the offense and the defendant's relative culpability and is a principal factor in determining the offense level under this guideline.

Theft from the person of another, such as pickpocketing or non-forceful purse-snatching, receives an enhanced sentence because of the increased risk of physical injury. This guideline does not include an enhancement for thefts from the person by means of force or fear; such crimes are robberies and are covered under § 2B3.1 (Robbery).

A minimum offense level of level 14 is provided for offenses involving an organized scheme to steal vehicles or vehicle parts. Typically, the scope of such activity is substantial, but the value of the property may be particularly difficult to ascertain in individual cases because the stolen property is rapidly resold or otherwise disposed of in the course of the offense. Therefore, the specific offense characteristic of "organized scheme" is used as an alternative to "loss" in setting a minimum offense level.

Use of false pretenses involving charitable causes and government agencies enhances the sentences of defendants who take advantage of victims' trust in government or law enforcement agencies or the generosity and charitable motives of victims. Taking advantage of a victim's self-interest does not mitigate the seriousness of fraudulent conduct; rather, defendants who exploit victims' charitable impulses or trust in government create particular social harm. In a similar vein, a defendant who has been subject to civil or administrative proceedings for the same or similar fraudulent conduct demonstrates aggravated criminal intent and is deserving of additional punishment for not conforming with the requirements of judicial process or orders issued by federal, state, or local administrative agencies.

Offenses that involve the use of financial transactions or financial accounts outside the United States in an effort to conceal illicit profits and criminal conduct involve a particularly high level of

sophistication and complexity. These offenses are difficult to detect and require costly investigations and prosecutions. Diplomatic processes often must be used to secure testimony and evidence beyond the jurisdiction of United States courts. Consequently, a minimum offense level of level 12 is provided for these offenses.

Subsection (b)(6) implements the instruction to the Commission in [section 2 of Public Law 105-101](#).

Subsection (b)(7)(D) implements, in a broader form, the directive in section 3 of the College Scholarship Fraud Prevention Act of 2000, [Public Law 106- 420](#).

Subsection (b)(8) implements, in a broader form, the instruction to the Commission in [section 6\(c\)\(2\) of Public Law 105-184](#).

Subsections (b)(9)(A) and(B) implement the instruction to the Commission in section 4 of the Wireless Telephone Protection Act, [Public Law 105-172](#).

Subsection (b)(9)(C) implements the directive to the Commission in section 4 of the Identity Theft and Assumption Deterrence Act of 1998, [Public Law 105- 318](#). This subsection focuses principally on an aggravated form of identity theft known as "affirmative identity theft" or "breeding", in which a defendant uses another individual's name, social security number, or some other form of identification (the "means of identification") to "breed" (i.e., produce or obtain) new or additional forms of identification. Because [18 U.S.C. § 1028\(d\)](#) broadly defines "means of identification", the new or additional forms of identification can include items such as a driver's license, a credit card, or a bank loan. This subsection provides a minimum offense level of level 12, in part because of the seriousness of the offense. The minimum offense level accounts for the fact that the means of identification that were "bred" (i.e., produced or obtained) often are within the defendant's exclusive control, making it difficult for the individual victim to detect that the victim's identity has been "stolen." Generally, the victim does not become aware of the offense until certain harms have already occurred (e.g., a damaged credit rating or an inability to obtain a loan). The minimum offense level also

accounts for the non-monetary harm associated with these types of offenses, much of which may be difficult or impossible to quantify (e.g., harm to the individual's reputation or credit rating, inconvenience, and other difficulties resulting from the offense). The legislative history of the Identity Theft and Assumption Deterrence Act of 1998 indicates that Congress was especially concerned with providing increased punishment for this type of harm.

Subsection (b)(11)(B) implements, in a broader form, the instruction to the Commission in [section 110512 of Public Law 103-322](#).

Subsection (b)(12)(A) implements, in a broader form, the instruction to the Commission in [section 2507 of Public Law 101-647](#).

Subsection (b)(12)(B) implements, in a broader form, the instruction to the Commission in [section 961\(m\) of Public Law 101-73](#).

Historical Note: Effective November 1, 1987. Amended effective June 15, 1988 (see Appendix C, amendment 7); November 1, 1989 (see Appendix C, amendments 99- 101 and 303); November 1, 1990 (see Appendix C, amendments 312, 317, and 361); November 1, 1991 (see Appendix C, amendments 364 and 393); November 1, 1993 (see Appendix C, amendments 481 and 482); November 1, 1995 (see Appendix C, amendment 512); November 1, 1997 (see Appendix C, amendment 551); November 1, 1998 (see Appendix C, amendment 576); November 1, 2000 (see Appendix C, amendment 596); November 1, 2001 (see Appendix C, amendment 617); November 1, 2002 (see Appendix C, amendments 637, 638, and 646).

USSG § 2B1.1 (11/1/02)

[U.S. Sentencing Commission's Proposed Amendments to the Guidelines that Relate to Computer Intrusions \(Effective November 1, 2003\)](#)

Pursuant to section 994(p) of title 28, United States Code, the United States Sentencing Commission hereby submits to the Congress the following

amendments to the sentencing guidelines and the reasons therefor. As authorized by such section, the Commission specifies an effective date of November 1, 2003, for these amendments.

Amendments to the Sentencing Guidelines,
Policy Statements, and Official Commentary

3. Amendment: Section 2B1.1(b) is amended by inserting after subsection (b)(12) the following:

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

(i) 18 U.S.C. § 1030, and the offense involved (I) 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; or (II) an intent to obtain personal information, 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."

The Commentary to §2B1.1 captioned "Statutory Provisions" is amended by inserting ", 2701" after "2332b(a)(1)".

The Commentary to §2B1.1 captioned "Application Notes" is amended in Note 3(A)(v), as redesignated by Amendment 2, by striking subdivision (III) and inserting the following:

"(III) 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."

The Commentary to §2B1.1 captioned "Application Notes" is amended by inserting before Note 13, as redesignated by Amendment 2, the following:

"12. Application of Subsection (b)(13).—

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

‘Personal information’ means sensitive or private information (including such information in the possession of a third party), including (i) medical records; (ii) wills; (iii) diaries; (iv) private correspondence, including e-mail; (v) financial records; (vi) photographs of a sensitive or private nature; or (vii) similar information.

(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)."

The Commentary to §2B1.1 captioned "Application Notes" is amended in Note 18, as redesignated by Amendment 2, by adding at the end of subdivision (A)(ii) the following:

"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.";

by redesignating subdivision (B) as subdivision (C); and by inserting after subdivision (A) the following:

"(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."

The Commentary to §2B1.1 captioned "Background" is amended by adding at the end the following paragraph:

" Subsection (b)(13) implements the directive in section 225(b) of Public Law 107–296. The minimum offense level of level 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."

Section 2B2.3(b)(1) is amended by striking "or " after "airport;" and by inserting after "residence" the following:

"; or (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".

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.

A definition of critical infrastructure is provided in the commentary. This definition is derived in part from the definition of critical infrastructure in the USA PATRIOT Act (see Pub. L. 107–56, section 1016; 42 U.S.C. § 5195c(e)) but was modified to ensure that the enhancement will apply to substantial disruptions of critical infrastructure that are regional, rather than national, in scope. Examples of critical infrastructures are provided.

Second, the proposed amendment modifies the rule of construction relating to the calculation of loss in protected computer cases. This change was made to incorporate more fully the statutory definition of loss at 18 U.S.C. § 1030(e)(11), added as part of the USA PATRIOT Act, and to clarify its application to all 18 U.S.C. § 1030 offenses sentenced under §2B1.1.

Third, the proposed amendment expands the upward departure note in §2B1.1. That note provides that an upward departure may be warranted if an offense caused or risked substantial non-monetary harm, including physical harm. The amendment adds a provision that expressly states 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.

Fourth, the amendment modifies §2B2.3, to which 18 U.S.C. § 1030(a)(3) (misdemeanor trespass on a government computer) offenses are referenced, and §2B3.2, 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 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. The amendment expands the scope of existing enhancements to ensure that trespasses and extortions involving these types of important computer systems are addressed.

Finally, the amendment references offenses under 18 U.S.C. § 2701 (unlawful access to stored communications) to §2B1.1. Prior to the Act, a first offense under section 2701 was classified as a misdemeanor offense, and the guidelines did not reference the statute in Appendix A (Statutory Index). Given that the Act increased the penalties available for 18 U.S.C. § 2701 offenses, the amendment references the statute in Appendix A. Section 2701 offenses are referenced to §2B1.1 because such offenses involve the obtaining, altering, or denial of authorized access to stored wire or electronic communications, conduct that is related to fraud, theft, and property damage, which are covered by §2B1.1.

IP Sentencing Guidelines

§2B5.3. Criminal Infringement of Copyright or Trademark

(a) Base Offense Level: 8

(b) Specific Offense Characteristics

(1) If the infringement amount (A) exceeded \$2,000 but did not exceed \$5,000, increase by 1 level; or (B) exceeded \$5,000, increase by the number of levels from the table in §2B1.1 (Theft, Property Destruction, and Fraud) corresponding to that amount.

(2) If the offense involved the manufacture, importation, or uploading of infringing items, increase by 2 levels. If the resulting offense level is less than level 12, increase to level 12.

(3) If the offense was not committed for commercial advantage or private financial gain, decrease by 2 levels, but the resulting offense level shall be not less than level 8.

(4) If the offense involved (A) the conscious or reckless risk of serious bodily injury; or (B) possession of a dangerous weapon (including a firearm) in connection with the offense, increase by 2 levels. If the resulting offense level is less than level 13, increase to level 13.

Commentary

Statutory Provisions: 17 U.S.C. § 506(a); 18 U.S.C. §§ 2318-2320, 2511. For additional statutory provision(s), see Appendix A (Statutory Index).

Application Notes:

1. Definitions. §8212; For purposes of this guideline:

"Commercial advantage or private financial gain" means the receipt, or expectation of receipt, of anything of value, including other protected works.

"Infringed item" means the copyrighted or trademarked item with respect to which the crime against intellectual property was committed.

"Infringing item" means the item that violates the copyright or trademark laws.

"Uploading" means making an infringing item available on the Internet or a similar electronic bulletin board with the intent to enable other persons to download or otherwise copy, or have access to, the infringing item.

2. Determination of Infringement Amount. §8212; This note applies to the determination of the infringement amount for purposes of subsection (b)(1).

(A) Use of Retail Value of Infringed Item. §8212; The infringement amount is the retail value of the infringed item, multiplied by the number of infringing items, in a case involving any of the following:

(i) The infringing item (I) is, or appears to a reasonably informed purchaser to be, identical or substantially equivalent to the infringed item; or (II) is a digital or electronic reproduction of the infringed item.

(ii) The retail price of the infringing item is not less than 75% of the retail price of the infringed item.

(iii) The retail value of the infringing item is difficult or impossible to determine without unduly complicating or prolonging the sentencing proceeding.

(iv) The offense involves the illegal interception of a satellite cable transmission in violation of 18 U.S.C. § 2511. (In a case involving such an offense, the "retail value of the infringed item" is the price the user of the transmission would have paid to lawfully receive that transmission, and the "infringed item" is the satellite transmission rather than the intercepting device.)

(v) The retail value of the infringed item provides a more accurate assessment of the pecuniary harm to the copyright or trademark owner than does the retail value of the infringing item.

(B) Use of Retail Value of Infringing Item §8212; The infringement amount is the retail value of the infringing item, multiplied by the number of infringing items, in any case not covered by subdivision (A) of this Application Note, including a case involving the unlawful recording of a musical performance in violation of 18 U.S.C. § 2319A.

(C) Retail Value Defined. §8212; For purposes of this Application Note, the "retail value" of an infringed item or an infringing item is the retail price of that item in the market in which it is sold.

(D) Determination of Infringement Amount in Cases Involving a Variety of Infringing Items. §8212; In a case involving a variety of infringing items, the infringement amount is the sum of all calculations made for those items under subdivisions (A) and (B) of this Application Note. For example, if the defendant sold both counterfeit videotapes that are identical in quality to the infringed videotapes and obviously inferior counterfeit handbags, the infringement amount, for purposes of subsection

(b)(1), is the sum of the infringement amount calculated with respect to the counterfeit videotapes under subdivision (A)(i) (i.e., the quantity of the infringing videotapes multiplied by the retail value of the infringed videotapes) and the infringement amount calculated with respect to the counterfeit handbags under subdivision (B) (i.e., the quantity of the infringing handbags multiplied by the retail value of the infringing handbags).

3. Uploading. §8212; *With respect to uploading, subsection (b)(2) applies only to uploading with the intent to enable other persons to download or otherwise copy, or have access to, the infringing item. For example, this subsection applies in the case of illegally uploading copyrighted software to an Internet site, but it does not apply in the case of downloading or installing that software on a hard drive on the defendant's personal computer.*

4. Application of §3B1.3. §8212; *If the defendant de-encrypted or otherwise circumvented a technological security measure to gain initial access to an infringed item, an adjustment under §3B1.3 (Abuse of Position of Trust or Use of Special Skill) shall apply.*

5. Upward Departure Considerations. §8212; *If the offense level determined under this guideline substantially understates the seriousness of the offense, 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 may be warranted:*

(A) *The offense involved substantial harm to the reputation of the copyright or trademark owner.*

(B) *The offense was committed in connection with, or in furtherance of, the criminal activities of a national, or international, organized criminal enterprise.*

Background: This guideline treats copyright and trademark violations much like theft and fraud. Similar to the sentences for theft and fraud offenses, the sentences for defendants convicted of intellectual property offenses should reflect the nature and magnitude of the pecuniary harm caused by their crimes.

Accordingly, similar to the loss enhancement in the theft and fraud guideline, the infringement amount in subsection (b)(1) serves as a principal factor in determining the offense level for intellectual property offenses.

Subsection (b)(1) implements section 2(g) of the No Electronic Theft (NET) Act of 1997, Pub. L. 105-147, by using the retail value of the infringed item, multiplied by the number of infringing items, to determine the pecuniary harm for cases in which use of the retail value of the infringed item is a reasonable estimate of that harm. For cases referred to in Application Note 2(B), the Commission determined that use of the retail value of the infringed item would overstate the pecuniary harm or otherwise be inappropriate. In these types of cases, use of the retail value of the

infringing item, multiplied by the number of those items, is a more reasonable estimate of the resulting pecuniary harm.

Section 2511 of title 18, United States Code, as amended by the Electronic Communications Act of 1986, prohibits the interception of satellite transmission for purposes of direct or indirect commercial advantage or private financial gain. Such violations are similar to copyright offenses and are therefore covered by this guideline.