Keeping Government Secrets: A Pocket Guide for Judges on the State-Secrets Privilege, the Classified Information Procedures Act, and Court Security Officers

Robert Timothy Reagan

Federal Judicial Center
2007

Contents

Preface

Most federal judges come into contact with classified information infrequently, if at all, but when they do, they are faced with the dilemma of how to protect government secrets in the context of an otherwise public proceeding.

This pocket guide is designed to familiarize federal judges with statutes and procedures established to help public courts protect government secrets when courts are called upon to do so. The guide provides information about the Classified Information Procedures Act (CIPA), information security officers, and secure storage facilities.

I hope you will find this guide useful in meeting the challenge of protecting government secrets in a public forum.

Barbara Jacobs Rothstein
Director, Federal Judicial Center

Introduction

As courts adjudicate cases involving classified information, they must protect government secrets. The Classified Information Procedures Act (CIPA) provides procedures for protecting classified information in criminal prosecutions. Similar procedures are used in civil cases. The courts are assisted in their protection of government secrets by court security officers provided by a small office in the Department of Justice's Management Division called the Litigation Security Group.

According to an executive order of President Clinton, "Security policies designed to protect classified information must ensure consistent, cost effective, and efficient protection of our Nation's classified information, while providing fair and equitable treatment to those Americans upon whom we rely to guard our national security."[1]

I. Classified Information

Classified information is information designated by the executive branch as not subject to public discussion.

> The national interest requires that certain information be maintained in confidence through a system of classification in order to protect our citizens, our democratic institutions, and our participation within the community of nations. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life.[2]

The Classified Information Procedures Act defines "classified information" as

> information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph r. of

1. Exec. Order No. 12,968, 60 Fed. Reg. 40,245 (Aug. 7, 1995).
2. *Id.*

> section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)).[3]

Other laws define classified information similarly.[4] The act, in turn, defines "national security" as "the national defense and foreign relations of the United States."[5] Other laws define national security similarly.[6]

There are three levels of classification: (1) confidential, (2) secret, and (3) top secret. Information is classified by an "original classification authority," who is "an individual authorized in writing, either by the President, the Vice President in the performance of executive duties, or by agency heads or other officials designated by the President, to classify information in the first instance."[7] Confidential information is "information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe."[8] Secret information is "information, the unauthorized disclosure of which reasonably could be expected to cause *serious* damage to the national security that the original classification authority is able to identify or describe."[9] Top secret information is "information the unauthorized disclosure of which reasonably could be expected to cause *exceptionally grave* damage to the national security that the original classification authority is able to identify or describe."[10]

3. 18 U.S.C. app. 3 § 1(a) (2000).

4. Exec. Order No. 13,292 § 6.1(h), 68 Fed. Reg. 15,315 (Mar. 28, 2003) ("'Classified national security information' or 'classified information' means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form."); Exec. Order No. 12,968, 60 Fed. Reg. 40,245 (Aug. 7, 1995) ("'Classified information' means information that has been determined pursuant to Executive Order No. 12958 [superseded by Executive Order No. 13292], or any successor order, Executive Order No. 12951 [concerning Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems], or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure.").

5. 18 U.S.C. app. 3 § 1(b) (2000).

6. Exec. Order No. 13,292 § 6.1(y), 68 Fed. Reg. 15,315 (Mar. 28, 2003) ("the national defense or foreign relations of the United States").

7. *Id.* § 6.1(cc).

8. *Id.* § 1.2(a)(3).

9. *Id.* § 1.2(a)(2) (emphasis added).

10. *Id.* § 1.2(a)(1) (emphasis added).

Generally, access to classified information requires a security clearance.[11] Article III judges are automatically entitled to access to classified information necessary to resolve issues before them, but their law clerks must obtain security clearances to have access to classified information.[12]

Compartmentation can provide an additional layer of security. "Sensitive compartmented information" is "information that not only is classified for national security reasons as Top Secret, Secret, or Confidential, but also is subject to special access and handling requirements because it involves or derives from particularly sensitive intelligence sources and methods."[13] Usually sensitive compartmented information is top secret information, access to which is restricted to a limited set of individuals on a need-to-know basis specific to the information.

Courts do not have authority to overrule classification determinations.[14]

II. The State-Secrets Privilege

The government has a common-law right to keep state secrets secret. The modern articulation of the privilege is a 1952 Supreme Court case.

Three civilian observers were among those killed when a B-29 bomber crashed on October 6, 1948, during a flight to test secret electronic equipment.[15] The observers' widows sued the government and sought to discover the Air Force's official accident investigation report and investigative statements of the three surviving crew members.[16] The Supreme Court determined, in *United States*

11. *E.g.*, United States v. Bin Laden, 58 F. Supp. 2d 113, 118 (S.D.N.Y. 1999).

12. Security Procedures Established Pursuant to PL 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information ¶ 4, 18 U.S.C. app. 3 § 9 note, issued Feb. 12, 1981 [hereinafter Courts' Security Procedures]; United States v. Smith, 899 F.2d 564 (6th Cir. 1990) (holding that executive branch investigations of court staff for security clearances do not violate the constitutional separation of powers).

13. 28 C.F.R. § 17.18(a) (2007).

14. United States v. Fernandez, 913 F.2d 148, 154 (4th Cir. 1990); United States v. Musa, 833 F. Supp. 752, 755 (E.D. Mo. 1993).

15. United States v. Reynolds, 345 U.S. 1, 2–3 (1952).

16. *Id.* at 3.

v. Reynolds, that the evidence was subject to a privilege against revealing military secrets.[17]

The district court had ordered production and awarded the plaintiffs damages as a sanction for the government's failure to produce the evidence and refusal to allow ex parte in camera inspection by the court.[18] The Secretary of the Air Force filed a formal claim of privilege in response to the production order, and the Air Force's judge advocate general filed an affidavit declaring that production of the evidence would seriously hamper national security.[19] The government offered as a substitute production of the surviving crew members for examination as witnesses.[20] The Supreme Court, which did not examine the classified evidence, determined that the proposed substitute was adequate.[21]

> The privilege belongs to the Government and must be asserted by it; it can neither be claimed nor waived by a private party. It is not to be lightly invoked. There must be a formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer. The court itself must determine whether the circumstances are appropriate for the claim of privilege, and yet do so without forcing a disclosure of the very thing the privilege is designed to protect.[22]

A. Invocation of the Privilege

There are three steps to invocation of the state-secrets privilege.[23] First, the privilege must be (1) invoked by the United States government[24] (2) by formal claim made by the head of the department

17. *Id.* at 6.
18. *Id.* at 4–5.
19. *Id.*
20. *Id.* at 5.
21. *Id.* at 11.
22. *Id.* at 7–8 (footnotes omitted).
23. El-Masri v. United States, 479 F.3d 296, 304 (4th Cir. 2007).
24. *El-Masri*, 479 F.3d at 304; Bareford v. Gen. Dynamics Corp., 973 F.2d 1138, 1141 (5th Cir. 1992); Zuckerbraun v. Gen. Dynamics Corp., 935 F.2d 544, 546 (2d Cir. 1991); Fitzgerald v. Penthouse Int'l Ltd., 776 F.2d 1236, 1239 n.4 (4th Cir. 1985); Ellsberg v. Mitchell, 709 F.2d 51, 56 (D.C. Cir. 1983).

controlling the secret[25] (3) after personal review of the matter.[26] Second, the court must determine that the secret information is legitimately secret, in which case it is absolutely protected.[27] Third, the court must determine how protection of the secret affects the case.[28]

B. Secrecy Validity

The court does not determine what information should be secret, but it does have the responsibility to determine what information legitimately has the status of a state secret.

> Judicial control over the evidence in a case cannot be abdicated to the caprice of executive officers. Yet we will not go so far as to say that the court may automatically require a complete disclosure to the judge before the claim of privilege will be accepted in any case. It may be possible to satisfy the court, from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged. When this is the case, the occasion for the privilege is appropriate, and the court should not jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone, in chambers.[29]

The court's review of classified evidence or arguments is not necessary if the public record sufficiently establishes the need to

25. *El-Masri*, 479 F.3d at 304; Sterling v. Tenet, 416 F.3d 338, 345 (4th Cir. 2005); McDonnell Douglas Corp. v. United States, 323 F.3d 1006, 1022 (Fed. Cir. 2003); Kasza v. Browner, 133 F.3d 1159, 1169 (9th Cir. 1998); *Bareford*, 973 F.2d at 1141; *Zuckerbraun*, 935 F.2d at 546; Halkin v. Helms, 690 F.2d 977, 991 (D.C. Cir. 1982); *Fitzgerald*, 776 F.2d at 1242; Halpern v. United States, 258 F.2d 36, 38 (2d Cir. 1958).

26. *El-Masri*, 479 F.3d at 304; *Sterling*, 416 F.3d at 345; *Kasza*, 133 F.3d at 1169; *Bareford*, 973 F.2d at 1141–42; *Zuckerbraun*, 935 F.2d at 546; *Halkin*, 690 F.2d at 991; *Halpern*, 258 F.2d at 38.

27. *El-Masri*, 479 F.3d at 304–06; *Sterling*, 416 F.3d at 343; *McDonnell Douglas Corp.*, 323 F.3d at 1021; *Kasza*, 133 F.3d at 1166; Black v. United States, 62 F.3d 1115, 1119 (8th Cir. 1995); *Zuckerbraun*, 935 F.2d at 546–47; *Fitzgerald*, 776 F.2d at 1243; *Halkin*, 690 F.2d at 990, 992–94.

28. *El-Masri*, 479 F.3d at 304, 306–13; *Kasza*, 133 F.3d at 1166; *Bareford*, 973 F.2d at 1141–44; *Halkin*, 690 F.2d at 990, 997–99; *Fitzgerald*, 776 F.2d at 1243; *Halpern*, 258 F.2d at 43–44.

29. United States v. Reynolds, 345 U.S. 1, 10 (1952).

keep the evidence secret.[30] Whether or not the court reviews classified evidence or arguments also depends upon a balancing of how necessary the evidence is to a party's case and how imperative it is that the evidence remain secret.[31]

C. Disposition of the Case

A case may be dismissed if it cannot be litigated without compromising state secrets.[32] If a plaintiff is denied access to state secrets that are essential to the plaintiff's claim, then the claim may be dismissed.[33] If a defendant is denied access to, or prevented from entering into evidence, state secrets that are essential to a defense, then also the claim may be dismissed.[34] But unavailability of material evidence does not necessarily result in dismissal; sometimes the case is simply litigated without the unavailable evidence.[35]

If both the plaintiff and the defendant have access to state-secrets evidence, the court may be able to use various protective procedures to litigate the case without exposing state secrets to

30. *Sterling*, 416 F.3d at 343–45; *Halkin*, 690 at 992–94.

31. *Sterling*, 416 F.3d at 343; Ellsberg v. Mitchell, 709 F.2d 51, 58–59 (D.C. Cir. 1983).

32. *Sterling*, 416 F.3d at 345–48; *McDonnell Douglas Corp.*, 323 F.3d at 1021; *Kasza*, 133 F.3d at 166; *Fitzgerald*, 776 F.2d at 1243.

33. *McDonnell Douglas Corp.*, 323 F.3d at 1024; Monarch Assurance P.L.C. v. United States, 244 F.3d 1356, 1361 (Fed. Cir. 2001); *Kasza*, 133 F.3d at 166; Black v. United States, 62 F.3d 1115, 1119 (8th Cir. 1995); *Bareford*, 973 F.2d at 1142; *Zuckerbraun*, 935 F.2d at 547–48.

34. *In re* Sealed Case, 494 F.3d 139, 149 (D.C. Cir. 2007); *Sterling*, 416 F.3d at 344; Tenenbaum v. Simonini, 372 F.3d 776, 777 (6th Cir. 2004); *Kasza*, 133 F.3d at 166; Molerio v. FBI, 749 F.2d 815, 825 (D.C. Cir. 1984).

35. *In re Sealed Case*, 494 F.3d at 148 ("even after evidence relating to covert operatives, organizational structure and functions, and intelligence-gathering sources, methods, and capabilities is stricken from the proceedings under the state secrets privilege, [the plaintiff] has alleged sufficient facts to survive a motion to dismiss"); *Kasza*, 133 F.3d at 166; *In re* United States, 872 F.2d 472, 480 (D.C. Cir. 1989) ("We share the district court's confidence that it can police the litigation so as not to compromise national security."); Farnsworth Cannon, Inc. v. Grimes, 635 F.2d 268, 270–71 (4th Cir. 1980) ("When the government is not a party and successfully resists disclosure sought by a party, the result is simply that the evidence is unavailable, as though a witness had died, and the case will proceed accordingly, with no consequences save those resulting from the loss of the evidence.") (quoting McCormick's Handbook of the Law of Evidence § 109, at 233 (1972)).

the public.[36] The case may also proceed if evidence is available that suitably substitutes for state-secrets evidence.[37]

D. Covert Espionage Agreements

Courts may not hear suits premised on covert espionage agreements.[38]

> It may be stated as a general principle, that public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential, and respecting which it will not allow the confidence to be violated. On this principle, suits cannot be maintained which would require a disclosure of the confidences of the confessional, or those between husband and wife, or of communications by a client to his counsel for professional advice, or of a patient to his physician for a similar purpose. Much greater reason exists for the application of the principle to cases of contract for secret services with the government, as the existence of a contract of that kind is itself a fact not to be disclosed.[39]

The Supreme Court determined in *Totten v. United States* that the survivor of an alleged Civil War spy could not recover from the government unpaid compensation for the spying.[40] Chief Justice William Rehnquist determined for the Court in *Tenet v. Doe* that *Totten*'s absolute bar is not just an example of the state-secrets privilege.[41]

36. Loral Corp. v. McDonnell Douglas Corp., 558 F.2d 1130, 1132 (2d Cir. 1977) ("[A] large amount of material properly classified confidential and secret must be submitted to the trier of fact in the case. We are persuaded that this circumstance is enough to make it inappropriate for jury trial."); Halpern v. United States, 258 F.2d 36, 43 (2d Cir. 1958) ("Under the circumstances of this case, we are not convinced that a trial *in camera* is either undesirable or unfeasible.").

37. United States v. Reynolds, 345 U.S. 1, 11 (1952) ("Here, necessity was greatly minimized by an available alternative, which might have given respondents the evidence to make out their case without forcing a showdown on the claim of privilege.").

38. Tenet v. Doe, 544 U.S. 1 (2005).

39. Totten v. United States, 92 U.S. 105, 107 (1876).

40. *Totten*, 92 U.S. 105.

41. *Tenet*, 544 U.S. at 10.

III. The Classified Information Procedures Act

The Classified Information Procedures Act (CIPA) was enacted on October 15, 1980, and it is codified as the third appendix to Title 18 of the U.S. Code, the title concerning crimes and criminal procedures.[42]

CIPA, by its terms, covers only criminal cases; in civil cases, courts and the government follow procedures similar to those provided by CIPA.[43]

If either the government or the defendant believes that classified information will come into play in a criminal case, then that party must bring the matter to the court's attention, and the court must establish and implement procedures to keep classified information secret.[44]

IV. Bringing Classified Information to the Court's Attention

The court should receive prompt notice if classified information will be at play in a prosecution, and the court should promptly establish procedures to protect the information:

> At any time after the filing of the indictment or information, any party may move for a pretrial conference to consider matters relating to classified information that may arise in connection with the prosecution. Follow-

42. The text of CIPA is reproduced in Appendix A.

43. 28 C.F.R. § 17.17(c) (2007).

44. United States v. Mejia, 448 F.3d 436, 455 (D.C. Cir. 2006) ("CIPA is a procedural statute that does not itself create a privilege against discovery of classified information."); United States v. O'Hara, 301 F.3d 563, 568 (7th Cir. 2002) ("CIPA's fundamental purpose [is] protecting and restricting the discovery of classified information in a way that does not impair the defendant's right to a fair trial."); United States v. Klimavicius-Viloria, 144 F.3d 1249, 1261 (9th Cir. 1998) ("Congress intended CIPA to clarify the court's power to restrict discovery of classified information."); United States v. Anderson, 872 F.2d 1508, 1514 (11th Cir. 1989) ("CIPA was enacted by Congress in an effort to combat the growing problem of greymail, a practice whereby a criminal defendant threatens to reveal classified information during the course of his trial in the hope of forcing the government to drop the criminal charge against him.").

> ing such motion, or on its own motion, the court shall promptly hold a pretrial conference . . . .[45]

A. Classified Information Held by the Government

The government may bring concerns about classified information to the court's attention ex parte: "The court may permit the United States to make a request for [authorization to withhold classified information from the defendant] in the form of a written statement to be inspected by the court alone."[46]

If the court is to implement procedures to protect classified information, the government should provide the defendant with notice that classified information is at issue.[47]

> Before any [CIPA hearing], the United States shall provide the defendant with notice of the classified information that is at issue. Such notice shall identify the specific classified information at issue whenever that information previously has been made available to the defendant by the United States. When the United States has not previously made the information available to the defendant in connection with the case, the information may be described by generic category, in such form as the court may approve, rather than by identification of the specific information of concern to the United States.[48]

A court of appeals held that it was improper for a government agency to initiate secret proceedings, without the knowledge of either the defense or the prosecution, to determine whether certain classified information had to be disclosed to the defendant.[49]

B. Classified Information Held by a Defendant

If a criminal defendant contemplates use of classified information, the defendant must notify both the court and the government of its intentions.

45. 18 U.S.C. app. 3 § 2 (2000).
46. *Id.* § 4.
47. United States v. Baptista-Rodriguez, 17 F.3d 1354, 1363 (11th Cir. 1994).
48. 18 U.S.C. app. 3 § 6(a)(1) (2000).
49. *Mejia*, 448 F.3d at 453–54 (concerning a district court finding in a drug-crime prosecution that classified evidence presented ex parte and in camera by the Drug Intelligence Unit of the Justice Department's Narcotic and Dangerous Drug Section would not be helpful to the defense).

> If a defendant reasonably expects to disclose or to cause the disclosure of classified information in any manner in connection with any trial or pretrial proceeding involving the criminal prosecution of such defendant, the defendant shall, within the time specified by the court or, where no time is specified, within thirty days prior to trial, notify the attorney for the United States and the court in writing. Such notice shall include a brief description of the classified information. Whenever a defendant learns of additional classified information he reasonably expects to disclose at any such proceeding, he shall notify the attorney for the United States and the court in writing as soon as possible thereafter and shall include a brief description of the classified information.[50]

A court of appeals held that "a brief description of the classified information," as prescribed in the text of the statute, is sufficient, overruling a trial court holding that the defendant's notice must include justifications of relevance.[51] But the notice must contain sufficient detail so that the government can determine how presentation of the evidence might damage national security.[52]

Evidence preclusion is the statutory remedy for failure to comply with the notice requirement.[53] When a defendant identified virtually every classified document that the government had produced in discovery as reasonably expected to be used at trial, the court determined that the vastly overinclusive notice was in bad faith, and so the court required the defendant to identify for use at trial approximately the same number of classified documents as the government had identified its intent to use.[54]

V. Protective Procedures

A. CIPA Hearing

Protective procedures generally are established through a CIPA hearing. Both parties are present, but the hearing may be conduct-

50. 18 U.S.C. app. 3 § 5(a) (2000).

51. United States v. Miller, 874 F.2d 1255, 1276 (9th Cir. 1989).

52. United States v. Collins, 720 F.2d 1195, 1200 (11th Cir. 1983).

53. 18 U.S.C. app. 3 § 5(b) (2000); United States v. Badia, 827 F.2d 1458, 1464–66 (11th Cir. 1987).

54. United States v. North, 708 F. Supp. 389 (D.D.C. 1988).

ed in camera if the government certifies that an in camera hearing is necessary to protect classified information.

> Within the time specified by the court for the filing of a motion under this section, the United States may request the court to conduct a hearing to make all determinations concerning the use, relevance, or admissibility of classified information that would otherwise be made during the trial or pretrial proceeding. Upon such a request, the court shall conduct such a hearing. Any hearing held pursuant to this subsection (or any portion of such hearing specified in the request of the Attorney General) shall be held in camera if the Attorney General certifies to the court in such petition that a public proceeding may result in the disclosure of classified information.[55]

The record of a hearing concerning classified information should be preserved for use in an appeal, but should be sealed to prevent unauthorized disclosure of the classified information.

> If at the close of an in camera hearing under this Act (or any portion of a hearing under this Act that is held in camera) the court determines that the classified information at issue may not be disclosed or elicited at the trial or pretrial proceeding, the record of such in camera hearing shall be sealed and preserved by the court for use in the event of an appeal. The defendant may seek reconsideration of the court's determination prior to or during trial.[56]

B. Protective Orders

A key tool in protecting classified information is the protective order. "Upon motion of the United States, the court shall issue an order to protect against the disclosure of any classified information disclosed by the United States to any defendant in any criminal case in a district court of the United States."[57]

55. 18 U.S.C. app. 3 § 6(a) (2000); *see also id.* § 6(c)(1) ("The court shall hold a hearing on any motion under this section. Any such hearing shall be held in camera at the request of the Attorney General.").

56. *Id.* § 6(d).

57. *Id.* § 3.

C. Classification Designations

In the prosecution of Admiral John Poindexter for obstruction of Congress in the Iran–Contra scandal, the government produced in discovery hundreds of thousands of pages of documents, many of which were classified.[58] But the practices of the agencies who supplied the documents did not always result in the documents' being marked to reflect their level of classification or precisely what parts of the documents were classified.[59] On the one hand, a full classification review of all of the documents would have been too burdensome for the government; but on the other hand, the defendant needed to know the classification status of documents he wanted to use for trial.[60] The parties negotiated a procedure, which was approved by the court, in which the defendant would identify documents he wanted to share with witnesses or use for trial, and an interagency group of government security officers would perform a full classification review on those documents, but the group would not disclose to the attorneys representing the government which documents were reviewed.[61]

D. Withholding Discovery

Classified information may be withheld from the defendant. The act provides for three ways of withholding discovery: (1) deletion, (2) summarization, and (3) admission.

> The court, upon a sufficient showing, may authorize the United States to delete specified items of classified information, from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove.[62]

In a prosecution for conspiracy to bomb the Los Angeles International Airport in December 1999, the court reviewed classified intelligence information potentially discoverable by the defendant

58. United States v. Poindexter, 727 F. Supp. 1470, 1472, 1486 (D.D.C. 1989).
59. *Id.* at 1486 & n.33.
60. *Id.* at 1486.
61. *Id.*
62. 18 U.S.C. app. 3 § 4 (2000).

and, after determining what was discoverable, authorized the government to provide the defendant with unclassified summaries.[63]

The government must, however, provide the defendant with such information as is relevant and helpful to the defense.[64]

E. Ex Parte Presentation

To resolve discovery issues and pretrial motions, the government can present to the court in ex parte proceedings classified evidence to which neither the defendant nor defense counsel has access.[65]

During the discovery phase of an obstruction-of-justice prosecution of Vice President Dick Cheney's chief of staff, the court permitted the government to submit ex parte potentially discoverable classified material for the court's review so long as the government explained why the material was classified and why defense counsel with security clearances could not see it.[66] The court also allowed defense counsel to submit ex parte to the court their defense needs so that the court could better evaluate whether the government's classified submissions were discoverable.[67]

In a prosecution for helping to fund Hamas, the defendant sought to suppress confession statements that he claimed were obtained with torture by Israeli secret police officers.[68] The governments of the United States and Israel waived the classification designation regarding all evidence presented at the suppression hearing, except for a small amount of evidence that concerned the credibility of the Israeli witnesses but not the defendant's treatment or guilt.[69] The court heard this evidence in camera and ex

63. United States v. Ressam, 221 F. Supp. 2d 1252, 1256 (W.D. Wash. 2002).

64. United States v. Klimavicius-Viloria, 144 F.3d 1249, 1261 (9th Cir. 1998) ("In order to determine whether the government must disclose classified information, the court must determine whether the information is 'relevant and helpful to the defense of an accused.'"); United States v. Rezaq, 134 F.3d 1121, 1142 (D.C. Cir. 1998) ("[I]f some portion or aspect of a document is classified, a defendant is entitled to receive it only if it may be helpful to his defense. A court applying this rule should, of course, err on the side of protecting the interests of the defendant.").

65. *Klimavicius-Viloria*, 144 F.3d at 1261; United States v. Pringle, 751 F.2d 419, 427 (1st Cir. 1984).

66. United States v. Libby, 429 F. Supp. 2d 18, 25, 27 (D.D.C. 2006).

67. *Id.* at 26–27; *see also* United States v. North, 708 F. Supp. 389, 391 (D.D.C. 1988) (noting that the court obtained ex parte information about the intended defense before ordering extensive discovery on the government).

68. United States v. Marzook, 435 F. Supp. 2d 708 (N.D. Ill. 2006).

69. *Id.* at 745–47.

parte.[70] Because the defense did not have access to this evidence, the court drew "adverse inferences" against the government, which the court explained were like a thumb on the scale in favor of the defendant—not drawing any inferences from the evidence in the government's favor.[71]

F. Limited Presentation at Trial

The court may authorize the presentation of classified information at trial by summary or authorize admissions that would render the presentation of classified information unnecessary.[72] But the defendant must retain "substantially the same ability to make his defense as would disclosure of the specific classified information."[73]

> If the evidence would be admissible at trial, the burden shifts to the government to offer in lieu of the classified evidence either a statement admitting relevant facts that the classified information would tend to prove or a summary of the specific classified information. . . .
>
> . . . [But] the district court may not take into account the fact that evidence is classified when determining its use, relevance, or admissibility.[74]

Some courts have held that normal evidentiary principles govern the admissibility of classified evidence.[75] For example, a district court ruled that classified evidence was admissible as part of a hijacking defendant's argument that the hijacking was a CIA operation.[76] Other courts require a balancing of the public interest in protecting secrets against the right to a defense.[77]

Classified information may be presented to a jury without requiring security clearances for the jurors, but jurors may be cautioned not to disclose the classified information to others.[78]

70. *Id.* at 746.

71. *Id.* at 750.

72. 18 U.S.C. app. 3 § 6(c)(1) (2000).

73. *Id.*

74. United States v. Baptista-Rodriguez, 17 F.3d 1354, 1363–64 (11th Cir. 1994) (quotation marks omitted).

75. United States v. Anderson, 872 F.2d 1508, 1514 (11th Cir. 1989); United States v. Wilson, 750 F.2d 7, 9 (2d Cir. 1984).

76. United States v. Lopez-Lima, 738 F. Supp. 1404 (S.D. Fla. 1990).

77. United States v. Smith, 780 F.2d 1102, 1105 (4th Cir. 1985).

78. Courts' Security Procedures, *supra* note 12, ¶ 6.

When a defendant sought to prove that his confession was obtained with torture by Israeli secret police officers, the court permitted the government to make several admissions to obviate presentation of classified evidence.[79] For example, the government admitted that Israeli secret police officers were authorized to use hoods, handcuffs, and shackles during interrogations.[80] The defendant was able to question the police officers at trial about their treatment of him and "pursue extensive cross examination except in the limited areas that would elicit classified information."[81]

Courts will sometimes permit narrowly tailored procedures that present classified evidence to the judge, the parties, and the jury, but not to the public.[82]

However, in a trial for conspiracy to communicate national defense information to unauthorized persons, the government sought to use a "silent witness" procedure extensively.[83] Using this procedure, the court, the witness, the parties, and the jury would have access to classified documents, but the public would not. Testimony concerning classified information would be in code, such as by referring to persons as X, Y, and Z, and by referring to countries as A, B, and C. The trial judge ruled that extensive use of this procedure would impair the defendant's statutory right to make his defense and his constitutional right to a public trial.[84]

G. Declassification

Once the court determines what classified evidence must be admitted to ensure the defendant a fair trial, the government may decide to declassify the information.[85]

79. United States v. Salah, 462 F. Supp. 2d 915, 917–18, 925 (N.D. Ill. 2006).

80. *Id.* at 917.

81. *Id.* at 923, 925.

82. *E.g.*, United States v. Pelton, 696 F. Supp. 156 (D. Md. 1986) (allowing the playing of audio tapes containing "secret" information through headphones).

83. United States v. Rosen, 487 F. Supp. 2d 703, 705–09 (E.D. Va. 2007); *see also* United States v. Zettl, 835 F.2d 1059, 1063 (4th Cir. 1987) (describing the silent witness rule).

84. *Rosen*, 487 F. Supp. 2d at 714, 720.

85. United States v. O'Hara, 301 F.3d 563, 568 (7th Cir. 2002).

H. Jury Instructions

It may be helpful to instruct the jury on why trial proceedings appear to be skirting relevant information. One judge developed the following instruction:

> This case involves certain classified information. Classified information is information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure. In lieu of disclosing specific classified information, I anticipate that you will hear certain substitutions for the classified information during this trial. These substitutions are admissions of relevant facts by the United States for purposes of this trial. The witnesses in this case as well as attorneys are prohibited from disclosing classified information and, in the case of the attorneys, are prohibited from asking questions to any witness which if answered would disclose classified information. Defendants may not cross examine a particular witness regarding the underlying classified matters set forth in these admissions. You must decide what weight, if any, to give to these admissions.[86]

I. Dismissal

If the government's secrets cannot be protected adequately while affording the defendant a fair trial, then ordinarily the indictment is dismissed.[87]

VI. Flexibility

At the conclusion of the trial of Colonel Oliver North for his involvement in the Iran–Contra scandal, Judge Gerhard Gesell observed that the court and the attorneys served the purposes of CIPA, although they did not always conform to CIPA precisely.

> CIPA was ill-suited to a case of this type and amendments are needed to recognize practical difficulties. For some instances, the Court followed procedures which

86. United States v. Salah, 462 F. Supp. 2d 915, 924 (N.D. Ill. 2006).
87. United States v. Moussaoui, 382 F.3d 453, 466 n.18, 474–76 (4th Cir. 2004).

> were not in strict accord with the statutory framework to expedite resolution of unusual problems that arose. Fortunately, CIPA is a procedural statute, and the legislative history of it shows that Congress expected trial judges to fashion creative solutions in the interests of justice for classified information problems. The Executive cooperated with the Court by liberally waiving classification objections when to do otherwise might have halted the proceeding and interfered with a fair trial.[88]

VII. Interlocutory Appeal

The government has a statutory right to an expedited interlocutory appeal of an order "authorizing the disclosure of classified information, imposing sanctions for nondisclosure of classified information, or refusing a protective order sought by the United States to prevent the disclosure of classified information."[89]

VIII. Court Security Officers

The Department of Justice employs security specialists whose job it is to assist the courts in protecting the secrecy of classified information.

There are ten security specialists employed by the Department of Justice's Security and Emergency Planning Staff (SEPS). They, plus an associate director of SEPS and a secretary, constitute the Litigation Security Group, which is approximately one eighth of SEPS's personnel. The director of SEPS reports to the deputy assistant attorney general for Human Resources and Administration, a unit of the Department of Justice's Management Division, which is headed by an assistant attorney general. This assistant attorney general is designated by regulation as the Justice Department's manager of information classification and access to classified information.[90]

The security specialists are not lawyers, and they are organizationally quite separate from the government's representatives in

88. United States v. North, 713 F. Supp. 1452, 1452–53 (D.D.C. 1989).
89. 18 U.S.C. app. 3 § 7(a) (2000).
90. *Id.* § 17.11(a).

court. Their obligation is to help the court protect classified information, not to assist the government's representatives in court.[91] In fact, they often provide assistance to parties opposing the government.

Formally, in criminal cases, when the court needs assistance in protecting classified information, the director of SEPS submits to the presiding judge a nomination letter recommending a security specialist as the court's security officer. This nomination letter complies with procedures established by Chief Justice Warren Burger on February 12, 1981,[92] as required by the act:

> Within one hundred and twenty days of the date of the enactment of this Act, the Chief Justice of the United States, in consultation with the Attorney General, the Director of Central Intelligence, and the Secretary of Defense, shall prescribe rules establishing procedures for the protection against unauthorized disclosure of any classified information in the custody of the United States district courts, courts of appeal, or Supreme Court. Such rules, and any changes in such rules, shall be submitted to the appropriate committees of Congress and shall become effective forty-five days after such submission.[93]

Chief Justice Burger's procedures provide that the court security officer *shall* be selected from among the persons listed in the nomination letter.[94] The director of SEPS customarily recommends one security specialist as the court security officer for the case and recommends all others as alternates (including the SEPS associate director for the Litigation Security Group but excluding a security specialist whose job is largely administrative).

91. United States v. Yunis, 867 F.2d 617, 621 n.8 (D.C. Cir. 1989); United States v. Musa, 833 F. Supp. 752, 756 (E.D. Mo. 1993).

92. Courts' Security Procedures, *supra* note 12. The procedures are reproduced in Appendix B.

93. 18 U.S.C. app. 3 § 9(a) (2000) (as enacted Oct. 15, 1980). The phrase "Director of Central Intelligence" was changed to "Director of National Intelligence" when the latter position was created in 2004. P.L. 108-458 (Dec. 17, 2004), 118 Stat. 3691.

94. Courts' Security Procedures, *supra* note 12, ¶ 2.

IX. Sensitive Compartmented Information Facilities

The court security officer will assist the court in determining how to physically secure classified documents. Sometimes a safe in the judge's chambers is enough. Sometimes classified documents must be stored in a "Sensitive Compartmented Information Facility," or SCIF.

A SCIF (which usually is pronounced like "skiff") is a secure room—or building—that meets certain construction and access requirements. Courthouses where cases implicating classified information arise frequently—such as the Southern District of New York and the Eastern District of Virginia—have one or more SCIFs. Safes and locked file cabinets may be stored in a SCIF, and different judges may have access to different parts of a SCIF.

When a SCIF is required for a court to hear a case, the government will either construct a SCIF for the court or arrange for the court to have access to an existing SCIF.[95] It is even possible to "SCIF" a judge's bathroom.

Attorneys—and their clients if they have sufficient security clearances—may be required to review classified information within a SCIF. Sometimes secure computers are provided for attorneys' exclusive use within the SCIF.

X. Conclusion

The executive branch decides what information is classified as state secrets, and the judicial branch decides how to protect the rights of parties in civil and criminal cases while keeping government secrets. The Classified Information Procedures Act and court security officers help the courts meet their obligations to the parties and the government.

95. "Expenses of the United States Government which arise in connection with the implementation of these procedures shall be borne by the Department of Justice or other appropriate Executive Branch agency." *Id.* ¶ 12.

Appendix A

Classified Information Procedures Act[96]

§ 1. Definitions

(a) "Classified information," as used in this Act, means any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)).

(b) "National security," as used in this Act, means the national defense and foreign relations of the United States.

§ 2. Pretrial Conference

At any time after the filing of the indictment or information, any party may move for a pretrial conference to consider matters relating to classified information that may arise in connection with the prosecution. Following such motion, or on its own motion, the court shall promptly hold a pretrial conference to establish the timing of requests for discovery, the provision of notice required by section 5 of this Act, and the initiation of the procedure established by section 6 of this Act. In addition, at the pretrial conference the court may consider any matters which relate to classified information or which may promote a fair and expeditious trial. No admission made by the defendant or by any attorney for the defendant at such a conference may be used against the defendant unless the admission is in writing and is signed by the defendant and by the attorney for the defendant.

§ 3. Protective Orders

Upon motion of the United States, the court shall issue an order to protect against the disclosure of any classified information dis-

96. 18 U.S.C. app. 3 (2000), enacted by P.L. 96-456 (Oct. 15, 1980), 94 Stat. 2025–32.

closed by the United States to any defendant in any criminal case in a district court of the United States.

§ 4. Discovery of Classified Information by Defendants

The court, upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove. The court may permit the United States to make a request for such authorization in the form of a written statement to be inspected by the court alone. If the court enters an order granting relief following such an ex parte showing, the entire text of the statement of the United States shall be sealed and preserved in the records of the court to be made available to the appellate court in the event of an appeal.

§ 5. Notice of Defendant's Intention to Disclose Classified Information

(a) Notice by Defendant

If a defendant reasonably expects to disclose or to cause the disclosure of classified information in any manner in connection with any trial or pretrial proceeding involving the criminal prosecution of such defendant, the defendant shall, within the time specified by the court or, where no time is specified, within thirty days prior to trial, notify the attorney for the United States and the court in writing. Such notice shall include a brief description of the classified information. Whenever a defendant learns of additional classified information he reasonably expects to disclose at any such proceeding, he shall notify the attorney for the United States and the court in writing as soon as possible thereafter and shall include a brief description of the classified information. No defendant shall disclose any information known or believed to be classified in connection with a trial or pretrial proceeding until notice has been given under this subsection and until the United States has been afforded a reasonable opportunity to seek a determination pursuant to the procedure set forth in section 6 of this Act, and until the time for the United States to appeal such determination under

section 7 has expired or any appeal under section 7 by the United States is decided.

(b) Failure to Comply

If the defendant fails to comply with the requirements of subsection (a) the court may preclude disclosure of any classified information not made the subject of notification and may prohibit the examination by the defendant of any witness with respect to any such information.

§ 6. Procedure for Cases Involving Classified Information

(a) Motion for Hearing

Within the time specified by the court for the filing of a motion under this section, the United States may request the court to conduct a hearing to make all determinations concerning the use, relevance, or admissibility of classified information that would otherwise be made during the trial or pretrial proceeding. Upon such a request, the court shall conduct such a hearing. Any hearing held pursuant to this subsection (or any portion of such hearing specified in the request of the Attorney General) shall be held in camera if the Attorney General certifies to the court in such petition that a public proceeding may result in the disclosure of classified information. As to each item of classified information, the court shall set forth in writing the basis for its determination. Where the United States' motion under this subsection is filed prior to the trial or pretrial proceeding, the court shall rule prior to the commencement of the relevant proceeding.

(b) Notice

(1) Before any hearing is conducted pursuant to a request by the United States under subsection (a), the United States shall provide the defendant with notice of the classified information that is at issue. Such notice shall identify the specific classified information at issue whenever that information previously has been made available to the defendant by the United States. When the United States has not previously made the information available to the defendant in connection with the case, the information may be described by generic category, in such form as the court may

approve, rather than by identification of the specific information of concern to the United States.

(2) Whenever the United States requests a hearing under subsection (a), the court, upon request of the defendant, may order the United States to provide the defendant, prior to trial, such details as to the portion of the indictment or information at issue in the hearing as are needed to give the defendant fair notice to prepare for the hearing.

(c) Alternative Procedure for Disclosure of Classified Information

(1) Upon any determination by the court authorizing the disclosure of specific classified information under the procedures established by this section, the United States may move that, in lieu of the disclosure of such specific classified information, the court order—

(A) the substitution for such classified information of a statement admitting relevant facts that the specific classified information would tend to prove; or

(B) the substitution for such classified information of a summary of the specific classified information.

The court shall grant such a motion of the United States if it finds that the statement or summary will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information. The court shall hold a hearing on any motion under this section. Any such hearing shall be held in camera at the request of the Attorney General.

(2) The United States may, in connection with a motion under paragraph (1), submit to the court an affidavit of the Attorney General certifying that disclosure of classified information would cause identifiable damage to the national security of the United States and explaining the basis for the classification of such information. If so requested by the United States, the court shall examine such affidavit in camera and *ex parte*.

(d) Sealing of Records of In Camera Hearings

If at the close of an in camera hearing under this Act (or any portion of a hearing under this Act that is held in camera) the court determines that the classified information at issue may not be disclosed or elicited at the trial or pretrial proceeding, the record of such in camera hearing shall be sealed and preserved by the court for use

in the event of an appeal. The defendant may seek reconsideration of the court's determination prior to or during trial.

(e) Prohibition on Disclosure of Classified Information by Defendant, Relief for Defendant When United States Opposes Disclosure

(1) Whenever the court denies a motion by the United States that it issue an order under subsection (c) and the United States files with the court an affidavit of the Attorney General objecting to disclosure of the classified information at issue, the court shall order that the defendant not disclose or cause the disclosure of such information.

(2) Whenever a defendant is prevented by an order under paragraph (1) from disclosing or causing the disclosure of classified information, the court shall dismiss the indictment or information; except that, when the court determines that the interests of justice would not be served by dismissal of the indictment or information, the court shall order such other action, in lieu of dismissing the indictment or information, as the court determines is appropriate. Such action may include, but need not be limited to—

(A) dismissing specified counts of the indictment or information;

(B) finding against the United States on any issue as to which the excluded classified information relates; or

(C) striking or precluding all or part of the testimony of a witness.

An order under this paragraph shall not take effect until the court has afforded the United States an opportunity to appeal such order under section 7, and thereafter to withdraw its objection to the disclosure of the classified information at issue.

(f) Reciprocity

Whenever the court determines pursuant to subsection (a) that classified information may be disclosed in connection with a trial or pretrial proceeding, the court shall, unless the interests of fairness do not so require, order the United States to provide the defendant with the information it expects to use to rebut the classified information. The court may place the United States under a continuing duty to disclose such rebuttal information. If the United States fails to comply with its obligation under this subsection, the court may exclude any evidence not made the subject of a required

disclosure and may prohibit the examination by the United States of any witness with respect to such information.

§ 7. Interlocutory Appeal

(a) An interlocutory appeal by the United States taken before or after the defendant has been placed in jeopardy shall lie to a court of appeals from a decision or order of a district court in a criminal case authorizing the disclosure of classified information, imposing sanctions for nondisclosure of classified information, or refusing a protective order sought by the United States to prevent the disclosure of classified information.

(b) An appeal taken pursuant to this section either before or during trial shall be expedited by the court of appeals. Prior to trial, an appeal shall be taken within ten days after the decision or order appealed from and the trial shall not commence until the appeal is resolved. If an appeal is taken during trial, the trial court shall adjourn the trial until the appeal is resolved and the court of appeals (1) shall hear argument on such appeal within four days of the adjournment of the trial, (2) may dispense with written briefs other than the supporting materials previously submitted to the trial court, (3) shall render its decision within four days of argument on appeal, and (4) may dispense with the issuance of a written opinion in rendering its decision. Such appeal and decision shall not affect the right of the defendant, in a subsequent appeal from a judgment of conviction, to claim as error reversal by the trial court on remand of a ruling appealed from during trial.

§ 8. Introduction of Classified Information

(a) Classification Status

Writings, recordings, and photographs containing classified information may be admitted into evidence without change in their classification status.

(b) Precautions by Court

The court, in order to prevent unnecessary disclosure of classified information involved in any criminal proceeding, may order admission into evidence of only part of a writing, recording, or photograph, or may order admission into evidence of the whole writing, recording, or photograph with excision of some or all of the

classified information contained therein, unless the whole ought in fairness be considered.

(c) Taking of Testimony

During the examination of a witness in any criminal proceeding, the United States may object to any question or line of inquiry that may require the witness to disclose classified information not previously found to be admissible. Following such an objection, the court shall take such suitable action to determine whether the response is admissible as will safeguard against the compromise of any classified information. Such action may include requiring the United States to provide the court with a proffer of the witness' response to the question or line of inquiry and requiring the defendant to provide the court with a proffer of the nature of the information he seeks to elicit.

§ 9. Security Procedures

(a) Within one hundred and twenty days of the date of the enactment of this Act, the Chief Justice of the United States, in consultation with the Attorney General, the Director of National Intelligence,[97] and the Secretary of Defense, shall prescribe rules establishing procedures for the protection against unauthorized disclosure of any classified information in the custody of the United States district courts, courts of appeal, or Supreme Court. Such rules, and any changes in such rules, shall be submitted to the appropriate committees of Congress and shall become effective forty-five days after such submission.

(b) Until such time as rules under subsection (a) first become effective, the Federal courts shall in each case involving classified information adopt procedures to protect against the unauthorized disclosure of such information.

§ 9A. Coordination Requirements Relating to the Prosecution of Cases Involving Classified Information[98]

(a) Briefings Required.—The Assistant Attorney General for the Criminal Division or the Assistant Attorney General for National Security, as appropriate, and the appropriate United States attorney,

97. "Director of Central Intelligence" replaced by "Director of National Intelligence." P.L. 108-458 (Dec. 17, 2004), 118 Stat. 3691.

98. Section 9A added by P.L. 106-567 (Dec. 27, 2000), 114 Stat. 2855–56.

or the designees of such officials, shall provide briefings to the senior agency official, or the designee of such official, with respect to any case involving classified information that originated in the agency of such senior agency official.

(b) Timing of Briefings.—Briefings under subsection (a) with respect to a case shall occur—

(1) as soon as practicable after the Department of Justice and the United States attorney concerned determine that a prosecution or potential prosecution could result; and

(2) at such other times thereafter as are necessary to keep the senior agency official concerned fully and currently informed of the status of the prosecution.

(c) Senior Agency Official Defined.—In this section, the term "senior agency official" has the meaning given that term in section 1.1 of Executive Order No. 12958.

§ 10. Identification of Information Related to National Defense

In any prosecution in which the United States must establish that material relates to the national defense or constitutes classified information, the United States shall notify the defendant, within the time before trial specified by the court, of the portions of the material that it reasonably expects to rely upon to establish the national defense or classified information element of the offense.

§ 11. Amendments to Act

Sections 1 through 10 of this Act may be amended as provided in section 2076, Title 28, United States Code.

§ 12. Attorney General Guidelines

(a) Within one hundred and eighty days of enactment of this Act, the Attorney General shall issue guidelines specifying the factors to be used by the Department of Justice in rendering a decision whether to prosecute a violation of Federal law in which, in the judgment of the Attorney General, there is a possibility that classified information will be revealed. Such guidelines shall be transmitted to the appropriate committees of Congress.

(b) When the Department of Justice decides not to prosecute a violation of Federal law pursuant to subsection (a), an appropriate official of the Department of Justice shall prepare written findings

detailing the reasons for the decision not to prosecute. The findings shall include—

(1) the intelligence information which the Department of Justice officials believe might be disclosed,

(2) the purpose for which the information might be disclosed,

(3) the probability that the information would be disclosed, and

(4) the possible consequences such disclosure would have on the national security.

§ 13. Reports to Congress

(a) Consistent with applicable authorities and duties, including those conferred by the Constitution upon the executive and legislative branches, the Attorney General shall report orally or in writing semiannually to the Permanent Select Committee on Intelligence of the United States House of Representatives, the Select Committee on Intelligence of the United States Senate, and the chairmen and ranking minority members of the Committees on the Judiciary of the Senate and House of Representatives on all cases where a decision not to prosecute a violation of Federal law pursuant to section 12(a) has been made.

(b) In the case of the semiannual reports (whether oral or written) required to be submitted under subsection (a) to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, the submittal dates for such reports shall be as provided in section 507 of the National Security Act of 1947.[99]

(c) The Attorney General shall deliver to the appropriate committees of Congress a report concerning the operation and effectiveness of this Act and including suggested amendments to this Act. For the first three years this Act is in effect, there shall be a report each year. After three years, such reports shall be delivered as necessary.

99. Subsection (b) added by P.L. 107-306 (Nov. 27, 2002), 116 Stat. 2423.

§ 14. Functions of Attorney General Exercised by Deputy Attorney General, the Associate Attorney General, or Designated Assistant Attorney General

The functions and duties of the Attorney General under this Act may be exercised by the Deputy Attorney General, the Associate Attorney General, or by an Assistant Attorney General designated by the Attorney General for such purpose and may not be delegated to any other official.

§ 15. Effective Date

The provisions of this Act shall become effective upon the date of the enactment of this Act, but shall not apply to any prosecution in which an indictment or information was filed before such date.

§ 16. Short Title

That this Act may be cited as the "Classified Information Procedures Act."

Appendix B

Security Procedures Established Pursuant to PL 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information[100]

1. Purpose. The purpose of these procedures is to meet the requirements of Section 9(a) of the Classified Information Procedures Act of 1980, Pub. L. 96-456, 94 Stat. 2025, which in pertinent part provides that:

> [T]he Chief Justice of the United States, in consultation with the Attorney General, the Director of Central Intelligence, and the Secretary of Defense, shall prescribe rules establishing procedures for the protection against unauthorized disclosure of any classified information in the custody of the United States district courts, courts of appeal, or Supreme Court.

These procedures apply in all proceedings in criminal cases involving classified information, and appeals therefrom, before the United States district courts, the courts of appeal and the Supreme Court.

2. Court Security Officer. In any proceeding in a criminal case or appeal therefrom in which classified information is within, or reasonably expected to be within, the custody of the court, the court shall designate a court security officer. The Attorney General or the Department of Justice Security Officer, with the concurrence of the head of the agency or agencies from which the classified information originates, or their representatives, shall recommend to the court persons qualified to serve as court security officer. The court security officer shall be selected from among those persons so recommended.

The court security officer shall be an individual with demonstrated competence in security matters, and shall, prior to designation, have been certified to the court in writing by the Department of Justice Security Officer as cleared for the level and category of classified information that will be involved. The court security of-

100. 18 U.S.C. app. 3 § 9 note (2000), issued Feb. 12, 1981.

ficer may be an employee of the Executive Branch of the Government detailed to the court for this purpose. One or more alternate court security officers, who have been recommended and cleared in the manner specified above, may be designated by the court as required.

The court security officer shall be responsible to the court for document, physical, personnel and communications security, and shall take measures reasonably necessary to fulfill these responsibilities. The court security officer shall notify the court and the Department of Justice Security Officer of any actual, attempted, or potential violation of security procedures.

3. Secure Quarters. Any in camera proceeding—including a pretrial conference, motion hearing, or appellate hearing—concerning the use, relevance, or admissibility of classified information, shall be held in secure quarters recommended by the court security officer and approved by the court.

The secure quarters shall be located within the Federal courthouse, unless it is determined that none of the quarters available in the courthouse meets, or can reasonably be made equivalent to, security requirements of the Executive Branch applicable to the level and category of classified information involved. In that event, the court shall designate the facilities of another United States Government agency, recommended by the court security officer, which is located within the vicinity of the courthouse, as the site of the proceedings.

The court security officer shall make necessary arrangements to ensure that the applicable Executive Branch standards are met and shall conduct or arrange for such inspection of the quarters as may be necessary. The court security officer shall, in consultation with the United States Marshal, arrange for the installation of security devices and take such other measures as may be necessary to protect against any unauthorized access to classified information. All of the aforementioned activity shall be conducted in a manner which does not interfere with the orderly proceedings of the court. Prior to any hearing or other proceeding, the court security officer shall certify in writing to the court that the quarters are secure.

4. Personnel Security—Court Personnel. No person appointed by the court or designated for service therein shall be given access to any classified information in the custody of the court, unless such person has received a security clearance as provided herein

and unless access to such information is necessary for the performance of an official function. A security clearance for justices and judges is not required, but such clearance shall be provided upon the request of any judicial officer who desires to be cleared.

The court shall inform the court security officer or the attorney for the government of the names of court personnel who may require access to classified information. That person shall then notify the Department of Justice Security Officer, who shall promptly make arrangements to obtain any necessary security clearances and shall approve such clearances under standards of the Executive Branch applicable to the level and category of classified information involved. The Department of Justice Security Officer shall advise the court in writing when the necessary security clearances have been obtained.

If security clearances cannot be obtained promptly, personnel in the Executive Branch having the necessary clearances may be temporarily assigned to assist the court. If a proceeding is required to be recorded and an official court reporter having the necessary security clearance is unavailable, the court may request the court security officer or the attorney for the government to have a cleared reporter from the Executive Branch designated to act as reporter in the proceedings. The reporter so designated shall take the oath of office as prescribed by 28 U.S.C. § 753(a).

Justices, judges and cleared court personnel shall not disclose classified information to anyone who does not have a security clearance and who does not require the information in the discharge of an official function. However, nothing contained in these procedures shall preclude a judge from discharging his official duties, including giving appropriate instructions to the jury.

Any problem of security involving court personnel or persons acting for the court shall be referred to the court for appropriate action.

5. Persons Acting for the Defendant. The government may obtain information by any lawful means concerning the trustworthiness of persons associated with the defense and may bring such information to the attention of the court for the court's consideration in framing an appropriate protective order pursuant to Section 3 of the Act.

6. Jury. Nothing contained in these procedures shall be construed to require an investigation or security clearance of the mem-

bers of the jury or interfere with the functions of a jury, including access to classified information introduced as evidence in the trial of a case.

After a verdict has been rendered by a jury, the trial judge should consider a government request for a cautionary instruction to jurors regarding the release or disclosure of classified information contained in documents they have reviewed during the trial.

7. Custody and Storage of Classified Materials.

a. Materials Covered. These security procedures apply to all papers, documents, motions, pleadings, briefs, notes, records of statements involving classified information, notes relating to classified information taken during in camera proceedings, orders, affidavits, transcripts, untranscribed notes of a court reporter, magnetic recordings, or any other submissions or records which contain classified information as the term is defined in Section 1(a) of the Act, and which are in the custody of the court. This includes, but is not limited to (1) any motion made in connection with a pretrial conference held pursuant to Section 2 of the Act, (2) written statements submitted by the United States pursuant to Section 4 of the Act, (3) any written statement or written notice submitted to the court by the defendant pursuant to Section 5(a) of the Act, (4) any petition or written motion made pursuant to Section 6 of the Act, (5) any description of, or reference to, classified information contained in papers filed in an appeal, pursuant to Section 7 of the Act and (6) any written statement provided by the United States or by the defendant pursuant to Section 8(c) of the Act.

b. Safekeeping. Classified information submitted to the court shall be placed in the custody of the court security officer who shall be responsible for its safekeeping. When not in use, the court security officer shall store all classified materials in a safe or safe-type steel file container with built-in, dial-type, three position, changeable combinations which conform to the General Services Administration standards for security containers. Classified information shall be segregated from other information unrelated to the case at hand by securing it in a separate security container. If the court does not possess a storage container which meets the required standards, the necessary storage container or containers are to be supplied to the court on a temporary basis by the appropriate Executive

Branch agency as determined by the Department of Justice Security Officer. Only the court security officer and alternate court security officer(s) shall have access to the combination and the contents of the container unless the court, after consultation with the security officer, determines that a cleared person other than the court security officer may also have access.

For other than temporary storage (e.g., brief court recess), the court security officer shall insure that the storage area in which these containers shall be located meets Executive Branch standards applicable to the level and category of classified information involved. The secure storage area may be located within either the Federal courthouse or the facilities of another United States Government agency.

c. Transmittal of Classified Information. During the pendency of a trial or appeal, classified materials stored in the facilities of another United States Government agency shall be transmitted in the manner prescribed by the Executive Branch security regulations applicable to the level and category of classified information involved. A trust receipt shall accompany all classified materials transmitted and shall be signed by the recipient and returned to the court security officer.

8. Operating Routine.

a. Access to Court Records. Court personnel shall have access to court records only as authorized. Access to classified information by court personnel shall be limited to the minimum number of cleared persons necessary for operating purposes. Access includes presence at an in camera hearing or any other proceeding during which classified information may be disclosed. Arrangements for access to classified information in the custody of the court by court personnel and persons acting for the defense shall be approved in advance by the court, which may issue a protective order concerning such access.

Except as otherwise authorized by a protective order, persons acting for the defendant will not be given custody of classified information provided by the government. They may, at the discretion of the court, be afforded access to classified information provided by the government in secure quarters which have been approved in accordance with § 3 of these

procedures, but such classified information shall remain in the control of the court security officer.

b. Telephone Security. Classified information shall not be discussed over standard commercial telephone instruments or office intercommunication systems.

c. Disposal of Classified Material. The court security officer shall be responsible for the secure disposal of all classified materials which are not otherwise required to be retained.

9. Records Security.

a. Classification Markings. The court security officer, after consultation with the attorney for the government, shall be responsible for the marking of all court documents containing classified information with the appropriate level of classification and for indicating thereon any special access controls that also appear on the face of the document from which the classified information was obtained or that are otherwise applicable.

Every document filed by the defendant in the case shall be filed under seal and promptly turned over to the court security officer. The court security officer shall promptly examine the document and, in consultation with the attorney for the government or representative of the appropriate agency, determine whether it contains classified information. If it is determined that the document does contain classified information, the court security officer shall ensure that it is marked with the appropriate classification marking. If it is determined that the document does not contain classified information, it shall be unsealed and placed in the public record. Upon the request of the government, the court may direct that any document containing classified information shall thereafter be protected in accordance with § 7 of these procedures.

b. Accountability System. The court security officer shall be responsible for the establishment and maintenance of a control and accountability system for all classified information received by or transmitted from the court.

10. Transmittal of the Record on Appeal. The record on appeal, or any portion thereof, which contains classified information shall be transmitted to the court of appeals or to the Supreme Court in the manner specified in § 7(c) of these procedures.

11. Final Disposition. Within a reasonable time after all proceedings in the case have been concluded, including appeals, the court shall release to the court security officer all materials containing classified information. The court security officer shall then transmit them to the Department of Justice Security Officer who shall consult with the originating agency to determine the appropriate disposition of such materials. Upon the motion of the government, the court may order the return of the classified documents and materials to the department or agency which originated them. The materials shall be transmitted in the manner specified in § 7(c) of these procedures and shall be accompanied by the appropriate accountability records required by § 9(b) of these procedures.

12. Expenses. Expenses of the United States Government which arise in connection with the implementation of these procedures shall be borne by the Department of Justice or other appropriate Executive Branch agency.

13. Interpretation. Any question concerning the interpretation of any security requirement contained in these procedures shall be resolved by the court in consultation with the Department of Justice Security Officer and the appropriate Executive Branch agency security officer.

14. Term. These procedures shall remain in effect until modified in writing by The Chief Justice after consultation with the Attorney General of the United States, the Director of Central Intelligence, and the Secretary of Defense.

15. Effective Date. These procedures shall become effective forty-five days after the date of submission to the appropriate Congressional Committees, as required by the Act.

Issued this 12th day of February, 1981, after taking into account the views of the Attorney General of the United States, the Director of Central Intelligence, and the Secretary of Defense, as required by law.

Warren E. Burger
Chief Justice of the United States

The Federal Judicial Center

Board

The Chief Justice of the United States, *Chair*
Judge David O. Carter, U.S. District Court for the Central District of California
Judge Bernice B. Donald, U.S. District Court for the Western District of Tennessee
Judge Terence T. Evans, U.S. Court of Appeals for the Seventh Circuit
Magistrate Judge Karen Klein, U.S. District Court for the District of North Dakota
Judge Philip M. Pro, U.S. District Court for the District of Nevada
Judge Stephen Raslavich, U.S. Bankruptcy Court for the Eastern District of Pennsylvania
Judge William Traxler Jr., U.S. Court of Appeals for the Fourth Circuit
James C. Duff, Director of the Administrative Office of the U.S. Courts

Director

Judge Barbara J. Rothstein

Deputy Director

John S. Cooke

About the Federal Judicial Center

The Federal Judicial Center is the research and education agency of the federal judicial system. It was established by Congress in 1967 (28 U.S.C. §§ 620–629), on the recommendation of the Judicial Conference of the United States.

By statute, the Chief Justice of the United States chairs the Center's Board, which also includes the director of the Administrative Office of the U.S. Courts and seven judges elected by the Judicial Conference.

The organization of the Center reflects its primary statutory mandates. The Education Division plans and produces education and training programs for judges and court staff, including satellite broadcasts, video programs, publications, curriculum packages for in-court training, and Web-based programs and resources. The Research Division examines and evaluates current and alternative federal court practices and policies. This research assists Judicial Conference committees, who request most Center research, in developing policy recommendations. The Center's research also contributes substantially to its educational programs. The two divisions work closely with two units of the Director's Office—the Systems Innovations & Development Office and Communications Policy & Design Office—in using print, broadcast, and online media to deliver education and training and to disseminate the results of Center research. The Federal Judicial History Office helps courts and others study and preserve federal judicial history. The International Judicial Relations Office provides information to judicial and legal officials from foreign countries and assesses how to inform federal judicial personnel of developments in international law and other court systems that may affect their work.