0.01 INSTRUCTIONS BEFORE VOIR DIRE

Members of the Jury Panel, if you have a cell phone, PDA, Blackberry, Smartphone, I-phone and any other wireless communication device with you, please ~~pull~~ take it out now and turn it off. Do not turn it to vibration or silent; power it down. [During jury selection, you must leave it off.] (Pause for thirty seconds to allow them to comply, then tell them the following:)

If you are selected as a juror, ~~you must leave your cell phone, including all wireless communication devices, in the jury room during the trial. You may use them during any breaks; however, you are not allowed to have cell phones in the jury room during your deliberations. You may give the cell phone to the [bailiff] [deputy clerk] for safekeeping just before you start to deliberate. It will be returned to you when your deliberations are complete or you are excused as a juror.~~ (briefly advise jurors of your court's rules concerning cellphones, cameras and any recording devices).

I understand you may ~~desire~~ want to tell your family~~,~~ and friends, ~~teachers, coworkers, and employer~~ and other people about your participation in this trial so that you can explain when you are required to be in court, and ~~can~~ you should warn them not to ask you about this case, tell you anything they know or think they know about ~~this case,~~ it, or discuss this case in your presence. ~~However, y~~ You must not communicate with anyone about the parties, witnesses, participants, [claims] [charges], evidence, or anything else related to this case, or tell anyone anything about the jury's deliberations in this case until after I accept your verdict or until I give you specific permission to do so. If you discuss the case with someone other than the other jurors during deliberations, you may be influenced in your verdict by their opinions. That would not be fair to the parties and it ~~may~~ would result in a verdict that is not based on the evidence and the law.

~~During the trial, w~~ While you are in the courthouse and ~~after you leave for the day,~~ until you are discharged in this case, do not provide any information to anyone by any means about this case. Thus, for example, do not talk face-to-face or use any electronic device or media, such as the telephone, a cell or smart phone, Blackberry, PDA, computer, the Internet, any Internet service, any text or instant messaging service, any Internet chat room, blog, or Website such as

Facebook, MySpace, YouTube, or Twitter, or any other way to communicate to anyone any information about this case until I accept your verdict or until you have been excused as a juror.

Do not do any research -- on the Internet, in libraries, in the newspapers, or in any other way -- or make any investigation about this case on your own. Do not visit or view any place discussed in this case and do not use Internet programs or other device to search for or to view any place discussed in the testimony. Also, do not research any information about this case, the law, or the people involved, including the parties, the witnesses, the lawyers, or the judge until you have been excused as jurors.

The parties have a right to have this case decided only on evidence they know about and that has been presented here in court. If you do some research or investigation or experiment that we don't know about, then your verdict may be influenced by inaccurate, incomplete or misleading information that has not been tested by the trial process, including the oath to tell the truth and by cross-examination. ~~All~~ Each of the parties ~~are~~ is entitled to a fair trial, rendered by an impartial jury, and you must conduct yourself so as to maintain the integrity of the trial process. If you decide a case based on information not presented in court, you will have denied the parties a fair trial in accordance with the rules of this country and you will have done an injustice. It is very important that you abide by these rules. Failure to follow these instructions ~~may~~ could result in the case having to be retried.

~~Do any of you feel like you~~ [Are there any of you who cannot or will not abide by these rules concerning communication with others in any way, shape or form during this trial?] (And then continue with other voir dire.)

0.02. INSTRUCTIONS AT END OF VOIR DIRE

During this recess, and every other recess, do not discuss this case among yourselves or with anyone else, including your family and friends. Do not allow anyone to discuss the case with you or within your hearing. "Do not discuss" also means do not e-mail, send text messages, blog or engage in any other form of written, oral or electronic communication, as I instructed you before.

Do not read any newspaper or other written account, watch any televised account, or listen to any radio program on the subject of this trial. Do not conduct any Internet research or consult with any other sources about this case, the people involved in the case, or its general subject matter. You must keep your mind open and free of outside information. Only in this way will you be able to decide the case fairly based solely on the evidence and my instructions on the law. If you decide this case on anything else, you will have done an injustice. It is very important that you follow these instructions.

I may not repeat these things to you before every recess, but keep them in mind ~~throughout the trial.~~ until you are discharged.

1.01. GENERAL: NATURE OF CASE; NATURE OF INDICTMENT; BURDEN OF PROOF; PRESUMPTION OF INNOCENCE; DUTY OF JURY; CAUTIONARY

Ladies and gentlemen: I shall take a few moments now to give you some initial instructions about this case and about your duties as jurors. At the end of the trial I shall give you further instructions. I may also give you instructions during the trial. Unless I specifically tell you otherwise, all such instructions - both those I give you now and those I give you later - are equally binding on you and must be followed.

[Describe your court's policy, such as "You must leave your cell phone, PDA, Blackberry, Smartphone, I-phone and any other wireless communication devices in the jury room during the trial and may only use them during breaks. However, you are not allowed to have cell phones in the jury room during your deliberations. You may give the cell phone to the [bailiff] [deputy clerk] for safekeeping just before you start to deliberate. It will be returned to you when your deliberations are complete."]

This is a criminal case, brought against the defendant[s] by the United States Government. The defendant[s] [is] [are] charged with _____.[1] [That charge is] [Those charges are] set forth in what is called an indictment[,] [which reads as follows: (insert)] [which I will summarize as follows: (insert)] [which I will ask the government attorney to summarize for you].[2] You should understand that an indictment is simply an accusation. It is not evidence of anything. The defendant[s] [has] [have] pleaded not guilty, and [is] [are] presumed to be innocent unless and until proved guilty beyond a reasonable doubt.[3]

It will be your duty to decide from the evidence whether [the] [each] defendant is guilty or not guilty of the crime[s] charged. From the evidence, you will decide what the facts are. You are entitled to consider that evidence in the light of your own observations and experiences in the affairs of life. You may use reason and common sense to draw deductions or conclusions from facts which have been established by the evidence. You will then apply those facts to the law which I give you in these and in my other instructions, and in that way reach your verdict. You are the sole judges of the facts; but you must follow the law as stated in my instructions, whether you agree with it or not.

Do not allow sympathy or prejudice to influence you. The law demands of you a just verdict, unaffected by anything except the evidence, your common sense, and the law as I give it to you.

You should not take anything I may say or do during the trial as indicating what I think of the evidence or what I think your verdict should be.

Finally, please remember that only [this defendant] [these defendants], not anyone else, [is] [are] on trial here, and that [this defendant] [these defendants] [is] [are] on trial only for the crime[s] charged, not for anything else.

Notes on Use

1. The description of the offense should not track statutory language, but rather should be a simple, general statement (e.g., "unlawfully importing cocaine;" "embezzling bank funds"). Statutory citations are unnecessary.

2. Depending on the length and complexity of the indictment and the individual practices of each district judge, the indictment may be read, summarized by the court, summarized by the prosecutor or not read or summarized, depending on what is necessary to assist the jury in understanding the issues before it.

3. A brief summary of the defense may be included here if requested by the defendant.

Committee Comments

See Introductory Comment, Section 1.00, *supra*.

1.08. CONDUCT OF THE JURY

~~Finally, t~~To insure fairness, you as jurors must obey the following rules:

First, do not talk among yourselves about this case, or about anyone involved with it, until the end of the case when you go to the jury room to decide on your verdict.

Second, do not talk with anyone else about this case, or about anyone involved with it, until the trial has ended and you have been discharged as jurors.

Third, when you are outside the courtroom do not let anyone tell you anything about the case, or about anyone involved with it [until the trial has ended and your verdict has been accepted by me]. If someone should try to talk to you about the case [during the trial], please report it to ~~me.~~ the [bailiff] [deputy clerk]. (Describe person.)

Fourth, during the trial you should not talk with or speak to any of the parties, lawyers or witnesses involved in this case -- you should not even pass the time of day with any of them. It is important not only that you do justice in this case, but that you also give the appearance of doing justice. If a person from one side of the lawsuit sees you talking to a person from the other side -- even if it is simply to pass the time of day -- an unwarranted and unnecessary suspicion about your fairness might be aroused. If any lawyer, party or witness does not speak to you when you pass in the hall, ride the elevator or the like, it is because they are not supposed to talk to or visit with you.

Fifth, it may be necessary for you to tell your family, friends, teachers, coworkers, or employer about your participation in this trial. You can explain when you are required to be in court and can warn them not to ask you about this case, tell you anything they know or think they know about this case, or discuss this case in your presence. You must not communicate with anyone or post information about the parties, witnesses, participants, [claims] [charges], evidence, or anything else related to this case. You must not tell anyone anything about the jury's deliberations in this case until after I accept your verdict or until I give you specific permission to do so. If you discuss the case with someone other than the other jurors during deliberations, it could create the perception that you have clearly decided the case or that you may be influenced in your verdict by their opinions. That would not be fair to the parties and it may result in the verdict being thrown out and the case having to be retried. During the trial,

while you are in the courthouse and after you leave for the day, do not provide any information to anyone by any means about this case. Thus, for example, do not talk face-to-face or use any electronic device or media, such as the telephone, a cell or smart phone, Blackberry, PDA, computer, the Internet, any Internet service, any text or instant messaging service, any Internet chat room, blog, or Website such as Facebook, MySpace, YouTube, or Twitter, or any other way to communicate to anyone any information about this case until I accept your verdict.

Sixth, do not do any research -- on the Internet, in libraries, in the newspapers, or in any other way -- or make any investigation about this case on your own. Do not visit or view any place discussed in this case and do not use Internet programs or other device to search for or to view any place discussed in the testimony. Also, do not research any information about this case, the law, or the people involved, including the parties, the witnesses, the lawyers, or the judge.

Seventh, do not read any news stories or articles in print, or on the Internet, or in any blog, about the case, or about anyone involved with it, or listen to any radio or television reports about the case or about anyone involved with it. [In fact, until the trial is over, I suggest that you avoid reading any newspapers or news journals at all, and avoid listening to any television or radio newscasts at all. I do not know whether there might be any news reports of this case, but if there are, you might inadvertently find yourself reading or listening to something before you could do anything about it. If you want, you can have your spouse or a friend clip out any stories and set them aside to give you after the trial is over.] ~~It is important for you to understand that this case must be decided by the evidence presented in the case and the instructions I give you]~~[1]I can assure you, however, that by the time you have heard the evidence in this case, you will know what you need to return a just verdict.

~~*Sixth*, do not do any research or make any investigation on your own about any matter involved in this case. By way of examples, that means you must not read from a dictionary or a text book or an encyclopedia or talk with a person you consider knowledgeable or go to the Internet for information about some issue in this case. In fairness, learn about this case from the evidence you receive here at the trial and apply it to the law as I give it to you..~~

The parties have a right to have the case decided only on evidence they know about and that has been introduced here in court. If you do some research or investigation or experiment

that we don't know about, then your verdict may be influenced by inaccurate, incomplete or misleading information that has not been tested by the trial process, including the oath to tell the truth and by cross-examination. All of the parties are entitled to a fair trial, rendered by an impartial jury, and you must conduct yourself so as to maintain the integrity of the trial process. If you decide a case based on information not presented in court, you will have denied the parties a fair trial in accordance with the rules of this country and you will have done an injustice. It is very important that you abide by these rules. [Failure to follow these instructions may result in the case having to be retried and could result in you being held in contempt.]

Seventh Eighth, do not make up your mind during the trial about what the verdict should be. Keep an open mind until after you have gone to the jury room to decide the case and you and your fellow jurors have discussed the evidence.

~~**Notes on Use**~~

~~1. Optional for those cases in which media coverage is expected.~~

~~**Committee Comments**~~

~~*See* Pattern Criminal Jury Instructions for the District Courts of the First Circuit § 1.07 (1998); Pattern Criminal Federal Jury Instructions for the Seventh Circuit § 1.01 (1998); Ninth Instr. Circuit Criminal Jury Instructions § 1.9 (2000); 1A Kevin F. O'Malley, et al., *Federal Jury Practice and Instructions*: Criminal §§ 11.01 and 11.02 (5th ed. 2000); Federal Judicial Center, Pattern Criminal Jury Instructions § 1 (1988).~~

~~A similar instruction should be repeated before the first recess, and as needed before other recesses (for example, before a weekend recess). *See* Instruction 2.01, *infra*, for a form of instruction before recesses. *See also* Committee Comments, Instruction 2.01, *infra*, regarding the necessity of instructions relating to recesses.~~

2.01. DUTIES OF JURY - RECESSES [†]

~~We are about to take [our first] [a] recess[2] and I remind you of the instruction I gave you earlier. During this recess or any other recess, you must not discuss this case with anyone, including the other jurors, members of your family, people involved in the trial, or anyone else. If anyone tries to talk to you about the case, please let me know about it immediately. [Do not read, watch or listen to any news reports of the trial. Finally, keep an open mind until all the evidence has been received and you have heard the views of your fellow jurors.~~ During this recess, and every other recess, do not discuss this case among yourselves or with anyone else, including your family and friends. Do not allow anyone to discuss the case with you or within your hearing. "Do not discuss" also means do not e-mail, send text messages, blog or engage in any other form of written, oral or electronic communication, as I instructed you before.

Do not read any newspaper or other written account, watch any televised account, or listen to any radio program about this trial. Do not conduct any Internet research or consult with any other sources about this case, the people involved in the case, or its general subject matter. You must keep your mind open and free of outside information. Only in this way will you be able to decide the case fairly based solely on the evidence and my instructions on the law. If you decide this case on anything else, you will have done an injustice. It is very important that you follow these instructions.

I may not repeat these things to you before every recess, but keep them in mind throughout the trial.~~]~~[1]

Notes on Use

1. ~~This instruction should be given before the first recess and at subsequent recesses within the discretion of the court.~~ This language should be used for overnight and weekend recesses, but may be omitted for subsequent breaks during trial.

~~2. This language should be modified for overnight or weekend recesses.~~

~~Committee Comments~~

~~*See* Instruction 1.08, *supra*.~~

~~The court has considerable discretion to separate a jury before it has reached a verdict. *United States v. Dixon*, 913 F.2d 1305, 1312 (8th Cir. 1990) (distinguishing separation of jury prior to and after deliberations). However, the jury must be admonished as to their duties and~~

responsibilities when not in court. Such an instruction may be given at the beginning of trial, before recesses and lunchtime, and most importantly before separating for the evening. *Id.* *United States v. Williams*, 635 F.2d 744, 745 (8th Cir. 1990). Although failure to give any instruction of this nature during the course of a trial which was completed in one day has been held harmless error, *Morrow v. United States*, 408 F.2d 1390 (8th Cir. 1969), it is prejudicial error to fail to give a cautionary instruction at any stage of the trial prior to separation. *See United States v. Williams*, 635 F.2d at 746; *cf.*, *United States v. Lashley*, 251 F.3d 706, 712 (8th Cir. 2001). The jurors mistakenly left early during deliberations. The court held it was not reversible error for the trial judge to contact the jurors by telephone and admonish them not to speak to anyone about the case, where such admonition had been given during trial. However, the failure to give a cautionary instruction prior to an overnight separation was held not reversible error, absent any other claim of prejudice where the jury had been so cautioned on at least thirteen other occasions. *United States v. Weatherd*, 699 F.2d 959, 962 (8th Cir. 1983). *See also United States v. McGrane*, 746 F.2d 632 (8th Cir. 1984), holding that the jury was adequately cautioned when they were so instructed on ten occasions.

6.18.04 MISPRISION OF A FELONY (18 U.S.C. § 4)

The crime of misprision of a felony, as charged in [Count _____ of] the indictment, has four elements, which are:

One, (insert name of person other than the defendant) committed the crime of (insert description of felony offense);

Two, the defendant had full knowledge of that fact;

Three, the defendant failed to notify authorities that the crime had been committed; and

Four, the defendant took an affirmative step to conceal the crime.

(Insert paragraph describing Government's burden of proof; *see* Instruction 3.09, *supra*.)

Notes on Use

1. The defendant must commit some affirmative act to prevent discovery of the earlier felony. Mere failure to make the crime known will not suffice. *Neal v. United States*, 102 F.2d 643, 649 (8th Cir. 1939); *United States v. Adams*, 961 F.2d 505, 508 (5th Cir. 1992); *Lancey v. United States*, 356 F.2d 407, 410 (9th Cir. 1966) (mere silence without an affirmative act of concealment is insufficient to establish commission of the offense).

Committee Comments

Some recent cases suggest that the four elements of the offense can be collapsed into three: (1) the defendant knew that another person had committed the alleged felony; (2) the defendant failed to notify authorities; and (3) the defendant took an affirmative step to conceal the crime. *See, e.g., United States v. Adams*, 961 F.2d at 508. The Eighth Circuit follows the more traditional formulation with four elements. *Neal v. United States*, 102 F.2d at 646; *see also United States v. Cefalu*, 85 F.3d 964, 969 (2d Cir. 1996), *United States v. Baez*, 732 F.2d 780, 782 (10th Cir. 1984), and *United States v. Ciambrone*, 750 F.2d 1416, 1417 (9th Cir. 1984).

It is irrelevant whether at the time of concealment the authorities had knowledge of either the felony crime or the identity of the perpetrator. *Lancey v. United States*, 356 F.2d at 409 (recognizing *Neal v. United States*, 102 F.2d 643 (8th Cir. 1939), as the leading case on the subject).

The crime of misprision typically does not apply to those who participate in the commission of an offense. *United States v. Bolden*, 368 F.3d 1032, 1036-37 (8th Cir. 2004). Subject to Fifth Amendment concerns, however, the misprision statute can be applied to those who participate in the underlying criminal activity. *Roberts v. United States*, 445 U.S. 552, 558 (1980). The valid assertion of a Fifth Amendment privilege against self-incrimination would prevent a misprision prosecution for concealing evidence of one's own crime. *United States v. Caraballo-Rodriquez*, 480 F.3d 62, 72 (1st Cir. 2007) (citing *United States v. Suh*, 541 F.2d 672, 677 (7th Cir. 1976) ("if the duty to notify federal authorities is precluded by constitutional privilege, it is difficult to understand how a conviction [under 18 U.S.C. § 4] could be

substantiated")). Similarly, a common law privilege, such as that between an attorney and a client or between a doctor and patient, may excuse or justify the non-disclosure on the grounds of privilege. *United States v. Caraballo-Rodriquez*, 480 F.3d at 72.

Deciding what constitutes concealment is a question of fact for the jury. "Concealment of crime has been condemned throughout our history. The citizen's duty to 'raise the hue and cry' and report felonies to the authorities was an established tenet of Anglo-Saxon law at least as early as the 13th century. Although the term 'misprision of felony' now has an archaic ring, gross indifference to the duty to report known criminal behavior remains a badge of irresponsible citizenship." *Roberts v. United States*, 445 U.S. at 558. Disclosing only part but not all of what is known about the crime, or "throwing dust in the eyes" of investigators and thereby providing them with misleading information, qualifies as concealment. *Neal v. United States*, 102 F.2d at 649. Similarly, providing authorities with the false impression that the felony crime had not occurred satisfies the concealment requirement. *Patel v. Mukasey*, 526 F.3d 800, 803 (5th Cir. 2008). Harboring a perpetrator, with full knowledge that they committed a felony crime, can constitute concealment. *Lancey v. United States*, 356 F.2d at 410. The Eighth Circuit has discussed what constitutes "concealment" in the context of a related statute which makes it a crime to harbor or conceal a person for whom an arrest warrant or other process has been issued. *United States v. Hayes*, 518 F.3d 989, 993-95 (8th Cir. 2008) (construing 18 U.S.C. § 1071).

The language of the statute requires the one with actual knowledge that another has committed a felony to come forward and reveal that knowledge "as soon as possible." The cases have interpreted "as soon as possible" to mean when there is an opportunity to do so. *Lancey v. United States*, 356 F.2d at 411 (recognizing that one held captive by a perpetrator does not have an opportunity to notify authorities). Whether a defendant charged with misprision came forward "as soon as possible" is a question of fact for the jury to resolve and may require the trial court to modify element three to accommodate the facts unique to an individual case. Fear of the perpetrator, without more, does not excuse the failure to notify authorities. *Id.* (recognizing that if fear of the perpetrator were a defense, there seldom could be a misprision conviction).

6.18.1014. FALSE STATEMENT TO A FINANCIAL INSTITUTION (18 U.S.C. § 1014)

The crime of making a false statement to a financial institution,[1] as charged in [Count _____ of] the indictment, has three elements, which are:[2]

One, the defendant knowingly made a false statement (describe the alleged false statement, *e.g.*, that the defendant had no current indebtedness to another financial institution) to (name of financial institution);

Two, the defendant made the false statement for the purpose of influencing the action of (name of financial institution) upon (describe transaction, *e.g.*, an application for a loan);

Three, that (name of financial institution) was (describe federal relation, e.g., insured by the FDIC) at the time the statement was made.[3]

A statement is "false" if untrue when made.

(Insert paragraph describing Government's burden of proof; *see* Instruction 3.09, *supra*.)

Notes on Use

1. "Financial institution" is defined in 18 U.S.C. § 20 to include businesses other than banks, *e.g.*, the Federal Housing Administration, the Federal Crop Insurance Corp., the Federal Reserve Bank, the Small Business Administration, federal credit unions, and mortgage lending businesses that make federally-related mortgage loans. If the fraud was against a financial institution other than a bank, this phrase should be modified accordingly throughout the instruction.

2. Materiality is not an element of section 1014. *United States v. Wells*, 519 U.S. 482 (1997). "[A]ny reference to materiality in the jury instruction is unnecessary and has the potential to cause confusion." *United States v. Wells*, 127 F.3d 739, 744 (1997) (on remand).

3. Proof of federal relation is required. *United States v. Carlisle*, 118 F.3d 1271, 1274 (8th Cir. 1997); *United States v. Chandler*, 66 F.3d 1460, 1466 (8th Cir. 1995) (quoting United States v. White, 882 F.2d 250, 253-54 (7th Cir. 1989)).

Committee Comments

Reliance is not an element of a section 1014 violation. It is not necessary to prove that the financial institution was influenced by or actually relied on the false statement. *United States v. Copple*, 827 F.2d 1182, 1187 (8th Cir. 1987); *United States v. Huntress*, 956 F.2d 1309, 1317 (5th Cir. 1992). Materiality, likewise, is not an element of section 1014. *United States v. Wells*, 519 U.S. 482 (1997).

Multiple false statements in a single document constitutes only one violation of section 1014. *United States v. Sue*, 586 F.2d 70 (8th Cir. 1978).

6.18.1030A. COMPUTER FRAUD [OBTAINING NATIONAL SECURITY INFORMATION] (18 U.S.C. § 1030(a)(1))

The crime of accessing a computer to obtain national security information, as charged in [Count __] of the indictment, has four essential elements, which are:[1]

One, the defendant knowingly accessed a computer [without authorization][2] [exceeding authorized access][3];

Two, the defendant obtained information[4] that [has been determined by the United States government by [Executive Order] [statute] to require protection against unauthorized disclosure for reasons of [national defense] [foreign relations]] [was restricted data[5] regarding the design, manufacture or use of atomic weapons];

Three, the defendant had reason to believe that the information obtained could be used to the injury of the United States or to the advantage of any foreign nation;[6] and

Four, the defendant [[voluntarily and intentionally] [attempted to] [communicate[d]] [deliver[ed]] [transmit[ted]] the information to a person[7] not entitled to receive it] [voluntarily and intentionally retained the information and failed to deliver the information to the [officer] [employee] of the United States entitled to receive the information].[8]

The Government is not required to prove that the information obtained by the defendant was in fact used to the injury of the United States or to the advantage of any foreign nation.

[You are further instructed regarding the crime[s] charged in [Count[s] ____ of] the indictment that the following definitions apply: (Insert applicable portions of Instruction 6.18.1030H, unless the indictment charges multiple computer fraud violations and there will be no confusion in adding the definitions common to all counts after all of the substantive computer fraud instructions).][9]

(Insert paragraph describing Government's burden of proof; *see* Instruction 3.09, *supra*.)

Notes on Use

1. If an attempt to commit an offense under this subsection has been charged, *see* 18 U.S.C. § 1030(b), the instruction should be modified accordingly.

2. "Without authorization" is not defined in section 1030 but is commonly understood to refer to persons who have no permission or authority to do a thing whatsoever. *Condux Intern., Inc. v. Haugum*, 2008 WL 5244818 at *4 (D. Minn. Dec. 15, 2008) (citations omitted).

3. Although Congress did not squarely address the issue in the legislative history of section 1030, the Committee is of the opinion that the term "knowingly" modifies the term "accessed" as well as the phrases "without authorization" or "exceeding authorization." In other words, the Government must prove both that the defendant knew he or she was accessing a computer and that he or she knew that the access was without authorization or exceeding authorization. *See Flores-Figueroa v. United States*, __ U.S. __, 129 S. Ct. 1886, 1891 (2009) (citing *United States v. X-Citement Video, Inc.*, 513 U.S. 64, 79 (1994) (Stevens, J., concurring), and noting that courts ordinarily interpret the word "knowingly" in a criminal statute as applying to all subsequently listed elements, not just the verbs). *Compare* Committee Comments to Instruction 6.18.1030B (discussing the 1986 amendments to subsection 1030(a)(2) in which Congress changed the scienter requirement from "knowingly" to "intentionally" to clarify that it intended to criminalize those who clearly intended to enter computer files without proper authorization rather than those who inadvertently stumbled upon those files).

4. If desired, the court may instruct the jury that the phrase "obtained information" includes the mere observation of the data and does not require the Government to prove the data was removed from its original location or transcribed. *See* S. Rep. 99-432 at 6-7 (1986), *reprinted in* U.S.C.C.A.N. 2479, 2484 and *available at* 1986 WL 31918. In later amendments to other subsections of section 1030, Congress further clarified that the phrase "'obtaining information' includes merely reading the information. There is no requirement that the information be copied or transported." S. Rep. 104-357, 2d Sess. 8 (1996), *available at* 1996 WL 492169. The term "information" includes information stored in intangible form. *See* S. Rep. No. 357, 104th Cong., 2d Sess. 8 (1996).

5. The phrase "restricted data" means all data concerning the: (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, not declassified or removed pursuant to federal law. 18 U.S.C. § 1030(a)(1) (adopting the definition of restricted data set forth in the Atomic Energy Act, 42 U.S.C. § 2014(y)).

6. The phrase, "to the injury of the United States or to the advantage of any foreign nation," is not defined in section 1030. A similar phrase is used in espionage statutes. *See, e.g.*, 18 U.S.C. §§ 793, 794, 798. With regard to a predecessor espionage statute containing a similar phrase, the Espionage Act of 1917, the Supreme Court clarified that the meaning of this phrase turns on the defendant's intent and whether information at issue was in fact protected by the Government: "This [language] requires those prosecuted to have acted in bad faith. The sanctions apply only when scienter is established. Where there is no occasion for secrecy, as with reports relating to national defense, published by authority of Congress or the military departments, there can, of course, in all likelihood be no reasonable intent to give an advantage to a foreign government." *Gorin v. United States*, 312 U.S. 19, 28 (1941).

7. If a definition of "person" is desired, *see* 18 U.S.C. § 1030(e)(12).

8. The statute uses the term "willfully," but consistent with Committee Comments to Instruction 7.02, that term has been replaced with the words "voluntarily and intentionally."

9. The supplemental definitions contained in Instruction 6.18.1030H, *infra*, should be given in most cases where applicable.

Committee Comments

In 1996, Congress changed the scienter element of section 1030(a)(1) to track the scienter requirement of 18 U.S.C. § 793(e), a statute which prohibits gathering, transmitting or losing defense information. The Senate Committee stated,

> Although there is considerable overlap between 18 U.S.C. § 793(e) and section 1030(a)(1) . . . the two statutes would not reach exactly the same conduct. Section 1030(a)(1) would target those persons who deliberately break into a computer to obtain properly classified Government secrets and then try to peddle those secrets to others, including foreign governments. In other words, unlike existing espionage laws prohibiting the theft and peddling of Government secrets to foreign agents, section 1030(a)(1) would require proof that the individual knowingly used a computer without authority, for the purpose of obtaining classified information. In this sense then, it is the use of the computer which is being proscribed, not the unauthorized possession of, access to, or control over the classified information itself.

S. Rep. No. 357, 104th Cong., 2d Sess. 7, *available at* 1996 WL 492169 at * 16 (1996). Note, however, that section 1030(a)(1) can be violated even if the defendant has not delivered the information to a third party, such as if the defendant voluntarily and intentionally retained the information and failed to deliver it to the appropriate U.S. official.

6.18.1030B. COMPUTER FRAUD [OBTAINING CONFIDENTIAL INFORMATION] (18 U.S.C. § 1030(a)(2))

The crime of computer fraud to obtain confidential information, as charged in [Count __] of the indictment, has two essential elements, which are:[1]

One, the defendant intentionally accessed a computer [without authorization][2] [exceeding authorized access], and

Two, the defendant obtained information[3] [contained in a financial record of [a financial institution] [an issuer of a credit card][;] [contained in a file of a consumer reporting agency[4] on a consumer][;] [from any [legislative] [judicial] [executive] [department][5] [agency] of the United States][;] [or] [from any protected computer].

[You are further instructed regarding the crime[s] charged in [Count[s] ____ of] the indictment that the following definitions apply: (Insert applicable portions of Instruction 6.18.1030H, unless the indictment charges multiple computer fraud violations and there will be no confusion in adding the definitions common to all counts after all of the substantive computer fraud instructions).][6]

If you find these two elements unanimously and beyond a reasonable doubt, then you must find the defendant guilty of this crime [under Count __]. Record your determination on the Verdict Form which will be submitted to you with these instructions.

[If you find these two elements unanimously beyond a reasonable doubt, you must also unanimously decide whether the defendant: [acted for purposes of commercial advantage or private financial gain][;] [or] [acted in furtherance of (describe crime or tort)][7] [or] [obtained information having a value exceeding $5,000.00].[8] Record your determination on the Verdict Form.]

(Instruction 3.09, *supra*, which describes the Government's burden of proof, has already been incorporated in this instruction and should not be repeated.)

Notes on Use

1. If an attempt to commit an offense under this subsection has been charged, *see* 18 U.S.C. § 1030(b), the instruction should be modified accordingly.

2. "Without authorization" is not defined in section 1030 but is commonly understood to refer to persons who have no permission or authority to do a thing whatsoever. *Condux Intern., Inc. v. Haugum*, 2008 WL 5244818 at *4 (D. Minn. Dec. 15, 2008) (citations omitted).

3. If desired, the court may instruct the jury that the phrase "obtained information" "includes merely reading the information. There is no requirement that the information be copied or transported." S. Rep. 357, 104th Cong., 2d Sess. 8 (1996), *available at* 1996 WL 492169. In earlier amendments addressing other subsections of section 1030, Congress has also stated that the phrase "obtained information" includes the mere observation of the data and does not require the Government to prove the data was removed from its original location or transcribed. *See* S. Rep. 99-432 at 6-7 (1986), *reprinted in* U.S.C.C.A.N. 2479, 2484 *and available at* 1986 WL 31918. The term "information" includes information stored in intangible form. *See* S. Rep. No. 357, 104th Cong., 2d Sess. 8 (1996).

4. If a definition of "consumer reporting agency"is desired, *see* 18 U.S.C. § 1030(a)(2)(A) and 15 U.S.C. § 1681 *et seq*.

5. If a definition of the "department of the United States" is desired, *see* 18 U.S.C. § 1030(e)(7). If this subsection is applicable, the instruction should set forth the particular executive department enumerated in 5 U.S.C. § 101 and charged in the indictment.

6. The supplemental definitions contained in Instruction 6.18.1030H, *infra*, should be given in most cases where applicable.

7. The applicable penalty provision, section 1030(c)(B)(ii), provides that if "the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State," the defendant will face imprisonment for not more than five years and/or a fine under Title 18. If this provision is applicable, the court should make a preliminary finding on the record regarding whether the alleged offense was committed in furtherance of a criminal or tortious act that violates the Constitution or any law.

8. Any fact (other than a prior conviction) that increases the maximum penalty for a crime must be charged in the indictment, submitted to the jury, and proven beyond a reasonable doubt. *Apprendi v. New Jersey*, 530 U.S. 466 (2000). Typically, the indictment will not include these aggravating facts if the Government has charged a first-time offender of section 1030 solely with a misdemeanor, *see* 18 U.S.C. §1030(c)(2)(A), or if it has charged a felony offense that allegedly occurred after a conviction for another offense under section 1030. *See* 18 U.S.C. § 1030(c)(2)(C). However, if any of the additional aggravating facts set forth in the statute have been charged in the indictment, these facts should be submitted to the jury either as a formal element and/or by special interrogatory. 18 U.S.C. §§ 1030(c)(2)(B); *see* 6.18.1030B(a) for a verdict form with special interrogatories. In the Committee's view, a verdict form with special interrogatories is the preferred method for presenting these aggravating factors to the jury because it is less likely to result in confusion and because it creates a clear record of the basis for the jury's verdict.

Committee Comments

In 1986, Congress amended subsection 1030(a)(2) to change the scienter requirement from "knowingly" to "intentionally." In so doing, it made clear that element one requires the Government to prove not only that the defendant intentionally accessed a computer, but also that he or she knew that the access was without authorization or exceeding authorized access. Specifically, Congress expressed concern that the "knowingly" standard "might not be sufficient to preclude liability on the part of those who inadvertently 'stumble into' someone else's computer file or computer data. This is particularly true in those cases where an individual is authorized to sign onto and use a particular computer, but subsequently exceeds his authorized access by mistakenly entering another computer file or data that happens to be accessible from the same terminal. Because the user had 'knowingly' signed onto that terminal in the first place, the danger exists that he might incur liability for his mistaken access to another file. This is so because, while he may not have desired that result, i.e., the access of another file, it is possible that a trier of fact will infer that the user was 'practically certain' such mistaken access could result from his initial decision to access the computer. The substitution of an 'intentional' standard is designed to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another. Again, this will comport with the Senate Report on the Criminal Code, which states that "'intentional' means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective.'" S. Rep. No. 99-432, at 6 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2484 (quoting another Senate report).

Because subsection 1030(a)(2) focuses on privacy protection, the statute may be violated by the mere viewing of information online even without any downloading or copying. *See* S. Rep. No. 99-432, at § I, *available at* 1986 W.L. 31918, 1986 U.S.C.C.A.N. 2484.

Violations of this subsection may be either a felony or a misdemeanor. "The crux of the offense under subsection 1030(a)(2)(C) . . . is the abuse of a computer to obtain the information. The seriousness of a breach in confidentiality depends, in considerable part, on the value of the information taken, or on what is planned for the information after it is obtained. Thus, the statutory penalties are structured to provide that obtaining information of minimal value is only a misdemeanor, but obtaining valuable information, or misusing information in other more serious ways, is a felony." S. Rep. No. 104-357, § IV(1)(E), *available at* 1996 W.L. 492169 at *7.

6.18.1030B(a) SPECIAL VERDICT FORM (INTERROGATORIES TO FOLLOW FINDING OF GUILT) (18 U.S.C. § 1030(a)(2))

We, the jury, find Defendant (name) _____

(guilty/not guilty)

of computer fraud to obtain confidential information [as charged in Count _____ of the indictment] [under Instruction No. _____].

If you find the defendant "guilty," you must answer the following question[s] and you must unanimously agree on the answer[s]:

[a. Did the defendant act for purposes of commercial advantage or private financial gain?

Yes ____ No ____]

[b. Did the defendant act in furtherance of (describe crime or tort)?

Yes ____ No ____]

[c. Did the defendant obtain information that had a value exceeding $5,000.00?

Yes ____ No ____]

_____
Foreperson

_____
Date

6.18.1030C(1). COMPUTER FRAUD [TRANSMISSION OF PROGRAM TO CAUSE DAMAGE TO A COMPUTER] (18 U.S.C. § 1030(a)(5)(A))

The crime of transmission of a program to cause damage to a computer, as charged in [Count __] of the indictment, has two essential elements, which are:[1]

One, the defendant knowingly caused the transmission of a [program] [information] [code] [command] to a protected computer,[2] and

Two, the defendant, as a result of such conduct, intentionally caused damage to a protected computer without authorization.[3]

[You are further instructed regarding the crime[s] charged in [Count[s] ____ of] the indictment that the following definitions apply: (Insert applicable portions of Instruction 6.18.1030H, unless the indictment charges multiple computer fraud violations and there will be no confusion in adding the definitions common to all counts after all of the substantive computer fraud instructions).][4]

If you find these two elements unanimously and beyond a reasonable doubt, then you must find the defendant guilty of this crime [under Count __]. Record your determination on the Verdict Form.

[If you find these two elements unanimously beyond a reasonable doubt, you must also unanimously decide whether as a result of such conduct, the defendant

- [caused loss to one or more persons[5] during any one-year period of an aggregate value of $5,000.00 or more][;]
- [caused loss resulting from a related course of conduct affecting one or more other protected computers of an aggregate value of $5,000.00 or more][;]
- [caused the [potential] [modification] [impairment] of the medical [examination] [diagnosis] [treatment] [care] of one or more individuals]
- [caused physical injury to any person][;]
- [caused a threat to public health or safety][;]
- [caused damage affecting a computer used [by] [for] a governmental entity (describe entity at issue),[6] in furtherance of [the administration of justice] [national defense] [national security]][;]

- [caused damage affecting ten or more protected computers during any one-year period]][;] [or]
- [[attempted to cause] [knowingly] [recklessly] [caused] [serious bodily injury] [death] from such conduct].[7] Record your determination on the Verdict Form.]

(Instruction 3.09, *supra*, which describes the Government's burden of proof, has already been incorporated in this instruction and should not be repeated.)

Notes on Use

1. If an attempt to commit an offense under this subsection has been charged, *see* 18 U.S.C. § 1030(b), the instruction should be modified accordingly.

2. Although Congress did not squarely address the issue in the legislative history of section 1030, the Committee is of the opinion that the term "knowingly" modifies the phrase "caused the transmission" as well as the phrase "protected computer." In other words, the Government must prove both that the defendant knew he or she was causing the transmission of a program, code, command, etc., and that he or she knew the transmission was to a protected computer. *See Flores-Figueroa v. United States*, __ U.S. __, 129 S. Ct. 1886, 1891 (2009) (citing *United States v. X-Citement Video, Inc.*, 513 U.S. 64, 79 (1994) (Stevens, J., concurring), and noting that courts ordinarily interpret the word "knowingly" in a criminal statute as applying to all subsequently listed elements, not just the verbs).

3. "Without authorization" is not defined in section 1030 but is commonly understood to refer to persons who have no permission or authority to do a thing whatsoever. *Condux Intern., Inc. v. Haugum*, 2008 WL 5244818 at *4 (D. Minn. Dec. 15, 2008) (citations omitted).

4. The supplemental definitions contained in Instruction 6.18.1030H, *infra*, should be given in most cases where applicable.

5. If a definition of "person" is desired, *see* 18 U.S.C. § 1030(e)(12).

6. If a definition of "governmental entity" is desired, *see* 18 U.S.C. § 1030(e)(9).

7. Any fact (other than a prior conviction) that increases the maximum penalty for a crime must be charged in the indictment, submitted to the jury, and proven beyond a reasonable doubt. *Apprendi v. New Jersey*, 530 U.S. 466 (2000). Typically, the indictment will not include these aggravating facts if the Government has charged a first-time offender of section 1030 solely with a misdemeanor, *see* 18 U.S.C. § 1030(c)(4)(G), or if it has charged a felony offense that allegedly occurred after a conviction for another offense under Section 1030. *See* 18 U.S.C. § 1030(c)(4)(C). However, if any of the additional aggravating facts set forth in the statute have been charged in the indictment, these facts should be submitted to the jury either as a formal element and/ or by special interrogatory. 18 U.S.C. §§ 1030(c)(4)(B), (E), and (F); *see* 6.18.1030C(1)(a) for a verdict form with special interrogatories. In the Committee's view, a verdict form with special interrogatories is the preferred method for presenting these aggravating

factors to the jury because it is less likely to result in confusion and because it creates a clear record of the basis for the jury's verdict.

Committee Comments

Subsection 1030(a)(5)(A) does not require the Government to prove the defendant accessed the protected computer. Some examples of conduct that would violate this subsection include the intentional release of certain viruses, worms and "trojan horses," as well as other forms of attacks on computer data. *See United States v. Trotter*, 478 F.3d 918, 919 (8th Cir. 2007)*; see also International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006).

For a discussion on the kind of proof deemed sufficient to establish the $5,000 aggregate loss amount, *see United States v. Millot*, 433 F.3d 1057, 1061 (8th Cir. 2006).

6.18.1030C(1)(a). SPECIAL VERDICT FORM (INTERROGATORIES TO FOLLOW FINDING OF GUILT) (18 U.S.C. § 1030(a)(5(A))

We, the jury, find Defendant (name) _____

(guilty/not guilty)

of computer fraud by transmission of a [program] [information][code] [command] to a protected computer [as charged in Count _____ of the indictment] [under Instruction No. _____].

If you find the defendant "guilty," you must answer the following question[s] and you must unanimously agree on the answer[s]:

As a result of such conduct,

[a._____ Did the defendant cause loss to one or more persons during any one year period of an aggregate value of $5,000.00 or more?

Yes ____ No ____]

[b. _____Did the defendant cause loss resulting from a related course of conduct affecting one or more other protected computers of an aggregate value of $5,000.00 or more?

Yes ____ No ____]

[c. _____Did the defendant cause the [potential] [modification][impairment] of the medical [examination][diagnosis][treatment][care] of one or more individuals?

Yes ____ No ____]

[d. _____Did the defendant cause physical injury to any person?

Yes ____ No ____]

[e. _____Did the defendant cause a threat to public health or safety?

Yes ____ No ____]

[f. _____ Did the defendant cause damage affecting a computer used [by][for] a government entity (describe entity at issue), in furtherance of [the administration of justice][national defense][national security]?

Yes ____ No ____]

[g. _____ Did the defendant cause damage affecting ten or more protected computers during any one year period?

Yes ____ No ____]

[h. _____ Did the defendant [attempt to cause] [knowingly][recklessly] [cause] [serious bodily injury] [death] from such conduct?

Yes ____ No ____]

_____
Foreperson

_____
(Date)

6.18.1030C(2). COMPUTER FRAUD [CAUSING DAMAGE TO A COMPUTER] (18 U.S.C. § 1030(a)(5)(B) and (C))

` The crime of causing damage to a computer or information, as charged in [Count __] of the indictment, has two essential elements, which are:[1]

One, the defendant intentionally accessed a protected computer without authorization, and[2, 3]

Two, the defendant, as a result of such conduct, [recklessly caused damage] [caused damage and loss].[4]

[You are further instructed regarding the crime[s] charged in [Count[s] ____ of] the indictment that the following definitions apply: (Insert applicable portions of Instruction 6.18.1030H, unless the indictment charges multiple computer fraud violations and there will be no confusion in adding the definitions common to all counts after all of the substantive computer fraud instructions).][5]

If you find these two elements unanimously and beyond a reasonable doubt, then you must find the defendant guilty of this crime [under Count __]. Record your determination on the Verdict Form which will be submitted to you with these instructions.

[If you find these two elements unanimously beyond a reasonable doubt, you must also unanimously decide whether the defendant, as a result of such conduct, caused

- [loss to one or more persons[6] during any one-year period of an aggregate value of $5,000.00 or more][;]
- [loss resulting from a related course of conduct affecting one or more other protected computers of an aggregate value of $5,000.00 or more][;]
- [the [potential] [modification] [impairment] of the medical [examination] [diagnosis] [treatment] [care] of one or more individuals]
- [physical injury to any person][;]
- [a threat to public health or safety][;]
- [damage affecting a computer used [by] [for] a governmental entity (describe entity at issue),[7] in furtherance of [the administration of justice] [national defense] [national security]][;] [or]

- [damage affecting ten or more protected computers during any one year period].[8]

  Record your determination on the Verdict Form.]

(Instruction 3.09, *supra*, which describes the Government's burden of proof, has already been incorporated in this instruction and should not be repeated.)

Notes on Use

1. If an attempt to commit an offense under this subsection has been charged, *see* 18 U.S.C. § 1030(b), the instruction should be modified accordingly.

2. "Without authorization" is not defined in section 1030 but is commonly understood to refer to persons who have no permission or authority to do a thing whatsoever. *Condux Intern., Inc. v. Haugum*, 2008 WL 5244818 at *4 (D. Minn. Dec. 15, 2008) (citations omitted).

3. The Committee is of the opinion that the term "intentionally" modifies both "accessed" and "without authorization." *See* S. Rep. No. 99-432, at 6 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2484 (discussing the 1986 amendments to subsection 1030(a)(2) in which Congress changed the scienter requirement from "knowingly" to "intentionally" to clarify that subsection 1030(a)(2) was designed to criminalize those who clearly intended to enter computer files without proper authorization rather than those who inadvertently stumbled upon those files, and observing that "'intentional' means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective").

4. Element two should be modified in accordance with whether the Government has charged a violation of 18 U.S.C. § 1030(a)(5)(B) (recklessly causing damage) or 18 U.S.C. § 1030(a)(5)(C) (negligently or accidentally causing damage and loss).

5. The supplemental definitions contained in Instruction 6.18.1030H, *infra*, should be given in most cases where applicable.

6. If a definition of "person" is desired, *see* 18 U.S.C. § 1030(e)(12).

7. If a definition of "governmental entity" is desired, *see* 18 U.S.C. § 1030(e)(9).

8. Any fact (other than a prior conviction) that increases the maximum penalty for a crime must be charged in the indictment, submitted to the jury, and proven beyond a reasonable doubt. *Apprendi v. New Jersey*, 530 U.S. 466 (2000). Typically, the indictment will not include these aggravating facts if the Government has charged a first-time offender of section 1030 solely with a misdemeanor, *see* 18 U.S.C. § 1030(c)(4)(G), or if it has charged a felony offense that allegedly occurred after a conviction for another offense under section 1030. *See* 18 U.S.C. § 1030(c)(4)(C). If any of the additional aggravating facts set forth in element three have been charged in the indictment, these facts should be submitted to the jury either as a formal element and/or by special interrogatory. 18 U.S.C. §§1030(c)(4)(A); *see* 6.18.1030C(2)(a) for a verdict form with special interrogatories. In the Committee's view, a verdict form with special interrogatories is the preferred method for presenting these aggravating factors to the jury

because it is less likely to result in confusion and because it creates a clear record of the basis for the jury's verdict.

Committee Comments

For a discussion on the kind of proof deemed sufficient to establish the $5,000 aggregate loss amount, *see United States v. Millot*, 433 F.3d 1057, 1061 (8th Cir. 2006).

6.18.1030C(2)(a). SPECIAL VERDICT FORM (INTERROGATORIES TO FOLLOW FINDING OF GUILT) (18 U.S.C. § 1030(a)(5)(B) and (C))

We, the jury, find Defendant (name) _____

(guilty/not guilty)

of computer fraud by causing damage to a computer [as charged in Count _____ of the indictment] [under Instruction No. _____].

If you find the defendant "guilty," you must answer the following question[s] and you must unanimously agree on the answer[s]:

As a result of such conduct,

[a. _____ Did the defendant cause loss to one or more persons[1] during any one-year period of an aggregate value of $5,000.00 or more?

Yes ____ No ____]

[b. _____ Did the defendant cause loss resulting from a related course of conduct affecting one or more other protected computers of an aggregate value of $5,000.00 or more?

Yes ____ No ____]

[c. _____ Did the defendant cause the [potential] [modification] [impairment] of the medical [examination] [diagnosis] [treatment] [care] of one or more individuals?

Yes ____ No ____]

[d. _____ Did the defendant cause physical injury to any person?

Yes ____ No ____]

[e. _____ Did the defendant cause a threat to public health or safety?

Yes ____ No ____]

[f. _____ Did the defendant cause damage affecting a computer used [by] [for] a government entity (describe entity at issue),[2] in furtherance of [the administration of justice] [national defense] [national security]?

Yes ____ No ____]

[g. _____ Did the defendant cause damage affecting ten or more protected computers during any one-year period?

Yes ____ No ____]

_____
Foreperson

_____
(Date)

Notes on Use

1. If a definition of "person" is desired, *see* 18 U.S.C. § 1030(e)(12).
2. If a definition of "government entity" is desired, *see* 18 U.S.C. § 1030(e)(9).

6.18.1030D. COMPUTER FRAUD [TRAFFICKING IN PASSWORDS] (18 U.S.C. § 1030(a)(6))

The crime of trafficking in passwords, as charged in [Count __] of the indictment, has three essential elements, which are:[1]

One, the defendant knowingly

- [transferred to another person any password or similar information through which a computer may be accessed without authorization[2]]
- [obtained control of any password or similar information through which a computer may be accessed without authorization, with the intent to transfer it to another person][3];

Two, the defendant acted with the intent to defraud[4]; and

Three, [the defendant's act[s] affected [interstate] [foreign] commerce] [the computer was used [by] [for] the United States government].

[You are further instructed regarding the crime[s] charged in [Count[s] ____ of] the indictment that the following definitions apply: (Insert applicable portions of Instruction 6.18.1030H, unless the indictment charges multiple computer fraud violations and there will be no confusion in adding the definitions common to all counts after all of the substantive computer fraud instructions).][5]

(Insert paragraph describing Government's burden of proof; *see* Instruction 3.09, *supra*.)

Notes on Use

1. If an attempt to commit an offense under this subsection has been charged, *see* 18 U.S.C. § 1030(b), the instruction should be modified accordingly.

2. "Without authorization" is not defined in section 1030 but is commonly understood to refer to persons who have no permission or authority to do a thing whatsoever. *Condux Intern., Inc. v. Haugum*, 2008 WL 5244818 at *4 (D. Minn. Dec. 15, 2008) (citations omitted).

3. Element one incorporates the definition of "traffic" found in 18 U.S.C. § 1030(a)(6) through its cross reference to 18 U.S.C. § 1029(e)(5). In addition to using the term "transfer," the definition of traffic from section 1029(e)(5) includes the phrase "dispose of." To avoid potential confusion, the Committee has eliminated the "dispose of" phrase in element one.

4. "The "intent to defraud" phrase is not defined by section 1030 or in its legislative history, and neither the Supreme Court nor the Eighth Circuit has defined the phrase in the context of section 1030. The Senate Committee has noted with respect to a similar phrase in

subsection 1030(a)(4) that "[t]he scienter requirement for this subsection, 'knowingly and with intent to defraud,' is the same as the standard used for 18 U.S.C. 1029 relating to credit card fraud." S. Rep. 99-432, S. Rep. No. 432, 99th Cong., 2nd Sess. 1986, 1986 U.S.C.C.A.N. 2479, *available at* 1986 WL 31918. In the section 1029 context, the Eighth Circuit appears to interpret "intent to defraud" very broadly. *See, e.g.,United States v. Kowal*, 527 F.3d 741, 748 (8th Cir. 2008) (stating that to "[d]efraud is to deprive of some right, interest or property by deceit"). Further, in *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc*., 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000), the court broadly held that the term "fraud" as used in subsection 1030(a)(4) means "wrongdoing" and does not require proof of the common law elements of fraud. For the definition of Intent to Defraud used in mail fraud cases, *see* Instruction 6.18.1341, *infra.*

5. The supplemental definitions contained in Instruction 6.18.1030H, *infra*, should be given in most cases where applicable.

Committee Comments

The Senate Committee stated that the term "password" "does not mean a single word that enables one to access a computer. The Committee recognizes that a 'password' may actually be comprised of a set of instructions or directions for gaining access to a computer and intends that the word 'password' be construed broadly enough to encompass both single words and longer more detailed explanations on how to access others' computers." S. Rep. No. 99-432 at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2491.

6.18.1030E. COMPUTER FRAUD [THREATENING TO DAMAGE A PROTECTED COMPUTER OR INFORMATION] (18 U.S.C. § 1030(a)(7))

The crime of threatening to damage a protected computer, as charged in [Count __] of the indictment, has three essential elements, which are:[1]

One, the defendant transmitted any communication in [interstate] [foreign] commerce;

Two, the defendant transmitted the communication with the intent to extort any [money] [thing of value] from any person;[2] and

Three, the communication contained any

- [threat to cause damage to a protected computer][;]
- [threat to obtain information from a protected computer [without authorization][3] [exceeding authorized access]][;]
- [threat to impair the confidentiality of information obtained from a protected computer [without authorization] [exceeding authorized access]][;] [or]
- [[demand] [request] for [money] [thing of value] in relation to damage to a protected computer, and the defendant caused the damage to facilitate the extortion of the [money] [thing of value]].

[The phrase "intent to extort" means an intent to obtain the property of another with his or her consent by the wrongful use of actual or threatened force, violence or fear or under color of official right.][4]

[You are further instructed regarding the crime[s] charged in [Count[s] ____ of] the indictment that the following definitions apply: (Insert applicable portions of Instruction 6.18.1030H, unless the indictment charges multiple computer fraud violations and there will be no confusion in adding the definitions common to all counts after all of the substantive computer fraud instructions).][5]

(Insert paragraph describing Government's burden of proof; *see* Instruction 3.09, *supra*.)

Notes on Use

1. If an attempt to commit an offense under this subsection has been charged, *see* 18 U.S.C. § 1030(b), the instruction should be modified accordingly.

2. If a definition of "person" is desired, *see* 18 U.S.C. § 1030(e)(12).

3. "Without authorization" is not defined in section 1030 but is commonly understood to refer to persons who have no permission or authority to do a thing whatsoever. *Condux Intern., Inc. v. Haugum*, 2008 WL 5244818 at *4 (D. Minn. Dec. 15, 2008) (citations omitted).

4. The Eighth Circuit has not defined "intent to extort" within the context of section 1030, but its use seems similar to that of 18 U.S.C. § 875(d) (interstate transmission of extortionate communication). Courts in the section 875(d) context have relied on the definition of "extortion" found in the Hobbs Act at 18 U.S.C. § 1951(b)(2). *See United States v. Cohen*, 738 F.2d 287, 289 (8th Cir. 1984) (in case charged under 18 U.S.C. § 875(d), court borrowed the definition of "extortion" found in the Hobbs Act, defining "intent to extort" as meaning "an intent to get the property of another with his consent, induced by wrongful use of actual or threatened force, violence or fear"). Thus, the definition of "intent to extort" adopted here for section 1030(a)(7) is based largely on the definition of extortion that is found in Instruction 6.18.1951, *infra*.

5. The supplemental definitions contained in Instruction 6.18.1030H, *infra*, should be given in most cases where applicable.

Committee Comments

Title 18 U.S.C. § 1030(a)(7) is intended to cover "computer-age blackmail" involving any "interstate or international transmissions of threats against computers, computer networks, and their data and programs whether the threat is received by mail, a telephone call, electronic mail, or through a computerized messaging service." S. Rep. No. 104-357, at 12, 1996 WL 492169, at *29 (1996).

6.18.1030F COMPUTER FRAUD [ACCESSING A COMPUTER TO DEFRAUD] (18 U.S.C. § 1030(a)(4))

The crime of accessing a computer to defraud, as charged in [Count __] of the indictment, has [four] [five] essential elements, which are:[1]

One, the defendant knowingly accessed a protected computer [without authorization][2] [exceeding authorized access];[3]

Two, the defendant did so with intent to defraud;[4]

Three, the defendant, by accessing the protected computer [without authorization] [exceeding authorized access], furthered the intended fraud; [and]

Four, the defendant thereby obtained any thing of value [; and][.]

[*Five,* the [object of the defendant's fraud] [thing of value the defendant obtained] consisted of more than just the use of the computer[.] [or] [the use of the computer was the only [object of the defendant's fraud] [thing of value the defendant obtained] and the total value of such use exceeded $5,000 during any one year period].][5]

[You are further instructed regarding the crime[s] charged in [Count[s] ____ of] the indictment that the following definitions apply: (Insert applicable portions of Instruction 6.18.1030H, unless the indictment charges multiple computer fraud violations and there will be no confusion in adding the definitions common to all counts after all of the substantive computer fraud instructions).][6]

(Insert paragraph describing Government's burden of proof; *see* Instruction 3.09, *supra*.)

Notes on Use

1. If an attempt to commit an offense under this subsection has been charged, *see* 18 U.S.C. § 1030(b), the language of the instruction should be modified accordingly.

2. "Without authorization" is not defined in section 1030 but is commonly understood to refer to persons who have no permission or authority to do a thing whatsoever. *Condux Intern., Inc. v. Haugum*, 2008 WL 5244818 at *4 (D. Minn. Dec. 15, 2008) (citations omitted).

3. Although Congress did not squarely address the issue in the legislative history of section 1030, the Committee is of the opinion that the term "knowingly" modifies the term "accessed" as well as the phrases "without authorization" or "exceeding authorization." In other words, the Government must prove both that the defendant knew he or she was accessing a computer and that he or she knew that the access was without authorization or exceeding authorization (in addition to proving that the defendant also acted with intent to defraud). *See*

Flores-Figueroa v. United States, __ U.S. __, 129 S. Ct. 1886, 1891 (2009) (citing *United States v. X-Citement Video, Inc.*, 513 U.S. 64, 79 (1994) (Stevens, J., concurring), and noting that courts ordinarily interpret the word "knowingly" in a criminal statute as applying to all subsequently listed elements, not just the verbs). *Compare* Committee Comments to Instruction 6.18.1030B (discussing the 1986 amendments to subsection 1030(a)(2) in which Congress changed the scienter requirement from "knowingly" to "intentionally" to clarify that it intended to criminalize those who clearly intended to enter computer files without proper authorization rather than those who inadvertently stumbled upon those files).

4. "The 'intent to defraud' phrase is not defined by section 1030 or in its legislative history, and neither the Supreme Court nor the Eighth Circuit has defined the phrase in the context of section 1030. The Senate Committee did note that "[t]he scienter requirement for this subsection, 'knowingly and with intent to defraud,' is the same as the standard used for 18 U.S.C. 1029 relating to credit card fraud." S. Rep. 99-432, S. Rep. No. 432, 99th Cong., 2nd Sess. 1986, 1986 U.S.C.C.A.N. 2479, *available at* 1986 WL 31918. In the section 1029 context, the Eighth Circuit appears to interpret "intent to defraud" very broadly. *See, e.g.,United States v. Kowal*, 527 F.3d 741, 748 (8th Cir. 2008) (stating that to "[d]efraud is to deprive of some right, interest or property by deceit"). Further, in *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000), the court broadly held that the term "fraud" as used in subsection 1030(a)(4) means "wrongdoing" and does not require proof of the common law elements of fraud. For the definition of Intent to Defraud used in mail fraud cases, *see* Instruction 6.18.1341, *infra.*

5. Section 1030(a)(4) contains an express "computer use" statutory exception. Thus, conduct that would otherwise violate the statute is not a crime if "the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period." 18 U.S.C. § 1030(a)(4). It is not clear whether Congress meant for the computer use exception to clarify the elements of the offense or to define an affirmative defense, and the Eighth Circuit has not addressed the issue. The Committee recommends that, if there is an issue about whether the statutory exception applies in a case, optional element five, modified to conform to the particulars of the case, should be submitted to the jury. Element five is stated in the alternative because if the Government proves either that the object of the fraud was more than the use of the computer or that the value of such use was not more than $5,000 in any 1-year period, the statutory exception will not apply.

6. The supplemental definitions contained in Instruction 6.18.1030H, *infra*, should be given in most cases where applicable.

Committee Comments

For a violation of subsection 1030(a)(4), there must be a sufficient tie in between the use of a computer and the fraud: "The Committee does not believe that a scheme or artifice to defraud should fall under the ambit of subsection (a)(4) merely because the offender signed onto a computer at some point near to the commission or execution of the fraud. While such a tenuous link might be covered under current law where the instrumentality used is the mails or the wires, the Committee does not consider that link sufficient with respect to computers. To be

prosecuted under this subsection, the use of the computer must be more directly linked to the intended fraud. That is, it must be used by an offender without authorization or in excess of his authorization to obtain property of another, which property furthers the intended fraud." S. Rep. 99-432, S. Rep. No. 432, 99th Cong., 2nd Sess. 1986, 1986 U.S.C.C.A.N. 2479, *available at* 1986 WL 31918.

For an example of conduct that a defendant agreed was in violation of subsection 1030(a)(4), *see United States v. Sykes*, 4 F.3d 697, 698 (8th Cir. 1993) (defendant pled guilty to making unauthorized use of an automatic teller machine and personal identification number).

With regard to the statutory exception set forth in section 1030(a)(4), the Senate Committee explained that, "[w]hile every trespass in a computer should not be converted into a felony scheme to defraud, a blanket exception for 'computer use' is too broad. Hackers, for example, have broken into Cray supercomputers for the purpose of running password cracking programs, sometimes amassing computer time worth far more than $5,000. In light of the large expense to the victim caused by some of these trespassing incidents, the amendment would limit the 'computer use' exception to cases where the stolen computer use involved less than $5,000 during any one-year period." S. Rep. 99-432, S. Rep. No. 432, 99th Cong., 2nd Sess. 1986, 1986 U.S.C.C.A.N. 2479, *available at* 1986 WL 31918.

6.18.1030G. COMPUTER FRAUD [ACCESSING A NONPUBLIC COMPUTER] (18 U.S.C. § 1030(a)(3))

The crime of accessing a nonpublic computer, as charged in [Count __] of the indictment, has three essential elements, which are:[1]

One, the defendant intentionally accessed a nonpublic computer of a[n] [department][2] [agency] of the United States;[3]

Two, the defendant was without authorization[4] to access not just the nonpublic computer [he] [she] accessed but was without authorization to access any nonpublic computer of that [department] [agency]; and

Three, the defendant accessed a nonpublic computer that was [exclusively for the use of the United States Government] [used [by] [for] the United States Government, and the defendant's conduct affected that use [by] [for] the United States Government].[5]

[You are further instructed regarding the crime[s] charged in [Count[s] ____ of] the indictment that the following definitions apply: (Insert applicable portions of Instruction 6.18.1030H, unless the indictment charges multiple computer fraud violations and there will be no confusion in adding the definitions common to all counts after all of the substantive computer fraud instructions).][6]

(Insert paragraph describing Government's burden of proof; *see* Instruction 3.09, *supra*.)

Notes on Use

1. If an attempt to commit an offense under this subsection has been charged, *see* 18 U.S.C. § 1030(b), the instruction should be modified accordingly.

2. If a definition of the "department of the United States" is desired, *see* 18 U.S.C. § 1030(e)(7).

3. The Committee is of the opinion that the term "intentionally" modifies both "accessed" as well as the phrase that follows, "a nonpublic computer of a[n] [department] [agency] of the United States." *See* S. Rep. No. 99-432, at 6 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2484 (discussing the 1986 amendments to subsection 1030(a)(2) in which Congress changed the scienter requirement from "knowingly" to "intentionally" to clarify that subsection 1030(a)(2) was designed to criminalize those who clearly intended to enter computer files without proper authorization rather than those who inadvertently stumbled upon those files, and observing that "'intentional' means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective").

4. "Without authorization" is not defined in section 1030 but is commonly understood to refer to persons who have no permission or authority to do a thing whatsoever. *Condux Intern., Inc. v. Haugum*, 2008 WL 5244818 at *4 (D. Minn. Dec. 15, 2008) (citations omitted).

5. The phrase, "affected that use [by] [for] the United States Government]" means the defendant's conduct affected the use of the Government's operation of the computer in question. There is no requirement that the defendant's conduct harmed the overall operation of the Government. S. Rep. No. 99-432, at *8-9, 1986 U.S.C.C.A.N. at 2485.

6. The supplemental definitions contained in Instruction 6.18.1030H, *infra*, should be given in most cases where applicable.

Committee Comments

While federal employees may not be subject to prosecution under section 1030(a)(3) as insiders as to their own agency's computers, they may be eligible for prosecution as outsiders where they engage in intrusions into other agencies' computers. S. Rep. No. 99-432, at 7, 1986 U.S.C.C.A.N. at 2485. Thus, Congress specifically provided that section 1030(a)(3) applies "where the offender's act of trespass is interdepartmental in nature." *Id.* at 8. Congress noted that "it is not difficult to envision an individual who, while authorized to use certain computers in one department, is not authorized to use them all. The danger existed that [the statute], as originally introduced, might cover every employee who happens to sit down, within his department, at a computer terminal which he is not officially authorized to use. These acts can also be best handled by administrative sanctions, rather than by criminal punishment. To that end, the Committee has constructed its amended version of (a)(3) to prevent prosecution of those who, while authorized to use some computers in their department, use others for which they lack the proper authorization."

In 1996 amendments to subsection 1030(a)(3), Congress replaced the phrase "computer of a department or agency of the United States" with the term "nonpublic" to "make clear that unauthorized access is barred to any 'non-public' Federal Government computer and that a person who is permitted to access publicly available Government computers, for example, via an agency's World Wide Web site, may still be convicted under (a)(3) for accessing without authority any nonpublic Federal Government computer." S. Rep. No. 104-357, at 9, *available at* 1996 WL 492169, * 21 (1996). Thus, although the phrase "nonpublic computer" is not defined by the statute, it would appear to have its ordinary meaning; that is, any government computer that is not available for access by the public. This is a much narrower definition than the statutory definition of "protected computer."

In earlier versions of 1030(a)(3), if the defendant was charged with unlawfully accessing a computer that was not exclusively for the government's use, the government was required to prove that the conduct "adversely" affected the use of that computer by or for the United States government. In 1996 amendments, Congress removed the word "adversely" in order to eliminate any suggestion "that trespassing in a computer used by the Federal Government, even if not exclusively, may be benign." S. Rep. No 357, 104th Cong., 2d Sess. 9 (1996).

Violations of section 1030(a)(3) are typically charged as misdemeanors and are punishable by a fine and up to one year in prison, 18 U.S.C. § 1030(c)(2)(A), unless the individual has previously been convicted of a section 1030 offense, in which case the crime is a felony punishable up to a maximum of ten years in prison, 18 U.S.C. § 1030(c)(2)(c). Section 1030(a)(3) applies to many of the same cases in which section 1030(a)(2) could be charged. Because section 1030(a)(2) is a felony if certain aggravating facts are present, cases are rarely prosecuted under section 1030(a)(3).

6.18.1030H. COMPUTER FRAUD - SUPPLEMENTAL INSTRUCTIONS[1]

(1) Computer

[The term "computer," as used in [this] [Instruction[s] _____ , means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand-held calculator, or other similar device.][2]

(2) Protected Computer

[The phrase "protected computer," as used in [this] [Instruction[s] _____ , means: [a computer exclusively for the use of [a financial institution] [the United States Government]]; [a computer used [by] [for] a financial institution] [the United States Government] and the conduct constituting the offense affects that use [by] [for] [the financial institution] [the United States Government]]; or [a computer which is [used in] [affecting] [interstate] [foreign] [commerce][3] [communication], including a computer located outside the United States that is used in a manner that affects [interstate] [foreign] [commerce] [communication] of the United States].][4]

(3) Exceeding Authorized Access

[The phrase "exceeding authorized access," as used in [this] [Instruction[s] _____ , means to access a computer with authorization and to use such access to obtain or alter information in the computer that the person accessing the information is not entitled to obtain or alter.][5]

(4) Financial Institution

[The phrase "financial institution," as used in [this] [Instruction[s] _____ , means: [an institution with deposits insured by Federal Deposit Insurance Corporation]; [the Federal Reserve or a member of the Federal Reserve, including any Federal Reserve Bank]; or [a credit union with accounts insured by the National Credit Union Administration].][6]

(5) Financial Record

[The phrase "financial record," as used in [this] [Instruction[s] _____ , means information derived from any record held by [a financial institution] [an issuer of a credit card] [a consumer reporting agency] pertaining to a customer's relationship with that entity.][7]

(6) Damage

[The term "damage," as used in [this] [Instruction[s] _____ , means any impairment to the integrity or availability of data, a program, a system, or information.][8]

(7) Loss

[The term "loss," as used in [this] [Instruction[s] _____ , means any reasonable cost of responding to an offense, conducting a damage assessment, and restoring of data, a 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.][9]

Notes on Use

1. The Committee recommends the court explain the terms and phrases set forth in this instruction which are applicable to the section 1030 count[s] in the indictment. They should, of course, be tailored to the facts of the particular case.

2. 18 U.S.C. § 1030(e)(1).

3. Although Congress has not defined interstate or foreign commerce in section 1030 or in its legislative history, the Eighth Circuit has held, within the context of section 1030, that computers connected to the Internet are instrumentalities and channels of interstate commerce, and "[n]o additional interstate nexus is required when instrumentalities or channels of interstate commerce are regulated." *See United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007) (internal citations omitted). If a definition of Interstate and Foreign Commerce is desired, *see* Instruction 6.18.1956J(2), *infra*.

4. 18 U.S.C. § 1030(e)(2).

5. 18 U.S.C. § 1030(e)(6). The Eighth Circuit "has not addressed the issue of whether one who accesses a computer with apparent authorization, and then arguably uses the information for an improper purpose, has violated" section 1030 by "exceeding authorized access." *American Family Mut. Ins. Co. v. Hollander*, 2009 WL 535990 at * 10-11 (N.D. Iowa Mar. 3, 2009). Courts have come down on both sides of this issue. *See LVRC Holdings LLC v. Brekka,* 581 F.3d 1127 (9th Cir. 2009) (court adopted a plain language approach to section 1030 and held that the defendant, who accessed his employer's computers while still employed and emailed documents to himself and his wife for their own competing consulting business, had not accessed a computer without authorization nor had he exceeded authorized access because he was entitled to access such documents); *Condux Intern., Inc. v. Haugum*, 2008 WL 5244818 at *4-6 (D.

Minn. 2008) (after discussing the split among authorities, court held that "[t]he legislative history of [section 1030] supports" the narrower "interpretation, which focuses on the propriety of the access of information rather than on the propriety of the use of information"); *but see International Airport Centers, LLC v. Citrin*, 440 F.3d 418, 419-20 (7th Cir. 2006) (court held employee lost his authorization to access employer's computer when he violated his duty of loyalty by starting up a competing business and deleting his employer's valuable data from his work laptop before quitting his employment)*; EF Cultural Travel BV v. Explorica, Inc*., 274 F.3d 577, 583-84 (1st Cir. 2001) (court held a former employee had likely violated section 1030 by exceeding authorized access when he used confidential information he had lawfully obtained as an employee to prepare a program that allowed him to compete against his former employer).

6. The statute provides several additional definitions of financial institution which may apply in a particular case. *See* 18 U.S.C. § 1030(e)(4).

7. 18 U.S.C. § 1030(e)(5).

8. 18 U.S.C. § 1030(e)(8). "Damage" can include deletion of data. *See Lasco Foods, Inc. v. Hall and Shaw Sales, Marketing & Consulting, LLC*, 600 F. Supp. 2d 1045, 1052 (E.D. Mo. 2009).

9. 18 U.S.C. § 1030(e)(11). The cost of the forensic analysis and other remedial measures associated with retrieving and analyzing a defendant's computers can constitute "loss" under section 1030. *See Lasco Foods, Inc. v. Hall and Shaw Sales, Marketing & Consulting, LLC*, 600 F. Supp. 2d 1045, 1052 (E.D. Mo. 2009). Although it is a question of fact for the jury whether an alleged loss is reasonable, loss can include not just the cost of outside experts, but also an estimate of the cost of salaried employees, calculated by adding up the total number of hours spent by salaried employees responding to the intrusion and fixing the problem and multiplying those hours by the imputed hourly rates for those employees. *United States v. Millot*, 433 F.3d 1057, 1061 (8th Cir. 2006). Moreover, section 1030 "does not restrict consideration of losses to only the person who owns the computer system." *Id.*

6.18.2251(a). SEXUAL EXPLOITATION OF A CHILD BY A PERSON OTHER THAN PARENT OR GUARDIAN (18 U.S.C. § 2251(a)) [1]

The crime of sexual exploitation of a child, as charged in [Count ___ of] the indictment, has four elements, which are:

One, at the time alleged, (name of minor) was under the age of eighteen years;

Two, the defendant knowingly:

a) [employed] [used] [persuaded] [induced] [enticed] [coerced] (name of minor) to engage in sexually explicit conduct; or

b) had (name of minor) assist another person or persons to engage in sexually explicit conduct; or

c) transported (name of minor) [across state lines] [in foreign commerce] [in any Territory or Possession of the United States] with the intent that (name of minor) engage in sexually explicit conduct;

Three, the defendant acted with the purpose of [producing a visual depiction of such conduct] [transmitting a live visual depiction of such conduct]; and

Four, a) the defendant knew or had reason to know that such visual depiction [*e.g.*, video tape] would be [mailed] [transported across state lines or in foreign commerce]; or

b) the visual depiction was produced using materials that had been mailed, shipped, or transported across state lines or in foreign commerce by any means, including by computer or cellular phone[2]; or

c) the visual depiction was actually [mailed or transported across state lines or in] [transported or transmitted using any means or facility of interstate or] foreign commerce.

A person is "used" if they are photographed or videotaped.[3]

"Sexually explicit conduct" means actual or simulated sexual intercourse, including [genital-genital] [oral-genital] [anal-genital] [oral-anal], whether between persons of the same or

opposite sex]; [bestiality] [masturbation] [sadistic or masochistic abuse] [lascivious exhibition of the genitals or pubic area of any person].[4]

The term "visual depiction"includes [a] [any] [photograph] [film] [video] [picture] [or] [computer or computer-generated image or picture], whether made or produced by electronic, mechanical, or other means. [It includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.][5]

An item is "produced" if it is produced, directed, manufactured, issued, published, advertised, created, made, or is in any other way brought into being by the involvement of an individual participating in the recording of child pornography.[6]

The Government is not required to prove that the defendant knew that (minor's name) was under the age of eighteen.

[Insert paragraph describing the Government's burden of proof. *See* Instruction 3.09, *supra*.]

Notes on Use

1. In the case of attempted sexual exploitation of a child, *see United States v. Pierson*, 544 F.3d 933 (8th Cir. 2008).

2. The fact that an item used in the production of the child pornography had traveled in interstate commerce is, by itself, sufficient to satisfy the analysis of whether there is an impact on interstate commerce sufficient to prohibit the charged conduct under Congress's Commerce Clause powers. *See United States v. Betcher*, 534 F.3d 820 (8th Cir. 2008) (discussing several other Eighth Circuit cases on the matter).

3. *See United States v. Fadl*, 498 F.3d 862, 867 (8th Cir. 2007).

4. The term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2). If lascivious exhibition of the genitals is at issue, it should be further defined. *See* Instruction 6.18.2252A(1).

5. 18 U.S.C. §§ 2256(5) and (8).

6. The term "producing" is defined in 18 U.S.C. § 2256(3). A defendant who allegedly took no directorial, editorial, or managerial role when he filmed minors engaged in explicit sexual conduct, or intended that the photographs be disseminated commercially, nonetheless, "produces" child pornography, within the meaning of the statute prohibiting production of child pornography because Congress's intention was to enact a broad definition of "producing" that encompassed the various means by which an individual might actively participate in the creation and distribution of child pornography. *See United States v. Fadl*, 498 F.3d 862, 867 (8th Cir. 2007).

Committee Comments

Knowledge of the age of the minor victim is not an element of the offense. *See United States v. Wilson*, 565 F.3d 1059, 1066 (8th Cir. 2009); *United States v. Pliego*, 578 F.3d 938 (8th Cir. 2009); *see also United States v. X-Citement Video, Inc.*, 513 U.S. 64, 76 n.5 (1994) ("[P]roducers may be convicted under § 2251(a) without proof they had knowledge of age . . ."). Mistake of age is not a defense to this crime. *Wilson*, 565 F.3d at 1069; *Pliego*, 578 F.3d at 944; *United States v. McCloud*, 590 F.3d 560 (8th Cir. 2009).

The age of the child depicted may be proved by, *inter alia*, language used by the defendant in correspondence, Postal Inspector's professional and personal familiarity with child development, and a pediatrics professor's testimony. *United States v. Broyles*, 37 F.3d 1314, 1317-18 (8th Cir. 1994); *United States v. Rayl*, 270 F.3d 709, 714 (8th Cir. 2001). In *United States v. Vig*, 167 F.3d 443, 449-50 (8th Cir. 1999), the court found that the jury could draw its own independent conclusion as to whether real children were depicted by examining the images presented to them.

The Eighth Circuit has repeatedly found federal jurisdiction based solely on the use of a camera or camera equipment that previously crossed state lines. *See United States v. Betcher*, 534 F.3d 820 (8th Cir. 2008); *United States v. Fadl*, 498 F.3d 862 (8th Cir. 2007).

Transportation in interstate or foreign commerce can be accomplished by any means, including by a computer. 18 U.S.C. § 2251(b).

A defendant who simply possesses, transports, reproduces, or distributes child pornography does not sexually exploit a minor in violation of 18 U.S.C. § 2251, even though the materials possessed, transported, reproduced, or distributed "involve" such sexual exploitation by the producer. *See United States v. Horn*, 187 F.3d 781 (8th Cir. 1999).

6.18.2251(b). SEXUAL EXPLOITATION OF A CHILD BY A PARENT OR GUARDIAN (18 U.S.C. § 2251(b)) [1]

The crime of sexual exploitation of a child, as charged in [Count ___ of] the indictment, has five elements, which are:

One, at the time, (name of minor) was under the age of eighteen years;

Two, the defendant was the [parent] [legal guardian] [person having custody or control] of (name of minor).

Three, the defendant knowingly:

a) permitted (name of minor) to engage in sexually explicit conduct; or

b) permitted (name of minor) to assist another person or persons to engage in sexually explicit conduct;

Four, the defendant acted with the purpose of [producing any visual depiction of such conduct] [transmitting a live visual depiction of such conduct]; and

Five, a) the defendant knew or had reason to know that such visual depiction [*e.g.*, video tape] would be [mailed] [transmitted] [transported across state lines or in foreign commerce]; or

b) the visual depiction was produced using materials that had been mailed, shipped, transmitted, or transported across state lines or in foreign commerce by any means, including by computer or cellular phone[2]; or

c) the visual depiction was actually [mailed or transported across state lines or in] [transported or transmitted using any means or facility of interstate or] foreign commerce.

"Sexually explicit conduct" means actual or simulated sexual intercourse, including [genital-genital] [oral-genital] [anal-genital] [oral-anal], whether between persons of the same or opposite sex]; [bestiality] [masturbation] [sadistic or masochistic abuse]] [lascivious exhibition of the genitals or pubic area of any person][3].

The term “visual depiction”includes [a] [any] [photograph] [film] [video] [picture] [or] [computer or computer-generated image or picture], whether made or produced by electronic,

mechanical, or other means. [It includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.][4]

An item is "produced" if it is produced, directed, manufactured, issued, published, advertised, created, made, or is in any other way brought into being by the involvement of an individual participating in the recording of child pornography.[5]

The Government is not required to prove that the defendant knew that (minor's name) was under the age of eighteen.

[Insert paragraph describing the Government's burden of proof. *See* Instruction 3.09, *supra*.]

Notes on Use

1. In the case of attempted sexual exploitation of a child, *see United States v. Pierson*, 544 F.3d 933 (8th Cir. 2008).

2. The fact that an item used in the production of the child pornography had traveled in interstate commerce is, by itself, sufficient to satisfy the analysis of whether there is an impact on interstate commerce sufficient to prohibit the charged conduct under Congress's Commerce Clause powers. *See United States v. Betcher*, 534 F.3d 820 (8th Cir. 2008) (discussing several other Eighth Circuit cases on the matter).

3. The term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2). If lascivious exhibition of the genitals is at issue, it should be further defined. *See* Instruction 6.18.2252A(1).

4. 18 U.S.C. §§ 2256(5) and (8).

5. The term "producing" is defined in 18 U.S.C. § 2256(3). A defendant who allegedly took no directorial, editorial, or managerial role when he filmed minors engaged in explicit sexual conduct, or intended that the photographs be disseminated commercially, nonetheless, "produces" child pornography, within the meaning of the statute prohibiting production of child pornography because Congress's intention was to enact a broad definition of "producing" that encompassed the various means by which an individual might actively participate in the creation and distribution of child pornography. *See United States v. Fadl*, 498 F.3d 862, 867 (8th Cir. 2007).

Committee Comments

Knowledge of the age of the minor victim is not an element of the offense. *See United States v. Wilson*, 565 F.3d 1059, 1066 (8th Cir. 2009); *United States v. Pliego*, 578 F.3d 938 (8th Cir. 2009); *see also United States v. X-Citement Video, Inc.*, 513 U.S. 64, 76 n.5 (1994) ("[P]roducers may be convicted under § 2251(a) without proof they had knowledge of age . . . "). Mistake of age is not a defense to this crime. *Wilson*, 565 F.3d at 1069; *Pliego*, 578 F.3d at 944; *United States v. McCloud*, 590 F.3d 560 (8th Cir. 2009).

The age of the child depicted may be proved by, *inter alia*, language used by the defendant in correspondence; Postal Inspector's professional and personal familiarity with child development; and a pediatrics professor's testimony. *United States v. Broyles*, 37 F.3d 1314, 1317-18 (8th Cir. 1994); *United States v. Rayl*, 270 F.3d 709, 714 (8th Cir. 2001). In *United States v. Vig*, 167 F.3d 443, 449-50 (8th Cir. 1999), the court found that the jury could draw its own independent conclusion as to whether real children were depicted by examining the images presented to them.

The Eighth Circuit has repeatedly found federal jurisdiction based solely on the use of a camera or camera equipment that previously crossed state lines. *See United States v. Fadl*, 498 F.3d 862 (8th Cir. 2007).

Transportation in interstate or foreign commerce can be accomplished by any means, including by a computer. 18 U.S.C. § 2251(b).

A defendant who simply possesses, transports, reproduces, or distributes child pornography does not sexually exploit a minor in violation of 18 U.S.C. § 2251, even though the materials possessed, transported, reproduced, or distributed "involve" such sexual exploitation by the producer. *United States v. Horn*, 187 F.3d 781 (8th Cir. 1999).

6.18.2251(c). SEXUAL EXPLOITATION OF A CHILD OUTSIDE THE UNITED STATES (18 U.S.C. § 2251(c)) [1]

The crime of sexual exploitation of a child, as charged in [Count ___ of] the indictment, has four elements, which are:

One, at the time, (name of minor) was under the age of eighteen years;

Two, the defendant:

a) [employed] [used] [persuaded] [induced] [enticed] [coerced] (name of minor) to engage in sexually explicit conduct outside the United States, its territories, or possessions; or

b) had (name of minor) assist another person or persons to engage in sexually explicit conduct outside the United States, its territories, or possessions;

Three, for the purpose of producing any visual depiction of such conduct; and

Four, a) the defendant intended such visual depiction to be transported to the United States, its territories, or possessions by any means, including by using mail or any means or facility of interstate or foreign commerce; or

b) the defendant did transport such visual depiction to the United States, its territories, or possessions by any means, including by using mail or any means or facility of interstate or foreign commerce.[2]

A person is "used" if they are photographed or videotaped.[3]

"Sexually explicit conduct" means actual or simulated sexual intercourse, including [genital-genital] [oral-genital] [anal-genital] [oral-anal], whether between persons of the same or opposite sex; [bestiality] [masturbation] [sadistic or masochistic abuse] [lascivious exhibition of the genitals or pubic area of any person].[4]

The term "visual depiction" includes [a] [any] [photograph] [film] [video] [picture] [or] [computer or computer-generated image or picture], whether made or produced by electronic, mechanical, or other means. [It includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.][5]

An item is "produced" if it is produced, directed, manufactured, issued, published, advertised, created, made, or is in any other way brought into being by the involvement of an individual participating in the recording of child pornography.[6]

The Government is not required to prove that the defendant knew that (minor's name) was under the age of eighteen.

[Insert paragraph describing the Government's burden of proof. *See* Instruction 3.09, *supra*.]

Notes on Use

1. In the case of attempted sexual exploitation of a child, *see United States v. Pierson*, 544 F.3d 933 (8th Cir. 2008).

2. The fact that an item used in the production of the child pornography had traveled in interstate commerce is, by itself, sufficient to satisfy the analysis of whether there is an impact on interstate commerce sufficient to prohibit the charged conduct under Congress's Commerce Clause powers. *See United States v. Betcher*, 534 F.3d 820 (8th Cir. 2008) (discussing several other Eighth Circuit cases on the matter).

3. *See United States v. Fadl*, 498 F.3d 862, 867 (8th Cir. 2007).

4. The term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2). If lascivious exhibition of the genitals is at issue, it should be further defined. *See* Instruction 6.18.2252A(1).

5. 18 U.S.C. §§ 2256(5) and (8).

6. The term "producing" is defined in 18 U.S.C. § 2256(3). A defendant who allegedly took no directorial, editorial, or managerial role when he filmed minors engaged in explicit sexual conduct, or intended that the photographs be disseminated commercially, nonetheless, "produces" child pornography, within the meaning of the statute prohibiting production of child pornography because Congress's intention was to enact a broad definition of "producing" that encompassed the various means by which an individual might actively participate in the creation and distribution of child pornography. *See United States v. Fadl*, 498 F.3d 862, 867 (8th Cir. 2007).

Committee Comments

Knowledge of the age of the minor victim is not an element of the offense. *See United States v. Wilson*, 565 F.3d 1059, 1066 (8th Cir. 2009); *United States v. Pliego*, 578 F.3d 938 (8th Cir. 2009); *see also United States v. X-Citement Video, Inc.*, 513 U.S. 64, 76 n.5 (1994) ("[P]roducers may be convicted under § 2251(a) without proof they had knowledge of age . . . "). Mistake of age is not a defense to this crime. *Wilson*, 565 F.3d at 1069; *Pliego*, 578 F.3d at 944.

The age of the child depicted may be proved by, *inter alia*, language used by the defendant in correspondence; Postal Inspector's professional and personal familiarity with child

development; and a pediatrics professor's testimony. *United States v. Broyles*, 37 F.3d 1314, 1317-18 (8th Cir. 1994); *United States v. Rayl*, 270 F.3d 709, 714 (8th Cir. 2001). In *United States v. Vig*, 167 F.3d 443, 449-50 (8th Cir. 1999), the court found that the jury could draw its own independent conclusion as to whether real children were depicted by examining the images presented to them.

The Eighth Circuit has repeatedly found federal jurisdiction based solely on the use of a camera or camera equipment that previously crossed state lines. *See United States v. Fadl*, 498 F.3d 862 (8th Cir. 2007).

Transportation in interstate or foreign commerce can be accomplished by any means, including by a computer. 18 U.S.C. § 2251(b).

A defendant who simply possesses, transports, reproduces, or distributes child pornography does not sexually exploit a minor in violation of 18 U.S.C. § 2251, even though the materials possessed, transported, reproduced, or distributed "involve" such sexual exploitation by the producer. *United States v. Horn*, 187 F.3d 781 (8th Cir. 1999).

6.18.2251D(1). SEXUAL EXPLOITATION OF A CHILD - NOTICE OR ADVERTISEMENT TO ACQUIRE (18 U.S.C. § 2251(d))

The crime of Sexual Exploitation of a Child, as charged in [Count ___ of] the indictment, has three elements, which are:

One, the defendant knowingly [made] [printed] [published] [caused to be made] [caused to be printed] [caused to be published] a [notice] [advertisement];

Two, the [notice] [advertisement] sought or offered:

a) to [receive] [exchange] [buy] [produce] [reproduce] [display] any (describe the visual depiction, *e.g.* a video tape), if the requested production of [the visual depiction] would involve a real person under the age of 18 years engaging in sexually explicit conduct,[1] or

b) participation in any act of sexually explicit conduct [by] [with] a person under the age of 18 years for the purpose of producing a visual depiction of such conduct; and

Three:

a) the defendant knew or had reason to know the [notice] [advertisement] would be transported [in interstate or foreign commerce by any means] [or transmitted using any means of facility of interstate or foreign commerce], including by computer or by mail; or

b) such [notice] [advertisement] was actually transported [in interstate or foreign commerce by any means] [using any means or facility of interstate or foreign commerce], including by computer or by mail.

"Sexually explicit conduct" means actual or simulated sexual intercourse, including [genital-genital] [oral-genital] [anal-genital] [oral-anal], whether between persons of the same or opposite sex; [bestiality] [masturbation] [sadistic or masochistic abuse] [lascivious exhibition of the genitals or pubic area of any person].[2]

The term “visual depiction” includes [a] [any] [photograph] [film] [video] [picture] [or] [computer or computer-generated image or picture], whether made or produced by electronic,

mechanical, or other means. [It includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.][3]

An item is "produced" if it was produced, directed, manufactured, issued, published, advertised, created, made, or in any other way brought into being by the involvement of an individual participating in the recording of child pornography.[4]

Notes on Use

1. Although the statute requires "and such visual depiction is of such conduct," that language is unclear in situations in which child pornography has been solicited but there is no evidence that such a request was acted upon (i.e. there is no evidence that materials were produced or transmitted). Some courts have interpreted this clause to mean that the government must show that the defendant requested child pornography, and that the defendant intended it be of a real child. *See United States v. Pabon-Cruz,* 255 F. Supp. 2d 200 (S.D.N.Y. 2003), *affirmed at* 391 F.3d 86 (2d Cir. 2004). This instruction reflects the same understanding. There is no Eighth Circuit case law on this subject.

2. If lascivious exhibition of the genitals is at issue, it should be further defined. *See* Instruction 6.18.2252A(1).

3. 18 U.S.C. §§ 2256(5) and (8).

4. A defendant who allegedly took no directorial, editorial, or managerial role when he filmed minors engaged in explicit sexual conduct, or did not intend that the photographs be disseminated commercially, nonetheless "produces" child pornography, within the meaning of the statute prohibiting production of child pornography because Congress's intention was to enact a broad definition of "producing" that encompassed the various means by which an individual might actively participate in the creation and distribution of child pornography. *United States v. Fadl*, 498 F.3d 862, 867 (8th Cir. 2007).

Committee Comments

In cases involving the intended acquisition of child pornography, proof that the defendant intentionally sought visual depictions of persons actually under the age of 18 (as opposed to simulated images or images of adults who looked younger than their actual age) is required. However, proof that images were then, in fact, produced using minors actually under the age of 18 is not required. *See* reasoning at *United States v. Pabon-Cruz*, 255 F. Supp. 2d 200 (S.D.N.Y. 2003), *affirmed at* 391 F.3d 86 (2d Cir. 2004). There is no Eighth Circuit case law on this subject.

6.18.2251D(2). SEXUAL EXPLOITATION OF A CHILD - NOTICE OR ADVERTISEMENTS TO FURNISH (18 U.S.C. § 2251(d))

The crime of Sexual Exploitation of a Child by, as charged in [Count ___ of] the indictment, has three elements, which are:

One, the defendant knowingly [made] [printed] [published] [caused to be made] [caused to be printed] [caused to be published] a [notice] [advertisement];

Two, the [notice] [advertisement] offered:

a) to [produce] [display] [distribute] [reproduce] any visual depiction (describe the visual depiction, *e.g.* a video tape), if the production of the visual depiction involves a person under the age of 18 years engaging in sexually explicit conduct and such visual depiction is of such conduct, or

b) participation in any act of sexually explicit conduct [by] [with] a person under the age of 18 years for the purpose of producing a visual depiction of such conduct; and

Three:

a) the defendant knew or had reason to know the [notice] [advertisement] would be transported in interstate or foreign commerce by any means, including by computer or by mail; or

b) such [notice] [advertisement] was actually transported in interstate or foreign commerce by any means, including by computer or by mail.

"Sexually explicit conduct" means actual or simulated sexual intercourse, including [genital-genital] [oral-genital] [anal-genital] [oral-anal], whether between persons of the same or opposite sex; [bestiality] [masturbation] [sadistic or masochistic abuse] [lascivious exhibition of the genitals or pubic area of any person].[1]

The term "visual depiction" includes [a] [any] [photograph] [film] [video] [picture] [or] [computer or computer-generated image or picture], whether made or produced by electronic, mechanical, or other means. [It includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.][2]

An item is "produced" if it is produced, directed, manufactured, issued, published, advertised, created, made, or in any other way brought into being by the involvement of an individual participating in the recording of child pornography.[3]

Notes on Use

1. If lascivious exhibition of the genitals is at issue, it should be further defined. *See* Instruction 6.18.2252A(1).

2. 18 U.S.C. §§ 2256(5) and (8).

3. A defendant who allegedly took no directorial, editorial, or managerial role when he filmed minors engaged in explicit sexual conduct, or did not intend that the photographs be disseminated commercially, nonetheless "produces" child pornography, within the meaning of the statute prohibiting production of child pornography because Congress's intention was to enact a broad definition of "producing" that encompassed the various means by which an individual might actively participate in the creation and distribution of child pornography. *United States v. Fadl*, 498 F.3d 862, 867 (8th Cir. 2007).