
No. 13-30077
[NO. CR12-119MJP, USDC, W.D. Washington]

**IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

MICHAEL ALLAN DREYER,

Defendant-Appellant.

**CORRECTED ANSWERING BRIEF OF THE
UNITED STATES**

Appeal from the United States District Court
for the Western District of Washington at Seattle
The Honorable Marsha J. Pechman
United States District Judge

JENNY A. DURKAN
United States Attorney
Western District of Washington

MARCI ELLSWORTH
Assistant United States Attorney
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
Telephone: 253-428-3800

TABLE OF CONTENTS

Table Of Authorities.....iii

PRELIMINARY STATEMENT AND
SUMMARY OF ARGUMENT.....1

ISSUES ON APPEAL.....3

 A. Was the posse comitatus act violated where
 a Special Agent of the Naval Criminal Investigative
 Service, who is a civilian employee of the navy,
 conducted the investigation identifying the
 defendant as a person who distributed child
 pornography on a peer-to-peer file-sharing
 network?.....3

 B. Did the district court properly find the
 affidavit supporting a state search warrant
 stated probable cause after the misstatements
 were excised and omissions considered?.....3

 C. Where the state warrant authorized a search
 of electronic storage media for child pornography,
 was the warrant sufficiently particularized so
 that it did not constitute a general warrant?.....3

 1. Where the law enforcement officers
 conducted a forensic preview of the contents
 of the computer at the defendant’s home,
 did the officers exceed the scope of the warrant?.....3

 D. Did the federal warrant that was based, in part,
 on the evidence obtained during the execution
 of the state warrant, constitute fruits of a prior
 unlawful search?.....4

E.	Did the district court abuse its discretion when it denied a request for a <i>Daubert</i> hearing regarding the reliability of the tool used by the Naval Criminal Investigative Service to identify the defendant as a distributor of child pornography where the reliability of this tool was established through the evidence obtained, and verified by the subsequent search?.....	4
STATEMENT OF JURISDICTION.....		4
STATEMENT OF THE CASE.....		5
I.	Statement Of Procedure.....	5
II.	Statement Of Revelant Facts	7
A.	The Identification Of Dreyer As An Individual Distributing Child Pornography Using The Internet	7
B.	The Search Of Dreyer’s Residence And Initial Discovery Of Child Pornography On Dreyer’s Computer.....	12
C.	The Full Forensic Examination Of Dreyer’s Computer And Discovery Of Evidence Of The Distribution And Possession Of Child Pornography	15
D.	The District Court’s Findings Following The <i>Franks</i> Hearing.....	17
ARGUMENT.....		19

I.	The Naval Criminal Investigative Service's Identification Of Dreyer As An Individual Distributing Child Pornography Over The Internet Did Not Violate The Posse Comitatus Act.....	19
A.	Standard Of Review.....	20
B.	The Posse Comitatus Act Was Not Violated	20
C.	Because The Naval Criminal Investigative Service Is A Civilian Law Enforcement Agency, With No Direct Reporting Relationship To Any Military Officer, The Provisions Of The Posse Comitatus Act Do Not Apply To Civilian Special Agents Of The Naval Criminal Investigative Service In The Execution Of Their Duties As Sworn Law Enforcement Officers	21
D.	The Posse Comitatus Act Prohibits Only The Direct Involvement Of Military Personnel In Civilian Law Enforcement, Not The Indirect Assistance Of Military Personnel	25
E.	Even If The Posse Comitatus Act Applies, The Suppression Of Evidence Is Not Available As Remedy Under The Posse Comitatus Act	29
II.	The Trial Judge Correctly Found There Was Probable Cause To Believe Evidence Of The Distribution And Possession Of Child Pornography Would Be Found At Dreyer's Residence	32
A.	Standard Of Review	33

B.	The Affidavit In Support Of The State Search Warrant Demonstrated Probable Cause To Search Dreyer’s Residence For Evidence Of Child Pornography	33
III.	The State Search Warrant Was Not A General Warrant, And Officers Did Not Exceed The Scope Of The Warrant In Executing Their Search Of Dreyer’s Residence	38
A.	The Standard Of Review	38
B.	The Scope Of The Particularized State Warrant Was Not Exceeded.....	38
C.	The Affidavit In Support Of The Federal Search Warrant Demonstrated Probable Cause To Search The Computers Seized From Dreyer’s Residence For Evidence Of Child Pornography	43
IV.	The District Court Did Not Abuse Its Discretion When It Denied Dreyer’s Motion In Limine To Exclude Evidence Obtained Through The Use Of The Roundup Software Program	45
A.	Standard Of Review	45
B.	The District Court Properly Concluded A <i>Daubert</i> Hearing Was Not Required Before The Roundup Evidence Could Be Introduced	46
CONCLUSION		51

TABLE OF AUTHORITIES

Federal Cases

<i>Andresen v. Maryland</i> , 427 U.S. 463 (1976).....	43
<i>Daubert v. Merrell Dow Pharmacueticals, Inc.</i> , 509 U.S. 579 (1993).....	46, 56
<i>Franks v. Delaware</i> , 438 U.S. 154 (1978).....	6, 34
<i>Gilbert v. United States</i> , 165 F.3d 470 (6th Cir. 1999).....	30
<i>United States v. Gourde</i> , 440 F.3d 1065 (9 th Cir. 2006)	34
<i>Hayes v. Hawes</i> , 921 F.2d 100 (7th Cir. 1990).....	27, 28
<i>Illinois v. Gates</i> , 462 U.S. 213 (1983).....	34, 37
<i>Kumho Tire Co. v. Carmichael</i> , 526 U.S. 137 (1999).....	46, 37, 50
<i>Maryland v. Pringle</i> , 540 U.S. 366 (2003).....	33

<i>Safford Unified School Dist. No. 1 v. Redding</i> , 557 U.S. 364 (2009).....	33
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979).....	31
<i>United States v. Adjani</i> , 452 F.3d 1140 (9th Cir. 2006).....	39, 41
<i>United States v. Alatorre</i> , 222 F.3d 1098 (9th Cir. 2000).....	48
<i>United States v. Bacon</i> , 851 F.2d 1312 (11th Cir. 1988).....	26
<i>United States v. Barajas-Avalos</i> , 377 F.3d 1040 (9th Cir. 2004).....	44
<i>United States v. Berisford</i> , 750 F.2d 57 (10th Cir. 1984).....	36
<i>United States v. Borowy</i> , 595 F.3d 1045 (9th Cir. 2010).....	31
<i>United States v. Brobst</i> , 558 F.3d 982 (9th Cir. 2009).....	38
<i>United States v. Chiaradio</i> , 684 F.3d 265 (1st Cir. 2012)	47, 48
<i>United States v. Chon</i> , 210 F.3d 990 (9th Cir. 2000).....	passim

<i>United States v. Christie</i> , 624 F.3d 558 (3rd Cir. 2010).....	31
<i>United States v. Comprehensive Drug Testing, Inc.</i> , 579 F.3d 989 (9th Cir. 2009).....	41
<i>United States v. Elliott</i> , 322 F.3d 710 (9th Cir. 2003).....	33
<i>United States v. Flores-Montano</i> , 424 F.3d 1044 (9th Cir. 2005).....	40
<i>United States v. Forrester</i> , 512 F.3d 500 (9th Cir. 2008).....	31
<i>United States v. Ganoë</i> , 538 F.3d 1117 (9th Cir. 2008).....	31
<i>United States v. Gonzales</i> , 307 F.3d 906 (9th Cir. 2002).....	45
<i>United States v. Grubbs</i> , 547 U.S. 90 (2006).....	39
<i>United States v. Hall</i> , 113 F.3d 157 (9th Cir. 1997).....	35
<i>United States v. Hankey</i> , 203 F.2d 1160 (9th Cir. 2000).....	54

<i>United States v. Harrington</i> , 681 F.2d 612 (9th Cir. 1982)	30
<i>United States v. Hill</i> , 459 F.3d 966 (9th Cir. 2006)	40
<i>United States v. Hitchcock</i> , 286 F.3d 1064 (9th Cir. 2002)	20, 25, 26
<i>United States v. Holloway</i> , 2011 WL 304580 (W.D. Ky. 2011),	26
<i>United States v. Jawara</i> , 474 F.3d 565 (9th Cir. 2007)	51
<i>United States v. Johnson</i> , 410 F.3d 137 (4th Cir. 2005)	29,
<i>United States v. Kelley</i> , 482 F.3d 1047 (9th Cir. 2003)	34, 37, 45
<i>United States v. Lauder</i> , 409 F.3d 1254 (10th Cir. 2005)	47
<i>United States v. Lingenfelter</i> , 997 F.2d 632 (9th Cir. 1993)	36
<i>United States v. Maddox</i> , 614 F.3d 1046 (9th Cir. 2010)	38
<i>United States v. Martinez-Garcia</i> , 397 F.3d 1205 (9th Cir. 2005)	34, 35

<i>United States v. Meek</i> , 366 F.3d 705 (9th Cir. 2004).....	41
<i>United States v. Mullins</i> , 178 F.3d 334 (5th Cir. 1999).....	29
<i>United States v. Roberts</i> , 779 F.2d 565 (9th Cir. 1986).....	29, 31, 32
<i>United States v. Ross</i> , 456 U.S. 798 (1982).....	39
<i>United States v. Schesso</i> , _ F.3d _, 2013 WL 5227071 (9th Cir. Sept. 18, 2013)	41, 42, 45
<i>United States v. Shi</i> , 525 F.3d 709 (9th Cir. 2008).....	39
<i>United States v. Smith</i> , 196 F.3d 1034 (9th Cir. 1999).....	30
<i>United States v. Tamura</i> , 694 F.2d 591 (9th Cir. 1982).....	41
<i>United States v. Walden</i> , 490 F.2d 372 (4th Cir. 1974).....	30
Federal Statutes	
Title 10, United States Code, Section 375.....	21

Section 1585a21

Section 501323

Section 7480(c)22

Title 18, United States Code,

Section 375	23
Section 1385	passim
Section 2252(a)(2)	3, 4
Section 2252(a)(4)(B)	3, 4
Section 3231	3
Section 3486	4

Title 28, United States Code

Section 1291	3
--------------------	---

**PRELIMINARY STATEMENT AND
SUMMARY OF ARGUMENT**

With this appeal, Defendant-Appellant Michael Allen Dreyer seeks reversal of his convictions for distribution and possession of child pornography. He argues that because he was identified as a person distributing child pornography on a peer-to-peer computer network as the result of an investigation by a Naval Criminal Investigative Service (“NCIS”) Special Agent, the evidence developed as a result of that investigation should be suppressed. Specifically, he claims suppression is required because the agent’s actions violated the Posse Comitatus Act, 18 U.S.C. § 1385. That argument fails, however, because NCIS agents are federal law enforcement officers who are civilian employees of the Navy. They report to civilians and not military commanders. Moreover, even if the agent’s conduct was within the statute’s reach, the agent’s investigation had a purpose related to the military and, thereafter, he only provided indirect assistance to civilian law enforcement referring the information developed during his investigation to other law enforcement officers for further investigation. Thus, there was no basis to suppress the resulting evidence.

The defense also argues that evidence from a subsequent state search should have been suppressed because of the misstatements contained in, and omissions from, the affidavit in support of that warrant. But as the district court correctly found after a *Franks* hearing, even after excising the misstatements and adding the omissions about which the defense complains, the affidavit still states probable cause. Moreover, because the affidavit makes clear the evidence forming the basis for the warrant was not obtained through the affiant's investigation, and correctly details the source of the evidence, the misstatements, although very sloppy, were not material.

Dreyer's other claims also lack merit. He argues the state search warrant was executed in an overboard manner because the agents conducted a forensic preview of the computer at Dreyer's residence. This practice, however, was contemplated in the supporting affidavit to ensure that the items taken for further off-site search actually contained child pornography. Dreyer also argues the warrant was a general warrant because it lacked a search protocol. But this court has never concluded a search protocol is required to particularize a warrant.

Finally, the defense argues the district court abused its discretion by failing to hold a *Daubert* hearing on the reliability of the software program used by the NCIS agent to identify Dreyer as an individual offering child pornography for download on a peer-to-peer file sharing program. This program, however, operated precisely as designed and identified files containing child pornography offered on the peer-to-peer site. The existence of those files on Dreyer's computer was verified in the subsequent search. Thus, the district court was not required to hold a *Daubert* hearing, and in any event, any error was harmless.

ISSUES ON APPEAL

- A. Was the Posse Comitatus Act violated where a Special Agent of the Naval Criminal Investigative Service, who is a civilian employee of the Navy, conducted the investigation identifying the defendant as a person who distributed child pornography on a peer-to-peer file-sharing network?
- B. Did the district court properly find the affidavit supporting a state search warrant stated probable cause after the misstatements were excised and omissions considered?
- C. Where the state warrant authorized a search of electronic storage media for child pornography, was the warrant sufficiently particularized so that it did not constitute a general warrant?
 1. Where the law enforcement officers conducted a forensic preview of the contents of the computer at the defendant's home, did the officers exceed the scope of the warrant?

- D. Did the federal warrant that was based, in part, on the evidence obtained during the execution of the state warrant, constitute fruits of a prior unlawful search?
- E. Did the district court abuse its discretion when it denied a request for a *Daubert* hearing regarding the reliability of the tool used by the Naval Criminal Investigative Service to identify the defendant as a distributor of child pornography where the reliability of this tool was established through the evidence obtained, and verified by the subsequent search?

STATEMENT OF JURISDICTION

Michael Allen Dreyer appeals his convictions, following a jury trial, for distribution of child pornography, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1), and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2). The district court had jurisdiction pursuant to 18 U.S.C. § 3231, and this Court has jurisdiction pursuant to 28 U.S.C. § 1291.

The district court imposed sentence on March 14, 2013, CR 120, and the judgment was entered on March 15, 2013. CR122; ER 70-75.¹ The defense filed a timely notice of appeal on March 22, 2013. CR125;ER 68.

¹ “CR_” refers, by docket entry number, to the district court clerk’s docket; and “ER_” refers, by page number to the Appellant’s Excerpts of Record.

BAIL STATUS OF THE DEFENDANT

Dreyer is currently serving the 216-month sentence imposed by the district court. His projected release date is December 8, 2027.

STATEMENT OF THE CASE

I. Statement of Procedure

On May 3, 2012, Michael Allen Dreyer was charged by Indictment with one count of distribution of child pornography, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1), and one count of possession of child pornography, in violation of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2).

CR 11; ER 482-484. Thereafter, Dreyer moved to suppress the evidence seized during execution of a state search warrant at his residence on July 6, 2011, and evidence found on his computer during a subsequent search of that computer pursuant to a federal search warrant. CR 17, 18. Among other things, the defense argued the administrative subpoena used to obtain Dreyer's subscriber information did not comply with the requirements of 18 U.S.C. § 3486,² and that there was insufficient probable cause to support issuance of a warrant. CR 17, 18.

² Dreyer has abandoned that claim in this appeal so that claim is now waived.

Dreyer also requested a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), alleging the affidavit in support of the state search warrant contained intentionally or recklessly false statements and misleading omissions which were then incorporated into the affidavit supporting the federal search warrant. CR 18, 20; ER 496.

In his reply brief in the district court, the defense suggested, for the first time, that the Navy Criminal Investigative Service Agent whose initial investigation led to the searches of Dreyer's residence and computer did not have the lawful authority to investigate child pornography offenses. CR 25 at 6. The only support provided for this one sentence assertion was a citation to the Posse Comitatus Act, 18 U.S.C. § 1385. CR 25 at 6. Nonetheless, the government filed a surreply brief addressing this issue. CR 31.

Thereafter, the district court held a two-day evidentiary hearing regarding these motions. CR 34, 43. At the conclusion of the hearing,

the court denied Dreyer's motions to suppress the evidence from the searches.³ ER 60-65.

Prior to trial, by way of a pretrial motion in limine, Dryer sought to exclude the electronic data obtained through use of the RoundUp software program. CR 68-70. Following briefing from the government, CR 72, the district court denied that motion.

On September 27, 2012, after a four-day trial, the jury returned a verdict of guilty on both counts. ER 76.

II. Statement Of Revelant Facts

A. The Identification of Dreyer as an Individual Distributing Child Pornography Using the Internet.

The investigation leading to Dreyer's prosecution began with an investigation by Naval Criminal Investigative Service ("NCIS") Special Agent Steve Logan. Agent Logan is a civilian employee of the

³ The defense also argued that there was insufficient probable cause to arrest him without a warrant, CR 17, 19; ER 496, and sought suppression of the statements Dreyer made to the officers who were driving him back to his house where the search was being conduct. The United States conceded these statements were inadmissible in its case-in-chief. The district court suppressed the statements, but found the statements could be used to impeach Dreyer if he testified in a manner contrary to those statements at trial. ER 60-65.

Department of the Navy. ER 111-12, 357. As a credentialed federal agent, Agent Logan's duties included conducting investigation of federal crimes and crimes in violation of the Uniform Code of Military Justice (UCMJ). ER 112. Possession and distribution of child pornography are crimes under both the UCMJ and federal law. ER 361.

On April 14, 2011, Agent Logan used a law enforcement investigative software tool called "RoundUp," to look for individuals using computers to share child pornography over the Internet on peer-to-peer file-sharing programs. ER 336-37, 346, 369-70. RoundUp is a web-based computer software program developed by the University of Massachusetts at Amherst for use by Internet Crimes Against Children Task Forces to investigate such offenses. ER 173, 338, 382. The program identifies computers using peer-to-peer networks to trade child pornography over the Internet. ER 114, 146, 173. To conduct an investigation using this software program, Agent Logan first would log-in using his unique access information, and then set the geographic search parameters in the program. ER 338-39. On April 14, 2011, the geographic parameter was Washington State. ER 338-39. Agent Logan

then entered particular search terms indicative of files containing child pornography. ER 344.

The RoundUp software program operates by first identifying and providing a list of the Internet Protocol (“IP”) addresses corresponding to computers on the particular peer-to-peer file sharing network with files available for sharing containing these particular search terms in the titles. ER 119. The RoundUp software program then takes the identified files and compares the hash values for these identified image files against databases maintained both by RoundUp and by the National Center for Missing and Exploited Children of the hash values for known child pornography images.⁴ ER 126-27. If the files identified through the search have hash values identical to hash values in the databases, the RoundUp software displays the file in red, indicating the file contains a known child pornography image. ER 31-32.

⁴ A hash value is a unique numerical identifier assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm. So long as there is no alteration in the file, the hash value for the film or image will remain the same even if a different name is attached to the file when saved to different storage devices. ER 125-26.

On April 14, 2011, Agent Logan observed a computer at IP address 67.160.77.21 (the “Target IP address”), making files of child pornography available over the Internet. ER 348-49, 371. Agent Logan established a direct connection with the computer at the Target IP address, and downloaded three files — two images and one video — which RoundUp identified in red as containing child pornography. ER 344, 349-52. All three files depicted naked females who appeared to Agent Logan to be minors. ER 350-53. One of the three files, a three-minute and nineteen-second video, depicted an adult male digitally penetrating the vagina of a naked prepubescent female child. ER 352.

Agent Logan then submitted a request for an administrative subpoena to the NCIS liaison at the National Center for Missing and Exploited Children. ER 139, 353. The purpose of the subpoena was to request subscriber information for the IP address at the date and time that Agent Logan downloaded the three child pornography files. ER 140, 354. The NCIS liaison passed the request to the FBI, which then sent an administrative subpoena to Comcast. ER 140, 354. From the response to the administrative subpoena, Agent Logan learned that

at the date and time of the download, the Target IP address had been assigned to Michael Dreyer.⁵ ER 142, 354.

Agent Logan also learned Dreyer's residential address, and then conducted a database check to see if Dreyer was affiliated with the military. ER 355. Because Agent Logan's investigation was focused on computers sharing child pornography over the Internet, before learning the identity of the subscriber to whom an IP address is assigned at a particular date and time, there is no way to know who is sharing the child pornography, or whether that individual is on active duty in the military. ER 361-62. From his database check, Agent Logan learned Dreyer had retired from the United States Air Force, and had a residence address in Washington. ER 355-56. Agent Logan then completed his report of investigation and referred the matter to the NCIS offices in Washington State. ER 356. Agent Logan had no further involvement in the investigation of Dreyer thereafter. ER 356.

⁵ In 2000, Dreyer was convicted in the Western District of Washington for possession of child pornography. *See* CR 71.

B. The Search of Dreyer's Residence and Initial Discovery of Child Pornography on Dreyer's Computer.

On May 25, 2011, an NCIS special agent in Washington State called Algona Police Department Detective James Schrimpscher to refer the Dreyer investigation to him. ER 387. Schrimpscher verified that Dreyer lived in Algona, and reviewed Agent Logan's investigative report. ER 388-90. Schrimpscher then contacted the local Internet Crimes Against Children ("ICAC") Task Force for assistance, and spoke with a Seattle Police Detective who had been on the ICAC Task Force for almost five years and had participated in at least 100 investigations related to child sexual exploitation. ER 227-28, 390. Schrimpscher testified that he contacted this detective about the referral of the information regarding Dreyer because this was Schrimpscher's first case involving child pornography and the Internet. ER 390. At Schrimpscher's request, that detective reviewed Agent Logan's investigative report, ER 229-30, and confirmed possession of the files as described in the reports constituted violations of state law. ER 390. The detective then provided Schrimpscher with a template to use in preparing a search warrant. ER 231.

Schrimpscher prepared his affidavit and application for a search warrant for Dreyer's residence by cutting and pasting from the template provided to him without any alteration to the background section. ER 231. For example, Schrimpscher's affidavit contained recitations about a software program called "E-Phex" and information stating that he, as the affiant, had conducted the investigation of Dreyer using "E-Phex." ER 281-83. Nonetheless, Schrimpscher had not used this program at any time. ER 424-25.

In the section on the investigation, Schrimpscher's affidavit outlines the fact that he had been contacted about Dreyer by an NCIS agent, and that the investigation of Dreyer had been conducted by that agent, that is, Agent Logan. ER 284. Schrimpscher's affidavit then incorporates Agent Logan's investigative report as an addendum, making it clear that Agent Logan had conducted the investigation on which the affidavit was based. ER 285, 295-335, 395, 425-26.

As a part of his preparation and consistent with his department's policy, Schrimpscher contacted a King County prosecutor, who reviewed the warrant application and approved it before the application was submitted to a State court judge. ER 391-92, 394. Before issuing the

warrant, the judge made a few handwritten changes to the face sheet of the warrant application, and asked Schrimpscher a question about specific information contained in Agent Logan's appended report. ER 394-95.

The warrant was executed July 6, 2011. ER 396-98. Seattle Police Detective Timothy Luckie, a computer forensics examiner, assisted with the execution. ER 252. Inside Dreyer's residence, Luckie found a computer that was powered up and running. ER 252-53. Before taking any action, Luckie photographed the computer system to document the scene, and then began an onsite preliminary forensic preview of the computer using the "TUX4N6" software program. ER 253-54. TUX4N6 is a forensic preview tool which allows the examiner to look at data stored on a computer hard drive without altering any of the original data on the hard drive. ER 250-51. Using an automated search function, TUX4N6 searched the "Michael Dreyer" user profile on the computer for any image files. ER 256-57, 267. The automatic search process took approximately fourteen minutes. ER 266. During the automatic search process, Luckie was able to review thumbnails of the images as they were identified by the

TUX4N6 forensic preview tool. ER 269. Once Luckie saw images of suspected child pornography, he notified the investigative team of his findings, and shut down the TUX4N6 program and the computer.

ER258. The computer and several other digital storage devices were seized consistent with the warrant. ER 258-59. Aside from the onsite preview using the TUX4N6 forensic preview tool, Luckie did not examine the computer further. ER 260.

While the search of Dreyer's residence was on-going, Schrimpsheer and another officer went to find Dreyer at a food bank where he was volunteering. ER 397-98. When the officers found Dreyer, they told him that police were executing a search warrant at his home and that he needed to accompany them back to this residence. ER 400. During the drive back to the house in the officer's truck, and without advising Dreyer of his *Miranda* rights, Dreyer was asked a series of questions. ER 401-02. After initially stating that he wanted a quiet ride, ER 402, Dreyer made a series of statements that were later suppressed by the district court. In particular, Dreyer admitted that child pornography would be on his computer. ER 106-07.

C. The Full Forensic Examination of Dreyer's Computer and Discovery of Evidence of the Distribution and Possession of Child Pornography.

On December 1, 2011, Homeland Security Investigations Special Agent Dan Huynh presented an application for federal search warrant to search the computer and digital devices seized from Dreyer's residence on July 6, 2011. ER 455-58. The application sought a warrant to search these items for evidence of the federal crimes of receipt, possession, and distribution of child pornography. ER 455-58. Agent Huynh's affidavit incorporated information from Agent Logan's original investigation identifying Dreyer as an individual distributing child pornography over the Internet, ER 462-63, the statements Dreyer made on the date the state search warrant was executed, ER 464-65, and the discovery of child pornography on a computer found during the forensic preview of the computer at Dreyer's residence, ER 465-66. The warrant was issued, ER 455, and the resulting full forensic examination of the computer uncovered more than 20 video files containing child pornography as well as more than 1,300 image files of child pornography and included the three files Agent Logan had downloaded. ER 488, 492-93; RT9/25 at 109-113. The examination also uncovered

evidence of the installation of a peer-to-peer file-sharing program.

ER 488, 492-93.

D. The District Court's Findings Following the Franks Hearing.

The district court granted the defense request for a *Franks* hearing but at the end of the hearing, denied the defense motion to suppress. In its findings of fact, the court noted that although the affidavit Schrimpsheer had prepared included an outline of his background as a law enforcement officer, he failed to include the fact that this was his first affidavit for a search warrant in a child pornography case. ER 61. The court also found Schrimpsheer “made an error and cut and pasted much of the background information,” from the template he received from the Seattle Police detective under the heading called “your affiant,” and that Schrimpsheer was not the person with the background and information on how computers work as described. ER 61. Nonetheless, the court found Schrimpsheer had correctly outlined in the affidavit the steps he had taken during his investigation and that he had also attached Agent Logan’s report to the affidavit. ER 61-62. That report contained a description of the images

Agent Logan had viewed, establishing that the images involved minors engaging in sexual activity. ER 61-62. The court found the reviewing judge had an opportunity to review and evaluate both Agent Logan's report and Schrimpsheer's affidavit, and to question Schrimpsheer about his work after he was sworn. ER 62.

The district court then found that even if the background section of the affidavit was stricken and Schrimpsheer had included a statement indicating that this was his first affidavit for a search warrant in a child pornography case, the remaining material was sufficient to establish probable cause. ER 62. As a result, the court denied the motion. ER 60.

The court also denied the motion to suppress the evidence obtained from the federal search warrant finding there was "nothing wrong" with the subpoena issued by the FBI to obtain the subscriber information for the IP address identified as a result of Agent Logan's investigation. ER 64. The court noted that there was nothing "unusual or inappropriate" in the actions taken by Agent Logan in referring the result of his investigation to others. ER 64. The court also noted that there was nothing in the record to suggest Detective Luckie had used

any information obtained during the inappropriate questioning of Dreyer in conducting his preliminary search of the computer. ER 64-65. Moreover, because of the search was being conducted pursuant to the warrant, it was inevitable that if there was child pornography on the computer, it would be found. ER 65.

ARGUMENT

I. The Naval Criminal Investigative Service's Identification Of Dreyer As An Individual Distributing Child Pornography Over The Internet Did Not Violate The Posse Comitatus Act.

The first issue raised in this appeal, is a claim that the evidence obtained as a result of the search of Dreyer's home and computer should be suppressed because the actions of the Naval Criminal Investigative Service agent violated the Posse Comitatus Act, 18 U.S.C. § 1385. Because Naval Criminal Investigative Service is a civil law enforcement agency, however, the Posse Comitatus Act does not apply.

A. *Standard of Review.*

Whether the Posse Comitatus Act has been violated is a mixed question of fact and law, and this Court reviews a district court's determination of the issue *de novo*. *United States v. Hitchcock*, 286 F.3d 1064, 1069 (9th Cir. 2002) amended and superseded by 298 F.3d 1021 (9th Cir. 2002).

B. *The Posse Comitatus Act Was Not Violated.*

The Posse Comitatus Act prohibits Army and Air Force military personnel from participating in civilian law enforcement activities except when expressly authorized to do so by the Constitution or Act of Congress.⁶ 18 U.S.C. § 1385. Although the Act does not directly reference the Navy or the Marine Corps, Congress directed the Department of Defense to prescribe “such regulations as might be

⁶ Specifically, 18 U.S.C. § 1385 states:

Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.

necessary” to prohibit any member of the Army, Navy, Air Force, or Marine Corps from directly participating in a “search, seizure, arrest, or other similar activity unless participation in such activity by such member is otherwise authorized by law.” 10 U.S.C. § 375. The Department of Defense then made the Act applicable to the Navy and the Marine Corps as a matter of policy. Department of Defense Directive 5525.5 (January 15, 1986).⁷ The Secretary of the Navy adopted this policy as well. SECNAVINST 5820.7B.

C. Because The Naval Criminal Investigative Service Is A Civilian Law Enforcement Agency, With No Direct Reporting Relationship To Any Military Officer, The Provisions Of The Posse Comitatus Act Do Not Apply To Civilian Special Agents Of The Naval Criminal Investigative Service In The Execution Of Their Duties As Sworn Law Enforcement Officers.

By statute, Congress directed that the civilian employees of the Department of the Navy who are special agents of the Naval Criminal Investigative Service (“NCIS”) may execute and serve warrants for any felony “cognizable under the law of the United States” if the agent has probable cause to believe the person has or is committing the felony.

⁷ Copies of this Directive and other Instructions cited in this portion of the argument are included in the addendum to this brief.

10 U.S.C. §§ 1585a and 7480. The statute further directs that this authority is to be exercised in accordance with guidelines proscribed by the secretary of the Navy, as approved by the Secretary of State and the Attorney General. 10 U.S.C. § 7480(c).

Prior to December 28, 2005, Instruction 5520.3B was the controlling guidance on the jurisdiction and responsibility for criminal investigations within the Department of the Navy. SECNAVINST 5520.3B (January 4, 1993). Paragraph 4 of Instruction 5520.3B clearly stated that although the Director of the NCIS reported directly to the Secretary of the Navy, the Director also reported to the Chief of Naval Operations for “physical, personnel and information security.” *Id.*; *United States v. Chon*, 210 F.3d 990, 994 (9th Cir. 2000) (“the NCIS Director has a direct reporting relationship to the Chief of Naval Operations, a military officer”). On December 28, 2005, however, the Secretary of the Navy issued Instruction 5430.107, to “set forth the authority, responsibilities, mission and functions of the [NCIS] and its relationship with other Department of the Navy (DON) organizations and activities.” SECNAVINST 5430.107. Instruction 5430.107 expressly cancelled Instruction 5520.3B, reaffirmed that the Director of

NCIS reports directly to the Secretary of the Navy, and eliminated any reporting relationship between the Director of NCIS and the Chief of Naval Operations. *Compare* SECNAVINST 5520.3B, paragraph 4, with SECNAVINST 5430.107, paragraph 5.

The holding in *Chon* that the NCIS was bound by the limitations of 18 U.S.C. § 375 was predicated on the then-existing reporting relationship between the Director of the NCIS and “the Chief of Naval Operations, a military officer.” *Chon*, 210 F.3d at 994. The fact that this reporting relationship was eliminated in 2005, (SECNAVINST 5430.107), provides a basis for distinguishing the outcome in *Chon* from the case now before the Court. Pursuant to the 2005 instruction, the Director of the NCIS is now accountable only to the Secretary of the Navy, who is himself a civilian employee of the United States. *See* 10 U.S.C. § 5013. Instruction 5430.107 now goes to great lengths to delineate the separation between the NCIS and the military command structure. Paragraph 6 of Instruction 5430.107, states that NCIS investigations and operations are initiated, conducted, and directed as it deems appropriate, “regardless of command authorization.” *Id.* In paragraph 6(b)(5), Instruction 5430.107 draws a clear distinction

between the use of military investigators and civilian NCIS Special Agents and their respective investigative authority; military investigators have authority to investigate only misdemeanor offenses, “purely military offenses,” or cases the NCIS has declined to investigate. *Id.* Similarly, paragraph 6(d)(2) states that when Marine Corps Criminal Investigation Division Special Agents are assigned to work with their civilian NCIS Special Agent counterparts, “given their military status, Marine Special Agents may not exercise the arrest authorities extended to NCIS civilian Special Agents pursuant to reference (b).” *Id.* Moreover, a comparison of the now-cancelled Instruction 5520.3B with Instruction 5430.107 shows the latter to make repeated references to the “civilian Special Agents” of NCIS, references which are absent from Instruction 5520.3B.

Given the purely civilian nature of the NCIS and the absence of any reporting relationship to a military officer, the provisions of the Posse Comitatus Act do not apply to civilian Special Agents of the NCIS in the execution of their duties as sworn law enforcement officers.

D. The Posse Comitatus Act Prohibits Only The Direct Involvement Of Military Personnel In Civilian Law Enforcement, Not The Indirect Assistance Of Military Personnel.

Even if the Court were to conclude that, in its current structure, the civilian Special Agents of the NCIS are military personnel to whom the Act applies, the Act does not prohibit indirect assistance by military personnel. When the Secretary of Defense promulgated Department of Defense Directive 5525.2, which was then implemented by the Secretary of the Navy Instruction 5820.7B, he prohibited only the “direct” military involvement in civilian law enforcement, not “indirect” assistance, such as the transfer of information. *United States v. Hitchcock*, 286 F.3d 1064, 1069, amended and superseded by 298 F.3d 1021 (9th Cir. 2002). *See also* Department of Defense Directive 5525.5, Enclosure 4 (E4) § 1.7.1 (“Other Permissible Assistance”); SECNAVINST 5820.7C (“Cooperation With Civilian Law Enforcement Officials”) (January 26, 2006). Both the Directive and Instruction 5820.7C make a further exception to the general prohibition against direct involvement “where the military participation is undertaken ‘for the primary purpose of furthering a military or foreign affairs function

of the United States, regardless of incidental benefits to civilian authorities.” *Hitchcock*, 286 F.3d at 1069; *see also Chon*, 210 F.3d at 994 (recognizing the independent military purpose exception to the prohibition against military involvement in civilian law enforcement activities); *United States v. Bacon*, 851 F.2d 1312 (11th Cir. 1988).

Agent Logan’s transfer of the information identifying Dreyer as an individual distributing child pornography over the Internet is an example of such “indirect” assistance. *United States v. Holloway*, 2011 WL 304580 (W.D. Ky. 2011), *aff’d* __ Fed.Appx.__, 2013 WL 3887665 (July 30, 2013). In *Holloway*, like the case before this court, an undercover NCIS Agent was conducting an investigation into the sexual exploitation of children over the Internet when she received child pornography from a Yahoo! chat room user during a nearly hour-long chat session. *Id.* at *1. After obtaining search warrants for subscriber information from Yahoo!, and from the Internet Service Provider, the NCIS Agent determined the suspect was not associated with the military. *Id.* The NCIS Agent then forwarded her investigation to local law enforcement officers, who used the information in her report to obtain a state search warrant for Holloway’s home. *Id.* at *2. Evidence

obtained pursuant to the search warrant revealed the presence of images and videos of child pornography and Holloway subsequently filed a motion to suppress evidence, arguing in part that the NCIS Agent violated the Posse Comitatus Act. *Id.*

Addressing this issue, the district court noted that “the sexual exploitation of children is prohibited under the [Uniform Code of Military Justice], and that because the NCIS Agent’s investigation was an attempt to stop such prohibited activity, it fell under the “independent military purpose exception” to the Posse Comitatus Act. *Id.* The district court also noted that the NCIS Agent immediately turned her investigation over to the appropriate civilian law enforcement authorities when she discovered her suspect was not associated with the military, and that she was not personally involved with the execution of the search warrant at Holloway’s home or the subsequent search for evidence. *Id.* This is in contrast to the facts of *Chon*, where NCIS agents interviewed multiple suspects and witnesses, searched business premises, recovered stolen property, and effectuated arrests. *Chon*, 210 F.3d at 992. *See also Hayes v. Hawes*, 921 F.2d 100, 103-04 (7th Cir. 1990) (a “magnitude of military involvement needed”

before a violation of the Posse Comitatus Act occurs). In *Holloway*, the district court characterized the NCIS Agent's involvement as "incidental," and held that no violation of the Act had occurred where Holloway was not "subjected to the regulatory, prescriptive, or compulsory use of military power." *Holloway*, 2011 WL 304580 at *3. Affirming that result, the Sixth Circuit noted that in order to violate the Act, "the military must permeate civil law enforcement; it is not a violation where the military does not participate in the arrest, search, or seizure of evidence." *Holloway*, 2013 WL 3887665 at *1.

Here, like in *Holloway*, Agent Logan's investigation was an attempt to stop the distribution of child pornography over the Internet, a crime under the Uniform Code of Military Justice, federal law, and state law. Agent Logan targeted a geographic area with an extensive military presence. Therefore, there was an "independent military purpose" for Agent Logan's investigation constituting an exception to the Act. *Chon*, 210 F.3d at 994; Department of Defense Directive 5525.5, E4, § 1.2.1.1. As in *Holloway*, as soon as Special Agent Logan discovered Dreyer was not associated with the military in active duty status, he transferred the information to the appropriate civilian law

enforcement authorities, and had no further involvement with the investigation. Similarly, Agent Logan's involvement here was "incidental," and Dreyer was never subjected to the regulatory, prescriptive, or compulsory use of military power. In fact, during the entire course of identifying Dreyer as someone distributing child pornography over the Internet, Agent Logan had no personal contact with Dreyer. Thus, no violation of the Posse Comitatus Act exists.

E. Even If The Posse Comitatus Act Applies, The Suppression Of Evidence Is Not Available As Remedy Under The Posse Comitatus Act.

Even if this Court were to conclude that the Posse Comitatus Act applies to the civilian NCIS Special Agents, and to Agent Logan's investigation, the Act does not provide for suppression of evidence gathered in violation of the Act. *See* 18 U.S.C. § 1385. As this Court has observed, "courts have uniformly refused to apply the exclusionary rule to evidence seized in violation of the [Posse Comitatus Act]."

United States v. Roberts, 779 F.2d 565, 568 (9th Cir. 1986). *See also* *United States v. Johnson*, 410 F.3d 137, 148 (4th Cir. 2005) (noting that "[a]s a general matter, the exclusionary rule is not a remedy for violations of the [Act]"); *United States v. Mullins*, 178 F.3d 334, 343

(5th Cir. 1999) (same); *United States v. Walden*, 490 F.2d 372, 376-77 (4th Cir. 1974) (observing that the Act and accompanying instructions cannot be fairly characterized as “expressly designed to protect the person rights of defendants.”) In fact, as the Sixth Circuit observed in *Holloway*, to date, no court has excluded evidence gathered in violation of the Posse Comitatus Act, and no court has found cause to create and apply an exclusionary rule for such evidence. *Holloway*, 2013 WL 3887665 at *1; *Gilbert v. United States*, 165 F.3d 470, 474 n.2 (6th Cir. 1999) (collecting cases).

Due to the social costs of suppressing evidence, this Court has held that the use of the exclusionary rule “is an exceptional remedy typically reserved for violations of constitutional rights.” *United States v. Smith*, 196 F.3d 1034, 1040 (9th Cir. 1999). *See also United States v. Harrington*, 681 F.2d 612, 615 (9th Cir. 1982) (“There must be an exceptional reason, typically the protection of a constitutional right, to invoke the exclusionary rule.”). Dreyer had no constitutional right to privacy in any evidence gathered by Agent Logan. As this Court has recognized, individuals who use peer-to-peer file-sharing programs have no objectively reasonable expectation of privacy in the files they chose to

share. *United States v. Borowy*, 595 F.3d 1045, 1048 (9th Cir. 2010); *United States v. Ganoë*, 538 F.3d 1117, 1127 (9th Cir. 2008).

Likewise, there is no objectively reasonable expectation of privacy with respect to an IP address or associated subscriber information.

United States v. Christie, 624 F.3d 558, 574 (3rd Cir. 2010);

United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008). *See also*

Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (“a person has no

legitimate expectation of privacy in information he voluntarily turns

over to third parties”). Without a reasonable expectation of privacy in

any of the evidence gathered by Agent Logan, there is no constitutional

violation and no reason to invoke application of the exclusionary rule in

this case.

Moreover, this Court has long refused to apply the exclusionary

rule to violations of the Posse Comitatus Act “until a need to deter

future violations is demonstrated.” *Roberts*, 779 F.2d at 568. Despite

the defense arguments to the contrary, the record here contains no

evidence of widespread or repeated violations of the Posse Comitatus

Act which would justify the application of the exclusionary rule for its

deterrent value. Those Courts that have considered the issue in

analogous circumstances have rejected such claims and Dreyer cannot cite a single case which has so found. Thus, even if this Court were to conclude a violation had occurred, it would not warrant suppression in this case since there was no reason for the NCIS Agent to conclude his actions violated the statute. Indeed, Dreyer has not cited even one case where a court has found widespread and repeated violations of the Posse Comitatus Act warranting application of the exclusionary rule. Simply put, he has failed to demonstrate that this case should be the first.

II. The Trial Judge Correctly Found There Was Probable Cause To Believe Evidence Of The Distribution And Possession Of Child Pornography Would Be Found At Dreyer's Residence.

The second issue raised in this appeal is a claim that, based on its findings at the *Franks* hearing, the district court should have found that probable cause was lacking for the issuance of the state search warrant. That claim too lacks merit.

A. Standard of Review.

This Court reviews for clear error a district court's finding that an affidavit did not contain purposefully or recklessly false statements or omissions and reviews *de novo* its determination that the misleading omissions or false information did not undermine a finding of probable cause. *United States v. Elliott*, 322 F.3d 710, 714 (9th Cir. 2003).

B. The Affidavit In Support Of The State Search Warrant Demonstrated Probable Cause To Search Dreyer's Residence For Evidence Of Child Pornography.

Before a warrant may issue, the Fourth Amendment requires a neutral and detached judge to find the facts and circumstances presented in an affidavit are “sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed,’ and that evidence bearing on that offense will be found in the place to be searched.” *Safford Unified School Dist. No. 1 v. Redding*, 557 U.S. 364, 369 (2009) (citations omitted). This requirement is a “‘practical, nontechnical conception’ that deals with ‘the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act.’” *Maryland v. Pringle*, 540 U.S. 366, 370 (2003). Probable cause to search is defined as “a fair

probability that contraband or evidence of a crime will be found in a particular place.” *Illinois v. Gates*, 462 U.S. 213, 238 (1983). It does not require a showing of “certainty or even a preponderance of the evidence,” *United States v. Gourde*, 400 F.3d 1065, 1069 (9th Cir. 2006) (en banc), only a “‘fair probability’ that contraband or evidence is located in a particular place,” a finding that, in turn, depends on “the totality of the circumstances, including reasonable inferences and is a ‘common sense, practical question.’” *United States v. Kelley*, 482 F.3d 1047, 1050 (9th Cir. 2003) (quoting *Gourde*, 400 F.3d at 1069). Moreover, the issuing judge’s determination that probable cause exists should be afforded great deference. *Gourde*, 440 F.3d at 1069.

A district court conducting a hearing pursuant to *Franks v. Delaware*, 483 U.S. 154 (1978) engages in a two-part process to determine whether suppression is warranted. *United States v. Martinez-Garcia*, 397 F.3d 1205, 1214-15 (9th Cir. 2005). The Court must first determine whether the affiant “intentionally or recklessly made false or misleading statements or omissions in support of the warrant.” *Id.* If that finding is made, the district court then must determine whether, after setting aside the false material, the remainder

of the affidavit still states probable cause. *Id.* Similarly, where the claim concerns omissions of material statements, a court must determine whether the affidavit continues to state probable cause once the omitted information is supplied. *United States v. Hall*, 113 F.3d 157, 159 (9th Cir. 1997).

As he acknowledged during the *Franks* hearing, Detective Schrimpscher used a template provided to him by a Seattle Police detective to prepare his affidavit and the application for a warrant to search Dreyer's residence. ER 231. Schrimpscher acknowledged he did not inform the state court judge to whom the warrant was presented that this was his first investigation involving child pornography and the Internet. Schrimpscher also acknowledged that some of the statements contained in the affidavit came directly from template he received from the Seattle Police detective without alteration and had no relevance to the investigation of Dreyer. Schrimpscher's affidavit contained recitations about a software program called "E-Phex" and a statement indicating that he, as the affiant, had conducted the investigation of Dreyer using "E-Phex." ER 281-83. Schrimpscher admitted during the

evidentiary hearing that he had never used this software and that this was simply part of the template he had received. ER 424-25.

Nonetheless, Schrimpscher's affidavit also clearly acknowledges that the only investigation that Schrimpscher himself conducted was to verify Dreyer's address and that the request for the warrant was based on the investigation that Agent Logan conducted as described in the appended copy of Agent Logan's investigative report.⁸ That report contained a description of the three files Agent Logan had downloaded and thus permitted the finding by the reviewing judge that the imagery constituted child pornography. Moreover, the description of Schrimpscher's limited investigation and the inclusion of Agent Logan's report, made clear to the state court judge reviewing the application

⁸ It was entirely proper for the affidavit to reference and append Agent Logan's report. *See United States v. Lingenfelter*, 997 F.2d 632, 639 (9th Cir. 1993) (where the unsworn expertise statement of the non-affiant was stapled to the search warrant affidavit and submitted to the issuing judge, the affiant effectively swore to it as well); *United States v. Berisford*, 750 F.2d 57, 58 (10th Cir. 1984) ("There is nothing unusual about reading together the several components of an affidavit for search warrant, where properly incorporated or related by reference.").

that Agent Logan had conducted the investigation of Dreyer, not Schrimpsheer. ER 295-335, 395, 425-26.

Given these facts, the district court properly concluded that even excising all of the background information Schrimpsheer had cut and pasted from the template, the affidavit still set forth probable cause. Similarly if Schrimpsheer had disclosed this was his first case of this kind, it would have done nothing to undermine probable cause because it was clear that Agent Logan had done the work. There is nothing about this fact that is concealed in the affidavit and the background section that Schrimpsheer cut and pasted in such an extremely sloppy manner adds nothing to the probable cause. Simply put, the section on the investigation itself raises a fair probability that child pornography would be found at Dreyer's residence. *Gates*, 462 U.S. at 238; *Kelley*, 482 F.3d at 1050.

III. The State Search Warrant Was Not A General Warrant, And Officers Did Not Exceed The Scope Of The Warrant In Executing Their Search Of Dreyer's Residence.

The defense also argues that suppression of the evidence obtained as a result of the state search warrant is required because the search exceeded the scope of the warrant and the warrant itself is a general

warrant. Although the officers acted reasonably in determining whether the computer they discovered at the residence actually contained child pornography, the defense argues that the warrant did not authorize the forensic preview on-site and also challenges the manner in which the preview was conducted. All of these claims lack merit.

A. The Standard of Review.

A district court's order granting or denying a motion to suppress, is reviewed de novo. *United States v. Maddox*, 614 F.3d 1046, 1048 (9th Cir. 2010).

B. The Scope of the State Warrant Was Not Exceeded.

The Fourth Amendment requires that “the scope of what may be seized under the warrant be limited by the probable cause on which the warrant is based.” *United States v. Brobst*, 558 F.3d 982, 993 (9th Cir. 2009). These standards apply whether the search is for a home, a computer or a business. A warrant must also contain objective standards for choosing the items to be seized. This reflects, in part, the Fourth Amendment's requirement that two things be stated with particularity: “the place to be searched’ and ‘the persons or things to be

seized.” *United States v. Grubbs*, 547 U.S. 90, 97 (2006). If the location to be searched and items to be seized are described with sufficient particularity, then “a lawful search . . . generally extends to the entire area in which the object of the search may be found.” *United States v. Ross*, 456 U.S. 798, 820 (1982). Whether this particularity standard has been met is determined in light of the information available at the time the warrant issued. *United States v. Shi*, 525 F.3d 709, 731-732 (9th Cir. 2008). “Warrants which describe generic categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible.” *Shi*, 525 F.3d at 731 (quoting *United States v. Adjani*, 452 F.3d 1140, 1147-48 (9th Cir. 2006)).

To the extent Dreyer raised this issue below, his arguments were limited to an assertion that the state search warrant did not “adequately describe the contents of the computer files,” *see* CR 17 at 10, and an assertion made during argument at the evidentiary hearing that the searching officers exceeded the scope of the warrant by conducting an on-site forensic examination of the computer at Dreyer’s

residence.⁹ ER 17-18. But Dreyer’s assertion that the warrant lacked particularity is belied by the warrant itself, which specifically permits a search for “digital video and/or image files depicting minors engaged in sexually explicit conduct” and defines the types of electronic storage devices on which such items might be found. ER 292-93. Moreover, the affidavit in support of the warrant makes clear that where it is feasible to do so, officers will attempt to conduct an initial on-site preview of computers to assist them in determining which computers to seize and which to leave. ER 287, 291. No more specific description of the computer files was necessary. This Court has expressly found a warrant is not overbroad merely because it lacks description of the actual search methodology to be employed. *See United States v. Hill*, 459 F.3d 966, 977-78 (9th Cir. 2006) (defendant’s proposed search methodology is unreasonable and overlooks the probability that perpetrators will save files using names not obviously associated with the crimes at issue). As this Court as observed,

⁹ New grounds for suppression that were not raised in a motion filed before trial are generally deemed waived. *United States v. Flores-Montano*, 424 F.3d 1044, 1047 n.2 (9th Cir. 2005).

The prohibition of general searches is not to be confused with a demand for precise ex ante knowledge of the location and content of evidence related to the suspected violation. The proper metric of sufficient specificity is whether it was reasonable to provide a more specific description of the items at that juncture of the investigation.

United States v. Meek, 366 F.3d 705, 715-16 (9th Cir. 2004). Moreover, as this Court recently observed, “[t]he government ha[s] no way of knowing which or how many illicit files there might be or where they might be stored, or of describing the items to be seized in a more precise manner.” *United States v. Schesso*, __ F.3d __, 2013 WL 5227071 (9th Cir. Sept. 18, 2013). *See also Adjani*, 452 F.3d at 1148 (affidavit limiting search to evidence of a specific crime satisfies specificity requirement).

In the district court, Dreyer did not challenge the manner in which the forensic examination was conducted other than to assert the officers should not have been allowed to conduct an onsite forensic preview in his home. Dreyer now appears to be taking a different approach essentially arguing that this Court’s holdings in *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982) and *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009), opinion revised and superseded by 621 F.3d 1162 (9th Cir. 2010) (en banc) (per

curiam) somehow require the suppression of evidence. Assuming these arguments were not waived by the failure to raise them in the district court, they have no merit.

In *Schesso*, this Court addressed a similar argument holding that the absence of the search protocols set out in the *Comprehensive Drug Testing, Inc. (“CDT”)* cases “neither violates the Fourth Amendment nor is inconsistent with CDT III or its predecessor case, *Tamura*.” 2013 WL 5227071 at *6. As in *Schesso*, the state search warrant at issue here was particular with respect to the place to be searched — Dreyer’s residence — and with respect to the things to be seized — computers, computer-related software, digital data, and evidence of the state crimes of possession and distribution of child pornography, including child pornography itself. ER 290-91. The officers seized only things covered by the warrant and for which there was probable cause. As was the case in *Schesso*, the officers searched for, and found, evidence of the possession and distribution of child pornography. That evidence should not be suppressed.

Focusing on the forensic preview conducted by Detective Luckie, the defense also argues that because the forensic program that was

used for this purpose searched for all image files and not merely child pornography that the scope of the warrant was somehow exceeded. But in any search it is inevitable that “some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those [items] authorized to be seized.” *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976). Here, the record established that the detective limited his search to image files, and then reviewed only thumb nail sized images to determine if there was, in fact, child pornography on the computer. That is precisely what the warrant required.

C. The Affidavit In Support Of The Federal Search Warrant Demonstrated Probable Cause To Search The Computers Seized From Dreyer’s Residence For Evidence Of Child Pornography.

Building on other arguments, the defense also argues that result of the subsequent federal warrant should be suppressed as fruits of the unlawful state warrant and Dreyer’s suppressed statements. As noted above, however, the district court properly denied the motion to suppress the evidence from the state warrant, so this argument fails on that ground alone. Similarly, Detective Luckie’s forensic preview was

within the scope of the warrant and thus provides no taint. Indeed, what Luckie observed during the brief forensic preview is itself enough to provide probable cause.

The reference to Dreyer's statements certainly does not render the warrant defective. Dreyer's statements to law enforcement were not critical to the determination of whether probable cause existed to conduct a search of the seized devices, and the inclusion of those statement in Special Agent Huynh's affidavit "does not, by itself, taint the warrant or the evidence seized pursuant to the warrant."

United States v. Barajas-Avalos, 377 F.3d 1040, 1058 (9th Cir. 2004).

As the defense acknowledges the question is whether the remaining information provided probable cause for the issuance of the warrant. If the information about Dreyer's statements—contained in a single paragraph of Special Agent Huynh's affidavit—is excised from the affidavit it still stated probable cause. Indeed, that would be the case even the observations by Detective Luckie were also not considered. Specifically, the affidavit described Agent Logan's investigation and identification of Dreyer as an individual distributing child pornography over the Internet. ER 462-466. This information alone would have

been more than sufficient to demonstrate probable cause to conduct a full forensic examination of the computer and other digital media seized from Dreyer's residence. *Schesso*, __ F.3d __, 2013 WL 5227071 *4-5; *Gourde*, 400 F.3d at 1069; *Kelley*, 482 F.3d at 1050. Thus, there simply is no basis to suppress the evidence discovered during the execution of the federal warrant.

IV. The District Court Did Not Abuse Its Discretion When It Denied Dreyer's Motion In Limine To Exclude Evidence Obtained Through The Use Of The Roundup Software Program.

The final issue raised in this appeal is a challenge to the district court conclusion that a *Daubert* hearing was not required before Agent Logan could testify his use of the RoundUp software to download the child pornography that Dreyer had offered on the peer-to-peer network. The district court did not abuse its discretion in making this determination.

A. Standard of Review.

A district court decision to admit or exclude evidence is reviewed for abuse of discretion and will only be reversed if manifestly erroneous. *United States v. Gonzales*, 307 F.3d 906, 908 (9th Cir. 2002).

B. The District Court Properly Concluded A Daubert Hearing was not required before the RoundUp Evidence Could Be Introduced.

In *Daubert v. Merrell Dow Pharmacueticals, Inc.*, 509 U.S. 579 (1993), the Supreme court established a “gatekeeper” function for trial judges under Federal Rule of Evidence 702. “Faced with a proffer of expert scientific testimony . . . the trial judge must determine at the outset . . . whether the expert is proposing to testify to (1) scientific knowledge that (2) will assist the trier of fact to understand or determine a fact in issue.” *Daubert*, 509 U.S. at 592. To exercise this “gatekeeper” role, *Daubert*, consistent with Federal Rule of Evidence 702, points the trial judge to a non-exhaustive list of factors to consider in assessing the reliability of the proffered testimony, including testing, peer review and publication, potential error rate, and general acceptance in the relevant community. *Id.* at 592-94; *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 141 (1999). The trial court may consider these factors even when the proffered testimony is technical, not scientific, in nature. *Id.* The Supreme Court was careful to emphasize that the trial court may consider one or more of the *Daubert* factors, but noted the ultimate decision on the reliability of the proposed testimony

in a particular case “is a matter that the law grants the trial judge broad latitude to determine.” *Id.* at 141, 153. In other words, “the gatekeeping inquiry must be tied to the facts of a particular case.” *Id.* at 150 (internal quotes and citations omitted).

As an initial matter, the defense has not actually established that the testimony challenged is expert testimony that required a *Daubert* hearing. As the trial court observed, the RoundUp law enforcement investigative software tool is simply that: a tool used to search for individuals trading child pornography over the Internet. ER 66. That observation is particularly relevant because the use of such a tool does not convert the results from the use of such a tool into an expert opinion requiring a *Daubert* hearing. *United States v. Lauder*, 409 F.3d 1254, 1264 (10th Cir. 2005) (*Daubert* “applies only to the qualifications of an expert and the methodology or reasoning used to render an expert opinion,” and generally does not regulate the underlying facts or data relied upon to form that opinion). Evidence obtained through use of law enforcement investigative software tools is routinely admitted in child pornography prosecutions. *See, e.g., United States v. Chiaradio*, 684

F.3d 265 (1st Cir. 2012) (evidence obtained through use of eP2P law enforcement software tool admitted at trial).

In any event, “the trial court must be afforded wide latitude both in deciding whether to admit expert testimony and in deciding how to test reliability.” *United States v. Alatorre*, 222 F.3d 1098, 1101-02 (9th Cir. 2000); *United States v. Hankey*, 203 F.2d 1160, 1168 (9th Cir. 2000). This Court has further recognized that, “in light of the Supreme Court’s emphasis on the broad discretion granted to trial courts in assessing the relevance and reliability of expert testimony,” and, given that there is no authority which mandates a *Daubert* hearing, “trial courts are not compelled to conduct pretrial hearings in order to discharge the gatekeeping function.” *Alatorre*, 222 F.3d at 1100. Other circuits have reached similar conclusions. *Id.* at 1103 (collecting cases).

On June 22, 2012, during the evidentiary hearing on his motion to suppress, Dreyer had ample opportunity to question Agent Logan on his use of the RoundUp law enforcement investigative software tool and its reliability, thus providing Dreyer with the “functional equivalent of a *Daubert* hearing.” *See Chiaradio*, 684 F.3d at 277-78. On direct examination, Agent Logan testified that RoundUp was created by the

Internet Crimes Against Children Training Academy, and described how he logged into the RoundUp software program. ER 338. Using screen shots of the RoundUp user interface that he captured during his investigation, Agent Logan described the specific steps that he took on April 14, 2011, to conduct his investigation. ER 346-51, 479-81. On cross-examination, Agent Logan testified that he did not know what the programming language was, did not know how many lines of source code the program contained, did not know how the program had been tested, and did not know the stated error rate. ER 380-81. However, Agent Logan also testified that he validated the RoundUp software program during his training, and agreed with Dreyer's counsel that it "worked as advertised." ER 381.

More than two months after Special Agent Logan's testimony, on September 13, 2012, Dreyer moved in limine to exclude "electronic evidence," particularly the evidence Agent Logan obtained using RoundUp. CR 68-70. Attached to Dreyer's motion was a press release from the University of Massachusetts at Amherst describing the development of RoundUp and its widespread use by law enforcement in online child pornography investigations. ER 173. As the trial judge

stated, “I’ve read both the motion and the response . . . in this instance, we did have a hearing where the NCIS officer explained how he uses [RoundUp].” ER 66. As the trial judge further stated, RoundUp “was developed by law enforcement. . . . It has been used extensively not only by various police agencies but also has been the basis for the courts issuing search warrants. . . it appears that peers are using it, that it was developed in an academic setting, [and] there’s been an opportunity for people to write about it.” ER 66-67. These are precisely the types of *Daubert* factors the trial judge is to consider in making her determination whether to admit the proffered evidence. *Daubert*, 509 U.S. at 592-94; *Kumho Tire*, 526 U.S. at 141. After considering these factors, and in the exercise of the broad discretion granted to her by *Daubert* and *Kumho Tire*, the trial judge properly concluded that a separate *Daubert* hearing was unnecessary, and that the evidence was admissible. ER 67.

As a final matter, the record itself establishes the reliability of the RoundUp program. Agent Logan testified both at the suppression hearing and at trial about his use of the program, how it operates, that the fact that it identified three files containing child pornography that

were offered for download at the IP address associated with Dreyer's computer. The trial evidence included testimony from the agent who conducted the forensic examination of Dreyer's computer. His testimony establishes that the very files that Agent Logan located and downloaded using the RoundUp program were located on Dreyer's computer on that date and time. RT 9/25 at 109-113. Thus, this adds further support for the conclusion that the district court did not abuse its discretion in denying the defense motion. Moreover, this evidence established that any error in failing to hold a *Daubert* hearing was harmless. See *United States v. Jawara*, 474 F.3d 565, 583 (9th Cir. 2007).

CONCLUSION

For all the foregoing reasons, the Court should affirm the decision of the district court denying Dreyer's motion to suppress and the decision of the district court denying Dreyer's motion to exclude

evidence obtained through use of the RoundUp investigative software tool.

DATED this 29th day of October, 2013.

Respectfully submitted,

JENNY A. DURKAN
United States Attorney
Western District of Washington

/s/ Marci L. Ellsworth
MARCI L. ELLSWORTH
Assistant United States Attorney
700 Stewart Street, Suite 5220
Seattle, Washington 98101
(206) 553-7970

STATEMENT OF RELATED CASES

Counsel for the United States is not aware of any related cases which should be considered with this matter.

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. 32(a)(7)(C) and Ninth Circuit Rule 32-1,
I certify that the foregoing brief is proportionately spaced, has a
Century Schoolbook typeface of 14 points, and contains 10,971 words.

Dated this 29th day of October, 2013.

/s/ Marci L. Ellsworth
MARCI L. ELLSWORTH
Assistant United States Attorney

CERTIFICATE OF SERVICE

I hereby certify that on October 29, 2013, I electronically filed the foregoing Answering Brief of the United States with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system to the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

DATED this 29th day of October, 2013.

/s/ Helen J. Brunner
HELEN J. BRUNNER
Assistant United States Attorney

ADDENDUM

TABLE OF CONTENTS

1. Department of Defense Directive, Number 5525.5,
January 15, 1986. 1

2. Department of the Navy, SECNAVINST 5430.107,
NCIS, 28 Dec. 2005. 32

3. Department of the Navy, SECNAVINST 5520.3B,
NCIS, 4 January 1993. 52

4. Department of the Navy, SECNAVINST 582037C,
N3/N5, 26, January 2006 65



Department of Defense DIRECTIVE

NUMBER 5525.5

January 15, 1986

Administrative Reissuance Incorporating Change 1, December 20, 1989

ASD(FM&P)

SUBJECT: DoD Cooperation with Civilian Law Enforcement Officials

References: (a) through (ll), see enclosure E1.

1. REISSUANCE AND PURPOSE

This Directive reissues reference (a) to update uniform DoD policies and procedures to be followed with respect to support provided to Federal, State, and local civilian law enforcement efforts; and assigns responsibilities.

2. APPLICABILITY AND SCOPE

2.1. This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified and Specified Commands, and the Defense Agencies (hereafter referred to collectively as DoD Components). The term "Military Service," as used herein, refers to the Army, Navy, Air Force, and Marine Corps.

2.2. DoD policy on assistance to law enforcement officials in foreign governments is not governed by this Directive except as specified by other DoD issuances.

3. DEFINITIONS

3.1. Civilian Agency. An agency of one of the following jurisdictions:

3.1.1. The United States (other than the Department of Defense, but

including the U.S. Coast Guard). This includes U.S. agencies in international areas dealing with U.S. flag vessels or aircraft in violation of U.S. law.

3.1.2. A State (or political subdivision of it) of the United States.

3.1.3. Commonwealth, Territory, or Possession (or political subdivision of it) of the United States.

3.2. Civilian Law Enforcement Official. An officer or employee of a civilian agency with responsibility for enforcement of the laws within the jurisdiction of that agency.

3.3. DoD Intelligence Component. An organization listed in subsection 3.4. of DoD Directive 5240.1 (reference (b)).

4. POLICY

It is DoD policy to cooperate with civilian law enforcement officials to the extent practical. The implementation of this policy shall be consistent with the needs of national security and military preparedness, the historic tradition of limiting direct military involvement in civilian law enforcement activities, and the requirements of applicable law, as developed in enclosures E2. through E7.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense (Force Management and Personnel) (ASD(FM&P)) shall:

5.1.1. Coordinate with civilian law enforcement agencies on long range policies to further DoD cooperation with civilian law enforcement officials.

5.1.2. Provide information to civilian agencies and The National Narcotics Border Interdiction System (NNBIS) to facilitate access to DoD resources.

5.1.3. Coordinate with the Department of Justice, the Department of Transportation (U.S. Coast Guard), and the Department of the Treasury (U.S. Customs Service) and represent the Department of Defense on interagency organizations regarding matters involving the interdiction of the flow of illegal drugs into the United States.

5.1.4. Develop guidance and, as required, take other actions as specified in enclosures E2. through E7., taking into account the requirements of DoD intelligence components and the interests of the Assistant Secretary of Defense (Health Affairs) (ASD(HA)) and the Assistant Secretary of Defense (Reserve Affairs) (ASD(RA)).

5.1.5. Inform the ASD(RA) of all requests for and taskings concerning National Guard and Reserve personnel and resources in support of civilian law enforcement.

5.1.6. Modify the sample report formats at enclosures E6. and E7.

5.2. The Inspector General of the Department of Defense (IG, DoD) shall issue guidance on cooperation with civilian law enforcement officials with respect to audits and investigations conducted, supervised, monitored, or initiated under DoD Directive 5106.1 (reference (c)), subject to coordination with the General Counsel.

5.3. The Assistant Secretary of Defense (Reserve Affairs) (ASD(RA)) shall:

5.3.1. Assist the ASD(FM&P) in the development of guidance for use by approving authorities in evaluating the impact on military preparedness of any request for assistance from units of the National Guard and Reserve.

5.3.2. At the request of the Secretary of Defense or the ASD(FM&P), determine the impact on military preparedness of any request for military assistance from units of the National Guard and Reserve.

5.4. The Secretaries of the Military Departments and the Directors of the Defense Agencies, as appropriate, shall:

5.4.1. Disseminate the guidance issued by the ASD(FM&P) under paragraph 5.1.4., above.

5.4.2. Review training and operational programs to determine how and where assistance can best be provided civilian law enforcement officials consistent with the policy in section 4., above. This review should identify those programs under which reimbursement would not be required under enclosure E5.

5.4.3. Issue implementing documents incorporating the guidelines and procedures of this Directive, including the following:

5.4.3.1. Procedures for prompt transfer of relevant information to law enforcement agencies.

5.4.3.2. Procedures for establishing local contact points in subordinate commands for purposes of coordination with Federal, State, and local civilian law enforcement officials.

5.4.3.3. Guidelines for evaluating requests for assistance in terms of impact on national security and military preparedness.

5.4.4. Inform the Joint Chiefs of Staff (JCS), through ASD(FM&P) of all requests for and taskings in support of civilian law enforcement that involve the resources of a Unified or Specified Command, which, if provided, could have significant impact on military preparedness or national security.

5.5. The Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS) shall establish appropriate guidance for the National Security Agency/Central Security Service (NSA/CSS).

5.6. The Joint Chiefs of Staff shall:

5.6.1. Assist the ASD(FM&P) in the development of guidance for use by approving authorities in evaluating the impact of requests for assistance on national security and military preparedness.

5.6.2. Provide advice on the impact on national security and military preparedness of any request for military assistance at the request of the Secretary of Defense, the ASD(FM&P), the Secretaries of the Military Departments, the Directors of Defense Agencies, or the Commanders of the Unified and Specified Commands.

6. INFORMATION REQUIREMENTS

A quarterly report of all requests for assistance (approved, denied, or pending) shall be submitted by the Secretaries of the Military Departments and the Directors of Defense Agencies to the ASD(FM&P), the General Counsel, the ASD(HA), and the ASD(RA), not later than 30 days after the end of each quarter. The report will show action taken (approval, denial, or pending) and other appropriate information. This information requirement has been assigned Report Control Symbol DD-FM&P(Q)1595. Actions involving the use of classified information or techniques may be exempted from such

report with the concurrence of the ASD(FM&P) if it is impractical to prepare an unclassified summary. The sample format at enclosure will be used to record all aviation assistance.

7. RELEASE OF INFORMATION

7.1. Release of information to the public concerning law enforcement operations is the primary responsibility of the civilian agency that is performing the law enforcement function. The Military Departments and the Directors of the Defense Agencies may release such information, however, when approved under the procedures established by the Secretaries of the Military Departments and the Directors of the Defense Agencies concerned. To the extent possible, the affected civilian law enforcement agencies shall be consulted before releasing such information.

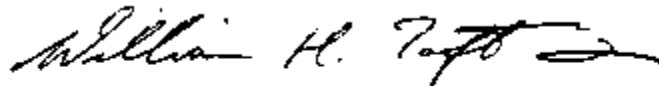
7.2. When assistance is provided under this Directive, such assistance may be conditioned upon control by the Secretaries of the Military Departments and Directors of the Defense Agencies before information is released to the public.

8. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward two copies of implementing documents to the Assistant Secretary of Defense (Force Management and Personnel) within 120 days.

DODD 5525.5 January 15, 86

8.1. MISCELLANEOUS *The provisions of paragraph E4.1.3. of enclosure E4. of Department of Defense Directive 5525.5, entitled "Restrictions on Direct Assistance," will continue to apply to all actions conducted by military personnel within the territorial boundaries of the United States. With regard to military actions conducted outside the territorial jurisdiction of the United States, however, the Secretary of Defense or the Deputy Secretary of Defense will consider for approval, on a case by case basis, requests for exceptions to the policy restrictions against direct assistance by military personnel to execute the laws. Such requests for exceptions to policy outside the territorial jurisdiction of the United States should be made only when there are compelling and extraordinary circumstances to justify them.*



William H. Taft, IV
Deputy Secretary of Defense

Enclosures - 7

1. References
2. Use of Information Collected During Military Operations
3. Use of Military Equipment and Facilities
4. Restrictions on Participation of DoD Personnel in Civilian Law Enforcement Activities
5. Funding
6. Sample Format for Preparing, "Report on Support to Civilian Law Enforcement (RCS DD-FM&P(Q)1595)"
7. Aviation Assistance to Law Enforcement Agencies (Sample Format)

E1. ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5525.5, subject as above, March 22, 1982 (hereby canceled)
- (b) DoD Directive 5240.1, "Activities of DoD Intelligence Components that Affect U.S. Persons," December 3, 1982
- (c) DoD Directive 5106.1, "Inspector General of the Department of Defense," March 14, 1983
- (d) Title 10, United States Code (10 U.S.C.), §§331-334, 337, 371-378, 2576, and 2667; and Chapter 47 (Uniform Code of Military Justice)
- (e) DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense," January 7, 1980
- (f) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1982, authorized by reference (b)
- (g) DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982
- (h) DoD 4515.13-R, "Air Transportation Eligibility," January 1980, authorized by DoD Directive 4515.13, June 26, 1979
- (i) Public Law, "The Economy Act, " (31 U.S.C. §1535)
- (j) Public Law, "The Intergovernmental Cooperation Act of 1968," (40 U.S.C. §§531-535 and 42 U.S.C. §§4201, 4211-4124, 4221-4225, 4231-4233, 4241-4244)
- (k) Public Law, "Federal Property and Administrative Services Act of 1949," (40 U.S.C. §§471-476, 481, 483, 483c, 484-492, 512, 514, 531-535, 541-544, 751-759; 41 U.S.C. §§5, 251-255, 257-260; 44 U.S.C., Chapters 21, 25, 29, 31; and 50 U.S.C. Appendix 1622)
- (l) DoD Directive 3025.12, "Employment of Military Resources in the Event of Civil Disturbances," August 19, 1971
- (m) DoD Instruction 4160.23, "Sale of Surplus Military Equipment to State and Local Law Enforcement and Firefighting Agencies," January 27, 1981
- (n) DoD Instruction 4160.24, "Disposal of Foreign Excess Personal Property for Substantial Benefits or the Discharge of Claims," July 24, 1981
- (o) DoD Directive 4165.6, "Real Property Acquisition, Management and Disposal," December 22, 1976
- (p) DoD Directive 4165.20, "Utilization and Retention of Real Property," January 31, 1985
- (q) DoD Directive 5410.12, "Economic Adjustment Assistance to Defense-Impacted Communities," April 21, 1973

- (r) DoD Instruction 7230.7, "User Charges," January 29, 1985
- (s) DoD Instruction 7310.1, "Disposition of Proceeds from Sales of DoD Excess and Surplus Personal Property," November 15, 1984
- (t) DoD Instruction 7730.53, "Specialized or Technical Services Provided to State and Local Government," December 23, 1982
- (u) DoD Directive 5030.46, "Assistance to the District of Columbia Government in Combating Crime," March 26, 1971
- (v) Public Law, "Posse Comitatus Act," (18 U.S.C. §1385)
- (w) [DoD Directive 5525.7](#), "Implementation of the Memorandum of Understanding Between the Department of Justice and the Department of Defense Relating to the Investigation and Prosecution of Certain Crimes," January 22, 1985
- (x) Title 5, United States Code, Appendix 3, Section 8(g)
- (y) Title 16, United States Code, §§23, 78, 593, and 1861(a)
- (z) Title 18, United States Code, §§112, 351, 831, 1116, 1751, and 3056; "Presidential Protection Assistance Act of 1976," Public Law 94-524, 90 Stat. 2475
- (aa) Title 22, United States Code, §§408 and 461-462
- (bb) Title 25, United States Code, §180
- (cc) Title 42, United States Code, §§97, 1989, and 3789
- (dd) Title 43, United States Code, §1065
- (ee) Title 48, United States Code, §§1418, 1422, and 1591
- (ff) Title 50, United States Code, §220
- (gg) Public Law, "The Controlled Substances Act," (21 U.S.C. §801 *et seq.*)
- (hh) Public Law, "The Controlled Substances Import and Export Act," (21 U.S.C. §951 *et seq.*)
- (ii) Public Law, "The Immigration and Nationality Act," (8 U.S.C. §§1324-1328)
- (jj) Title 19, United States Code §1401 (The Tariff Act of 1930) and §1202 (Tariff Schedules of the United States)
- (kk) Title 21, United States Code §873(b)
- (ll) DoD 7220.9-M, "Department of Defense Accounting Manual," October 1983, authorized by DoD Directive 7220.9

E2. ENCLOSURE 2

USE OF INFORMATION COLLECTED DURING MILITARY OPERATIONS

E2.1. ACQUISITION AND DISSEMINATION

Military Departments and Defense Agencies are encouraged to provide to Federal, State, or local civilian law enforcement officials any information collected during the normal course of military operations that may be relevant to a violation of any Federal or State law within the jurisdiction of such officials. The Secretaries of the Military Departments and Directors of the Defense Agencies shall prescribe procedures for releasing information upon reasonable belief that there has been such a violation.

E2.1.1. The assistance provided under this enclosure shall be in accordance with 10 U.S.C. §371 (reference (d)) and other applicable laws.

E2.1.2. The acquisition and dissemination of information under this enclosure shall be in accordance with DoD Directive 5200.27 (reference (e)), DoD Directive 5240.1 (reference (b)), and DoD 5240.1-R (reference (f)).

E2.1.3. Military Departments and Defense Agencies shall establish procedures for "routine use" disclosures of such information in accordance with DoD Directive 5400.11 (reference (g)).

E2.1.4. Under guidance established by the Secretaries of the Military Departments and the Directors of the Defense Agencies concerned, the planning and execution of compatible military training and operations may take into account the needs of civilian law enforcement officials for information when the collection of the information is an incidental aspect of training performed for a military purpose. In this regard, the needs of civilian law enforcement officials may be considered when scheduling routine training missions. This does not permit the planning or creation of missions or training for the primary purpose of aiding civilian law enforcement officials, and it does not permit conducting training or missions for the purpose of routinely collecting information about U.S. citizens. Local law enforcement agents may accompany routinely scheduled training flights as observers for the purpose of collecting law enforcement information. This provision does not authorize the use of DoD aircraft to provide point-to-point transportation and training flights for civilian law enforcement officials. Such assistance may be provided only in accordance with DoD 4515.13-R (reference (h)).

E2.1.5. Under procedures established by the Secretaries of Military Departments and the Directors of the Defense Agencies concerned, information concerning illegal drugs that is provided to civilian law enforcement officials under this provision (reference (f)) may be provided to the El Paso Intelligence Center.

E2.1.6. Nothing in this section modifies DoD policies or procedures concerning dissemination of information for foreign intelligence or counterintelligence purposes.

E2.1.7. The Military Departments and Defense Agencies are encouraged to participate in Department of Justice Law Enforcement Coordinating Committees situated in each Federal Judicial District.

E2.1.8. The assistance provided under this enclosure may not include or permit direct participation by a member of a Military Service in the interdiction of a vessel, aircraft, or a land vehicle, a search or seizure, arrest, or other similar activity unless participation in such activity by the member is otherwise authorized by law. See enclosure E4.

E2.2. MILITARY PREPAREDNESS

Assistance may not be provided under this enclosure if it could adversely affect national security or military preparedness.

E2.3. FUNDING

To the extent that assistance under this enclosure requires Military Departments and Defense Agencies to incur costs beyond those that are incurred in the normal course of military operations, the funding provisions of enclosure E5. apply.

E3. ENCLOSURE 3

USE OF MILITARY EQUIPMENT AND FACILITIES

E3.1. EQUIPMENT AND FACILITIES

Military Departments and Defense Agencies may make equipment, base facilities, or research facilities available to Federal, State, or local civilian law enforcement officials for law enforcement purposes in accordance with this enclosure.

E3.1.1. The ASD(FM&P) shall issue guidance to ensure that the assistance provided under this enclosure is in accordance with applicable provisions of 10 U.S.C. §§372, 2576, and 2667 (reference (d)); the Economy Act (reference (i)); the Intergovernmental Cooperation Act of 1968 (reference (j)); the Federal Property and Administrative Services Act of 1949 (reference (k)); and other applicable laws.

E3.1.2. The guidance in subsection E3.1.1., above, shall ensure that the following Directives are complied with: DoD Directive 3025.12 (reference (l)); DoD Instruction 4160.23 (reference (m)); DoD Instruction 4160.24 (reference (n)); DoD Directive 4165.6 (reference (o)); DoD Directive 4165.20 (reference (p)); DoD Directive 5410.12 (reference (q)); DoD Instruction 7230.7 (reference (r)); DoD Instruction 7310.1 (reference (s)); DoD Instruction 7730.53 (reference (t)); and other guidance that may be issued by the ASD(FM&P) and the Assistant Secretary of Defense (Comptroller) (ASD(C)).

E3.1.3. The assistance provided by DoD Intelligence Components is subject to DoD Directive 5240.1 (reference (b)) and DoD 5240.1-R (reference (f)).

E3.2. LIMITATIONS ON THE USE OF PERSONNEL

E3.2.1. A request for DoD personnel to operate or maintain or to assist in operating or maintaining equipment made available under section E3.1., above, shall be considered under the guidance in subsection E4.1.6. (enclosure E4.).

E3.2.2. Personnel in DoD intelligence components also are subject to the limitations in DoD Directive 5240.1 (reference (b)) and DoD 5240.1-R (reference (f)).

E3.3. MILITARY PREPAREDNESS

Assistance may not be provided under this enclosure if such assistance could adversely affect national security or military preparedness. The implementing documents issued by the Secretaries of the Military Departments and the Directors of the Defense Agencies shall ensure that approval for the disposition of equipment is vested in officials who can assess the impact of such disposition on national security and military preparedness.

E3.4. APPROVAL AUTHORITY

Requests by civilian law enforcement officials for DoD assistance in civilian law enforcement functions shall be forwarded to the appropriate approval authority under the guidance in this section.

E3.4.1. Approval authority for military assistance if there is a civil disturbance or related matters requiring immediate action is governed by DoD Directive 3025.12 (reference (l)).

E3.4.2. Approval authority for assistance to the government of the District of Columbia is governed by DoD Directive 5030.46 (reference (u)).

E3.4.3. The following governs approval for assistance to civilian law enforcement officials in other circumstances:

E3.4.3.1. Requests for training, expert advice, or use of personnel to operate or maintain equipment shall be forwarded for consideration under section E4.5.of enclosure E4.

E3.4.3.2. Requests for DoD intelligence components to provide assistance shall be forwarded for consideration under DoD Directive 5240.1 (reference (b)) and DoD 5240.1-R (reference (f)).

E3.4.3.3. Loans under the Economy Act (reference (i)) are limited to agencies of the Federal Government. Leases under 10 U.S.C. 2667 (reference (d)) may be made to entities outside the Federal Government.

E3.4.3.3.1. Requests for arms, ammunition, combat vehicles, vessels, and aircraft are subject to approval by the Secretaries of the Military Departments and the Directors of Defense Agencies. A notice of approval or denial shall be reported to the ASD(FM&P) within 48 hours after such action.

E3.4.3.3.2. Requests for loan or lease or other use of equipment or facilities are subject to approval by the Secretaries of the Military Departments and the Directors of the Defense Agencies, unless approval by a higher official is required by statute or DoD Directive applicable to the particular disposition. This authority may be delegated. The Secretaries of the Military Departments and the Directors of the Defense Agencies shall issue rules for taking action on requests for loan, lease, or other use of equipment or facilities that are not governed by paragraphs E3.4.3.1. through E3.4.3.3., above, subject to the following:

E3.4.3.3.2.1. Such rules shall ensure compliance with applicable statutes and DoD Directives requiring specific levels of approval with respect to particular dispositions.

E3.4.3.3.2.2. The ASD(FM&P) shall be notified within 48 hours after action is taken approving or denying a request for a loan, lease, or other use of equipment or facilities for more than 60 days.

E3.4.3.4. Requests for the use of equipment or facilities outside the Continental United States (CONUS) other than arms, ammunition, combat vehicles, vessels, and aircraft shall be approved in accordance with procedures established by the applicable Military Department or Defense Agency.

E3.4.3.5. Requests from Federal agencies for purchase of equipment (permanent retention) that are accompanied by appropriate funding documents may be submitted directly to the Military Departments or Defense Agencies. Requests for transferring equipment to non-Federal agencies must be processed under DoD Instruction 4160.23 (reference (m)) or DoD Directive 4165.20 (reference (p)).

E3.4.3.6. All requests, including those in which subordinate authorities recommend denial, shall be submitted promptly to the approving authority using the format and channels established by the ASD(FM&P). Requests will be forwarded and processed according to the urgency of the situation.

E3.5. FUNDING

Funding requirements for assistance under this enclosure shall be established under the guidance in enclosure E5.

E4. ENCLOSURE 4

RESTRICTIONS ON PARTICIPATION OF DoD PERSONNEL IN CIVILIAN LAW ENFORCEMENT ACTIVITIES

E4.1. STATUTORY REQUIREMENTS

E4.1.1. Posse Comitatus Act. The primary restriction on military participation in civilian law enforcement activities is the Posse Comitatus Act (reference (v)), which provides:

"Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined not more than \$10,000 or imprisoned not more than two years or both."

E4.1.2. Permissible direct assistance. The following activities are not restricted by reference (v).

E4.1.2.1. Actions that are taken for the primary purpose of furthering a military or foreign affairs function of the United States, regardless of incidental benefits to civilian authorities. This provision must be used with caution, and does not include actions taken for the primary purpose of aiding civilian law enforcement officials or otherwise serving as a subterfuge to avoid the restrictions of reference (v). Actions under this provision may include the following, depending on the nature of the DoD interest and the authority governing the specific action in question:

E4.1.2.1.1. Investigations and other actions related to enforcement of the Uniform Code of Military Justice (UCMJ) (reference (d)).

E4.1.2.1.2. Investigations and other actions that are likely to result in administrative proceedings by the Department of Defense, regardless of whether there is a related civil or criminal proceeding. See DoD Directive 5525.7 (reference (w)) with respect to matters in which the Departments of Defense and Justice both have an interest.

E4.1.2.1.3. Investigations and other actions related to the commander's inherent authority to maintain law and order on a military installation or facility.

E4.1.2.1.4. Protection of classified military information or equipment.

E4.1.2.1.5. Protection of DoD personnel, DoD equipment, and official guests of the Department of Defense.

E4.1.2.1.6. Such other actions that are undertaken primarily for a military or foreign affair's purpose.

E4.1.2.2. Audits and investigations conducted by, under the direction of, or at the request of IG, DoD, 5 U.S.C., Appendix 3, §8(g) (reference (x)), subject to applicable limitations on direct participation in law enforcement activities.

E4.1.2.3. Actions that are taken under the inherent right of the U.S. Government, a sovereign national entity under the U.S. Constitution, to ensure the preservation of public order and to carry out governmental operations within its territorial limits, or otherwise in accordance with applicable law, by force, if necessary. This authority is reserved for unusual circumstances, and will be used only under DoD Directive 3025.12 (reference (l)), which permits use of this power in two circumstances:

E4.1.2.3.1. The emergency authority authorizes prompt and vigorous Federal action, including use of military forces, to prevent loss of life or wanton destruction of property and to restore governmental functioning and public order when sudden and unexpected civil disturbances, disaster, or calamities seriously endanger life and property and disrupt normal governmental functions to such an extent that duly constituted local authorities are unable to control the situation.

E4.1.2.3.2. Protection of Federal property and functions authorizes Federal action, including the use of military forces, to protect Federal property and Federal Government functions when the need for protection exists and duly constituted local authorities are unable or decline to provide adequate protection.

E4.1.2.4. Actions taken pursuant to DoD responsibilities under 10 U.S.C. §§331-334 (reference (d)), relating to the use of the military forces with respect to insurgency or domestic violence or conspiracy that hinders the execution of State or Federal law in specified circumstances. Actions under this authority are governed by DoD Directive 3025.12 (reference (l)).

E4.1.2.5. Actions taken under express statutory authority to assist officials in executing the laws, subject to applicable limitations. The laws that permit direct military participation in civilian law enforcement, include the following:

E4.1.2.5.1. Protection of national parks and certain other Federal lands. See 16 U.S.C. §§23, 78, and 593 (reference (y)).

E4.1.2.5.2. Enforcement of the Fishery Conservation and Management Act of 1976. See 16 U.S.C. §1861(a) (reference (y)).

E4.1.2.5.3. Assistance in the case of crimes against foreign officials, official guests of the United States, and other internationally protected persons. See 18 U.S.C. §§112 and 1116 (reference (z)).

E4.1.2.5.4. Assistance in the case of crimes against members of Congress. See 18 U.S.C. §351 (reference (z)).

E4.1.2.5.5. Assistance in the case of crimes involving nuclear materials. See 18 U.S.C. §831 (reference (z)).

E4.1.2.5.6. Protection of the President, Vice President, and other designated dignitaries. See 18 U.S.C. §§1751 and the Presidential Protection Assistance Act of 1976 (reference (z)).

E4.1.2.5.7. Actions taken in support of the neutrality laws. See 22 U.S.C. §§408 and 461-462 (reference (aa)).

E4.1.2.5.8. Removal of persons unlawfully present on Indian lands. See 25 U.S.C. §180 (reference (bb)).

E4.1.2.5.9. Execution of quarantine and certain health laws. See 42 U.S.C. §97 (reference (cc)).

E4.1.2.5.10. Execution of certain warrants relating to enforcement of specified civil rights laws. See 42 U.S.C. §1989 (reference (cc)).

E4.1.2.5.11. Removal of unlawful inclosures from public lands. See 43 U.S.C. §1065 (reference (dd)).

E4.1.2.5.12. Protection of the rights of a discoverer of a guano island. See 48 U.S.C. §1418 (reference (ee)).

E4.1.2.5.13. Support of territorial governors if a civil disorder occurs. See 48 U.S.C. §§1422 and 1591 (reference (ee)).

E4.1.2.5.14. Actions in support of certain customs laws. See 50 U.S.C. §220 (reference (ff)).

E4.1.3. Restrictions on Direct Assistance. Except as otherwise provided in this enclosure, the prohibition on the use of military personnel "as a posse comitatus or otherwise to execute the laws" prohibits the following forms of direct assistance:

E4.1.3.1. Interdiction of a vehicle, vessel, aircraft, or other similar activity.

E4.1.3.2. A search or seizure.

E4.1.3.3. An arrest, apprehension, stop and frisk, or similar activity.

E4.1.3.4. Use of military personnel for surveillance or pursuit of individuals, or as undercover agents, informants, investigators, or interrogators.

E4.1.4. Training

E4.1.4.1. The Military Departments and Defense Agencies may provide training to Federal, State, and local civilian law enforcement officials. Such assistance may include training in the operation and maintenance of equipment made available under section E3.1. of enclosure E3. This does not permit large scale or elaborate training, and does not permit regular or direct involvement of military personnel in activities that are fundamentally civilian law enforcement operations, except as otherwise authorized in this enclosure.

E4.1.4.2. Training of Federal, State, and local civilian law enforcement officials shall be provided under the following guidance:

E4.1.4.2.1. This assistance shall be limited to situations when the use of non-DoD personnel would be unfeasible or impractical from a cost or time perspective and would not otherwise compromise national security or military preparedness concerns.

E4.1.4.2.2. Such assistance may not involve DoD personnel in a direct role in a law enforcement operation, except as otherwise authorized by law.

E4.1.4.2.3. Except as otherwise authorized by law, the performance of such assistance by DoD personnel shall be at a location where there is not a reasonable likelihood of a law enforcement confrontation.

E4.1.5. Expert Advice. Military Departments and Defense Agencies may provide expert advice to Federal, State, or local law enforcement officials in accordance with 10 U.S.C. §§371-378 (reference (d)). This does not permit regular or direct involvement of military personnel in activities that are fundamentally civilian law enforcement operations, except as otherwise authorized in this enclosure.

E4.1.6. Use of DoD Personnel to Operate or Maintain Equipment. The use of DoD personnel to operate or maintain or to assist in operating or maintaining equipment shall be limited to situations when the training of non-DoD personnel would be unfeasible or impractical from a cost or time perspective and would not otherwise compromise national security or military preparedness concerns.

E4.1.6.1. In general, the head of the civilian law enforcement agency may request a Military Department or Defense Agency to provide DoD personnel to operate or maintain or assist in operating or maintaining equipment for the civilian agency. This assistance shall be subject to the following guidance:

E4.1.6.1.1. Such assistance may not involve DoD personnel in a direct role in a law enforcement operation (see subsection E4.1.3., above), except as provided in paragraph E4.1.6.3., below, or as otherwise authorized by law.

E4.1.6.1.2. Except as otherwise authorized by law, the performance of such assistance by DoD personnel shall be at a location where there is not a reasonable likelihood of a law enforcement confrontation.

E4.1.6.1.3. The use of military aircraft to provide point-to-point transportation and training flights for civilian law enforcement officials may be provided only in accordance with DoD 4515.13-R (reference (h)).

E4.1.6.2. Additional provisions concerning drug, customs, immigration, and certain other laws: a request under this provision for DoD personnel to operate or maintain or to assist in operating or maintaining equipment made available under section E3.1. of enclosure E3. may be made by the head of a civilian agency empowered to enforce the following laws:

E4.1.6.2.1. The Controlled Substances Act (reference (gg)) or the Controlled Substances Import and Export Act (reference (hh)).

E4.1.6.2.2. Any of Sections 274 through 278 of the Immigration and Nationality Act (reference (ii)).

E4.1.6.2.3. A law relating to the arrival or departure of merchandise, as defined in Section 1401 of the Tariff Act of 1930 (reference (jj)), into or out of the Customs territory of the United States, as defined in the Tariff Schedules of the United States, (reference (jj)) or any other territory or possession of the United States; or

E4.1.6.2.4. Any other law that establishes authority for DoD personnel to provide direct assistance to civilian law enforcement officials. In addition to the assistance authorized under this paragraph, the following assistance may be provided:

E4.1.6.2.4.1. DoD personnel may be assigned to operate or assist in operating equipment to the extent the equipment is used for monitoring and communicating to civilian law enforcement officials the movement of air and sea traffic with respect to any criminal violation of the laws specified in paragraph E4.1.2.5., above. This includes communicating information concerning the relative position of civilian law enforcement officials and other air and sea traffic.

E4.1.6.2.4.2. In an emergency circumstance, equipment operated by or with the assistance of DoD personnel may be used outside the land area of the United States (or any Commonwealth, territory, or possession of the United States) as a base of operations by Federal law enforcement officials to facilitate the enforcement of a law in subparagraph E4.1.2.3.1., above, and to transport such law enforcement officials in connection with such operations, subject to the following limitations:

E4.1.6.2.4.2.1. Equipment operated by or with the assistance of DoD personnel may not be used to interdict or interrupt the passage of vessels or aircraft, except when DoD personnel are otherwise authorized to take such action with respect to a civilian law enforcement operation.

E4.1.6.2.4.2.2. There must be a joint determination by the Secretary of Defense and the Attorney General that an emergency circumstance exists under 10 U.S.C. §374(c) (2) (reference (d)). An emergency circumstance may be determined to exist for purposes of this subparagraph only when the size and scope of the suspected criminal activity in a given situation poses a serious threat to the interests of the United States; and enforcement of laws in paragraph E4.1.2.5., above, would be impaired seriously if the assistance described in this subparagraph were not provided.

E4.1.6.2.4.3. The emergency authority in this subparagraph may be used only with respect to large scale criminal activity at a particular point in time or over a fixed period. It does not permit use of this authority on a routine or extended

basis.

E4.1.6.2.4.4. Nothing in this subparagraph restricts the authority of military personnel to take immediate action to save life or property or to protect a Federal function as provided in paragraph E4.1.2.2., above.

E4.1.6.3. When DoD personnel are otherwise assigned to provide assistance with respect to the laws specified in paragraph E4.1.2.5., above, the participation of such personnel shall be consistent with the limitations in such laws, if any, and such restrictions as may be established by the Secretary of Defense, the ASD(FM&P), or the Secretaries of the Military Departments and the Directors of the Defense Agencies concerned.

E4.1.7. Other Permissible Assistance. The following forms of indirect assistance are not restricted by the Posse Comitatus Act (reference (d)) (see enclosure E3.):

E4.1.7.1. Transfer of information acquired in the normal course of military operations. See enclosure E2.

E4.1.7.2. Such other actions, approved in accordance with procedures established by the Secretaries of the Military Departments and the directors of the Defense Agencies concerned, that do not subject civilians to use military power that is regulatory, prescriptive, or compulsory.

E4.2. EXCEPTIONS BASED ON STATUS

The restrictions in section E4.1., above, do not apply to the following persons:

E4.2.1. A member of a Reserve component when not on active duty, active duty for training, or inactive duty for training.

E4.2.2. A member of the National Guard when not in the Federal Service.

E4.2.3. A civilian employee of the Department of Defense. If the civilian employee is under the direct command and control of a military officer, assistance will not be provided unless it would be permitted under section E4.3., below.

E4.2.4. A member of a Military Service when off duty, and in a private capacity. A member is not acting in a private capacity when assistance to law enforcement

officials is rendered under the direction or control of DoD authorities.

E4.3. EXCEPTIONS BASED ON MILITARY SERVICE

DoD guidance on the Posse Comitatus Act (reference (v)), as stated in enclosure E3., is applicable to the Department of the Navy and the Marine Corps as a matter of DoD policy, with such exceptions as may be provided by the Secretary of the Navy on a case-by-case basis.

E4.3.1. Such exceptions shall include requests from the Attorney General for assistance under 21 U.S.C. §873(b) (reference (kk)).

E4.3.2. Prior approval from the Secretary of Defense shall be obtained for exceptions that are likely to involve participation by members of the Navy or Marine Corps in an interdiction of a vessel or aircraft, a law enforcement search or seizure, an arrest, apprehension, or other activity that is likely to subject civilians to use military power that is regulatory, prescriptive, or compulsory. Such approval may be granted only when the head of the civilian agency concerned verifies that:

E4.3.2.1. The size or scope of the suspected criminal activity poses a serious threat to the interests of the United States and enforcement of a law within the jurisdiction of the civilian agency would be impaired seriously if the assistance were not provided because civilian assets are not available to perform the missions; or

E4.3.2.2. Civilian law enforcement assets are not available to perform the mission and temporary assistance is required on an emergency basis to prevent loss of life or wanton destruction of property.

E4.4. MILITARY PREPAREDNESS

Assistance may not be provided under this enclosure if such assistance could adversely affect national security or military preparedness. The implementing documents issued by the Secretaries of the Military Departments and the Directors of the Defense Agencies shall ensure that approval for the disposition of equipment is vested in officials who can assess the impact of such disposition on national security and military preparedness.

E4.5. APPROVAL AUTHORITY

Requests by civilian law enforcement officials for use of DoD personnel in civilian law enforcement functions shall be forwarded to the appropriate approval authority under the guidance in this section.

E4.5.1. The use of DoD personnel in civil disturbances and related matters is governed by DoD Directive 3025.12 (reference (l)), which includes the approval authorities.

E4.5.2. Approval authority for assistance to the government of the District of Columbia is governed by DoD Directive 5030.46 (reference (u)).

E4.5.3. The following governs approval for assistance to civilian law enforcement officials in other circumstances.

E4.5.3.1. The Secretary of Defense is the approval authority for requests that involve assignment of 50 or more DoD personnel or a period of assignment of more than 30 days.

E4.5.3.2. The Secretaries of the Military Departments and Directors of Defense Agencies may approve the following types of assistance, except as provided in E4.5.3.1., above:

E4.5.3.2.1. Use of DoD personnel to provide training or expert advice in accordance with subsections E4.1.4. and E4.1.5., above.

E4.5.3.2.2. Use of DoD personnel for equipment maintenance in accordance with subparagraph E4.1.6.2.1., above.

E4.5.3.2.3. Use of DoD personnel to monitor and communicate the movement of air and sea traffic in accordance with subparagraph E4.1.6.2.1., above.

E4.5.3.3. The ASD(FM&P) is the approval authority for other requests for assignment of personnel. This authority may be delegated to the Secretaries of the Military Departments and the Directors of the Defense Agencies with respect to specific categories of assistance.

E4.5.3.4. Requests that involve DoD intelligence components are subject to the limitations in DoD Directive 5240.1 (reference (b)) and DoD 5240.1-R (reference (f)), and are subject to approval by the Secretary of Defense.

E4.5.3.5. The views of JCS shall be obtained on all requests that are considered by the Secretary of Defense or the ASD(FM&P) or that otherwise involve personnel assigned to a Unified or Specified Command.

E4.5.3.6. The view of the ASD(RA) shall be obtained on all requests that are to be considered by the Secretary of Defense or the ASD(FM&P) that involve Reserve component personnel or equipment.

E4.5.3.7. All requests, including those in which subordinate authorities recommend denial, shall be submitted promptly to the approving authority using the format and channels established by the ASD(FM&P). Requests will be forwarded and processed according to priority.

E4.6. FUNDING

Funding requirements for assistance under this enclosure shall be established by the ASD(FM&P) under the guidance in enclosure E5.

E5. ENCLOSURE 5

FUNDING

E5.1. ESTABLISHMENT OF GUIDANCE

Funding requirements and related reporting procedures shall be established by the ASD(FM&P), after consultation with the Assistant Secretary of Defense (Comptroller) (ASD(C)), subject to the guidance of this enclosure.

E5.2. PROCEDURAL REQUIREMENTS

E5.2.1. As a general matter, reimbursement is required when equipment or services are provided to agencies outside the Department of Defense. The primary sources of law for reimbursement requirements are the Economy Act (reference (i)) for Federal agencies and the Leasing Statute, 10 U.S.C. §2667 (reference (d)). Other statutes may apply to particular types of assistance. (See section E3.1. of enclosure E3.)

E5.2.2. If reimbursement is not required by law for a particular form of assistance, the authority to waive reimbursement is delegated to the ASD(FM&P). The ASD(FM&P) may delegate to the Secretaries of the Military Departments and the Directors of the Defense Agencies (or designees) the authority to waive reimbursement on matters within their approval authority. See 10 U.S.C. §377 (reference (d)). The dollar value of a waiver shall be determined in accordance with Chapter 26 of DoD 7220.9-M (reference (II)). A request for waiver may be granted if reimbursement is not otherwise required by law and:

E5.2.2.1. Is provided as an incidental aspect of the activity that is conducted for military purposes.

E5.2.2.2. Involves the use of DoD personnel in an activity that provides DoD training operational benefits that are substantially equivalent to the benefit of DoD training or operations.

E5.2.3. The Secretary of the Military Department or the Director of the Defense Agency (or his or her designees) may request the views of the Joint Chiefs of Staff when acting on a request for waiver of reimbursement when such waiver may adversely affect military preparedness.

DODD 5525.5 January 15, 86

E5.2.4. In evaluating requests for waiver of reimbursement, consideration shall be given to the budgetary resources available to civilian law enforcement agencies.

E5.3. MILITARY PREPAREDNESS

Reimbursement may not be waived if deletion of such funds from a DoD account could adversely affect the national security or military preparedness of the United States.

E6. ENCLOSURE 6

Sample Format for Preparing, "Report on Support
to Civilian Law Enforcement (RCS DD-FM&P (Q) 1595)"

The quarterly report shall contain the following information for each request considered:

1. Number and type of assistance requested.
 - a. Facilities.
 - b. Information.
 - c. Equipment.
 - (1) Aircraft
 - (2) Vehicles
 - (3) Vessels
 - (4) Special (night vision goggles, weapons, etc.)
 - (5) Miscellaneous
 - d. Aviation Mission Support.
 - (1) Surveillance
 - (2) Identification aircraft support
 - (3) Logistics
 - (4) Miscellaneous
 - e. Surface Mission Support.
 - (1) Surveillance

etc.) (2) Ship services (towing, tactical law enforcement teams TACLETs,

(3) Logistics

(4) Miscellaneous

f. Ground-based Mission Support.

(1) Radar/Sensor Surveillance

(2) Aerostats

(3) Transportation of law enforcement personnel

(4) Border air and ground surveillance

(5) Logistics

(6) Miscellaneous

g. Explosive Ordnance Disposal.

h. Training provided to law enforcement agencies.

i. Personnel.

j. Other support not specifically addressed.

2. The length of time for which assistance is requested, if appropriate (if the request is for information or support for a brief time, enter "NA").

3. Status of the requests:

a. Number approved.

b. Number denied.

c. Number pending.

4. A brief discussion of the reason for any denial.

DODD 5525.5 January 15, 86

5. Manhours/mandays expended to support law enforcement agencies.

DODD 5525.5 January 15, 86

E7. ENCLOSURE 7AVIATION ASSISTANCE TO LAW ENFORCEMENT AGENCIES(Sample Format)Surveillance

Detections

Aircraft	Region State	Sorties	Flight Hours	Gained	Passed to LEA's	Remarks
E-2C	Pacific	18	76	10A	9	No CS support available
E-2C	Atlantic	23	88	13A	10	CHET successful intercept of one acft. Flown by Reserves.
P-3C	Atlantic	103	712	32S	28S	CG seized 3 vessels.

Identification

Aircraft	Region State	Sorties	Flight Hours	Visual/IRDS Attempts	Detections Successful	Remarks
OV-10	New Mexico	17	35	3A	1	Handover to USCS, 1200# Marijuana seized.

Logistics/Miscellaneous Support

Aircraft	Region State	Sorties	Flight Hours	Remarks
UH-1N	Bahamas	332	299	Bahamas police seized 12,200# marijuana, 2000# cocaine.
RF-4C	Texas	4	7	Reconnaissance of remote airfields

Abbreviation Key:

A - Airborne	SS - Secret Service
Acft- Aircraft	Res - Reserve
S - Surface	ANG - Air Nat'l Guard
L - Land	ARNG - Army Nat'l Guard
C S - U.S. Customs Service	LEA - Law Enforcement Agency
CG - U.S. Coast Guard	CHET - Customs High Endurance Tracker (aircraft)
D - DEA	IRDS - Infrared Detection System

DODD 5525.5 January 15, 86

Attachments - 1

1. Aid for Completing Aviation Assistance Portion of Quarterly Report 7-1.

DODD 5525.5 January 15, 86

E7.A1. ENCLOSURE 7, ATTACHMENT 1AID FOR COMPLETING AVIATION ASSISTANCE PORTION OF QUARTERLY REPORT

Aviation assistance is the largest area of DoD support to law enforcement agencies. This section is used to report to DoD the Services' aviation assistance. The following is an aid to complete this section.

Acft	-	Aircraft, " if flown by other than active duty units, indicate in the "Remarks" column (e.g., Res, ANG, ARNG).
Region State	-	Where sorties were flown. (e.g., Pacific, Caribbean, GA, TX, Bahamas, etc.).
Sorties	-	Number of flights flown by the platform aircraft during the quarter.
Flt Hrs.	-	Number of flight hours flown by the aircraft during the quarter.
Detections	-	Number of "raw data" detections against suspect air Gained or surface vessels.
Detections Gained	-	The number of detections passed to law enforcement agency for possible investigation.
Remarks	-	Used for comments to specify sorties flown by Reserve, ARG, ARNG units; amplify support contributing to known law enforcement success or failure, etc.
Visual/IRDS	-	Applies to visual or infrared detection to identify suspect vessel.
Identification	-	Aircraft (e.g., OV-10, OV-1) used to identify suspect aircraft prior to handover To the U.S. Customs Service tracker/interceptor aircraft.



DEPARTMENT OF THE NAVY

OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

SECNAVINST 5430.107
NCIS
28 DEC 2005

SECNAV INSTRUCTION 5430.107

From: Secretary of the Navy

Subj: MISSION AND FUNCTIONS OF THE NAVAL CRIMINAL
INVESTIGATIVE SERVICE

Ref: (a) Title 10 USC § 5013
(b) Title 10 USC § 7480
(c) Title 10 USC § 375
(d) SECNAVINST 5430.7N
(e) SECNAVINST 5820.7B
(f) through (dd), see Enclosure (1)

Encl: (1) References, continued.

1. Purpose. To set forth the authority, responsibilities, mission and functions of the Naval Criminal Investigative Service (NCIS) and its relationship with other Department of the Navy (DON) organizations and activities.

2. Cancellation. SECNAVINST 5520.3B

3. Definitions. As used in this instruction, the following definitions pertain:

a. Combating Terrorism: All actions including antiterrorism (defensive measures to reduce vulnerability to terrorist acts), counterterrorism (offensive measures taken to prevent, deter and respond to terrorism), terrorism consequence management (preparation for and response to the consequences of a terrorist incident or event), and intelligence support (collection and dissemination of terrorism-related information) taken to oppose terrorism throughout the entire threat spectrum, to include terrorist use of chemical, biological, radiological, nuclear materials, or high-yield explosive devices (CBRNE).

b. Counterintelligence (CI): Information gathered or activities conducted to protect against espionage, other

SECNAVINST 5430.107

28 DEC 2005

intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.

c. Criminal Operations: Efforts to acquire intelligence about or interdict criminal activities or enterprises that significantly affect the naval establishment, through the use of specialized investigative techniques or equipment, including: the employment of undercover agents; the formal registration or tasking of sources; technical surveillance equipment and investigative tools; oral, wire, and electronic intercepts; pen registers; trap and trace devices; and other sophisticated practices for surfacing and interdicting crime.

d. Critical Program Information (CPI): Information, technologies, or systems that, if compromised, would degrade combat effectiveness, shorten the expected combat-effective life of the system, or significantly alter program direction. This includes classified military information or unclassified controlled information about such programs, technologies, or systems.

e. Fraud Against the Government: A category of major criminal offenses characterized by intentional deception designed to unlawfully deprive the United States (U.S.) of something of value or to seek from the U.S. a benefit, privilege, allowance or consideration to which a person is not entitled.

f. Infrastructure Protection Operations: Offensive cyber-related operations involving DON computer networks designed to counter and identify foreign intelligence, international terrorist, fraud, and criminal activity targeting or involving DON computers and networks.

g. Investigation: The application of law enforcement and/or counterintelligence authorities and methodologies to conduct a detailed, sustained, structured, and objective inquiry to ascertain the truth about an event, situation, or individual.

h. Joint Operations Area (JOA): An area of land, sea, and airspace, defined by a geographic combatant commander or subordinate unified commander, in which a joint force

SECNAVINST 5430.107

28 DEC 2005

commander (normally a joint task force commander) conducts military operations to accomplish a specific mission.

i. Major Criminal Offense: Any offense punishable under the Uniform Code of Military Justice (UCMJ), or similarly framed federal, state, local, or foreign statutes, by confinement for a term of more than one year.

j. Purely Military Offense: An act that is a criminal offense under the UCMJ solely because of the status of the offender, such as desertion, unauthorized absence, fraternization, etc.

k. Threat Warning and Analysis: All actions taken to provide early indications and warning of terrorist, foreign intelligence, criminal, security, and cyber threats, to include analysis, production, and dissemination, in an effort to prevent, mitigate, or warn DON or Department of Defense (DOD) forces of possible hostile or threatening activities.

4. Background. Reference (a) provides the statutory basis for the Secretary of the Navy in conducting "all affairs of the Department of the Navy." In executing this authority, the Secretary must often rely on prompt investigative action by professionally trained personnel for the effective investigation and resolution of alleged, suspected, or actual criminal offenses, terrorist or intelligence threats, and security compromises. Moreover, good order, discipline, and the security of naval forces, operations, information, automated networks, and facilities are the responsibility of command. Commanders require timely and actionable information, and when necessary, the preservation of an evidentiary foundation in order to ensure effective command decisions and action. Under the authority of the Secretary of the Navy, NCIS has primary investigative and counterintelligence jurisdiction within the DON for the above offenses and incidents, on and off naval installations and aboard ships, except as noted elsewhere in this instruction. This jurisdiction is grounded in federal statutes, Executive Orders, and DOD and Secretary of the Navy policy.

5. Organization

a. General: The Director, NCIS reports directly to the Secretary of the Navy. Headquarters NCIS is an Echelon 2 activity. Consistent with references (b) through (e), the Under Secretary of the Navy, with the assistance of the

SECNAVINST 5430.107

28 DEC 2005

General Counsel of the Navy, shall have responsibility for oversight of NCIS and shall serve as chair of the NCIS Board of Directors. In addition, the Director, NCIS serves as Special Assistant for Naval Investigative Matters and Security to the Chief of Naval Operations (CNO) (N09N).

b. Authority over Organizational Matters: The Director, NCIS, is authorized to organize, assign, and reassign responsibilities among NCIS subordinate activities.

c. NCIS Board of Directors (BOD): To assist the Secretary in providing DON corporate governance and in aligning NCIS resources and requirements across the spectrum of NCIS mission areas in order to ensure maximum feasible NCIS support for all DON components, the Under Secretary shall, on a regular basis, convene an NCIS BOD which he shall chair and which shall be further comprised of the DON General Counsel; the Vice Chief of Naval Operations; the Assistant Commandant of the Marine Corps; and the Director, NCIS. The NCIS BOD shall:

(1) Review and validate NCIS Strategic Plans.

(2) Identify, validate, and prioritize requirements relating to NCIS' core mission areas of investigating major criminal offenses (felonies), counterintelligence, combating terrorism, law enforcement, and security.

(3) Assess the adequacy of NCIS resources and coordinate their allocation, as required, to respond to changing threats and mission demands.

(4) Address, as necessary, NCIS requirements that exceed core mission response capabilities, including issues associated with special means to support sensitive NCIS operations.

(5) Ensure that such mechanisms as are necessary to support the BOD in its assessment of NCIS requirements and capabilities and in addressing NCIS resource and mission issues are in place.

(6) Assess the effectiveness of NCIS' linkage and coordination with other DON, DOD, and federal law enforcement, intelligence, and investigative entities.

SECNAVINST 5430.107

28 DEC 2005

(7) Review and evaluate such other areas as the BOD may determine.

6. Authority and Responsibility

a. The Director, NCIS is the senior official for criminal investigations, counterintelligence, and security within the DON. Furthermore, the Director, NCIS is the senior official within the DON for terrorism investigations and related operations designed to identify, detect, neutralize, or prevent terrorist planning and activities, and provides antiterrorism expertise and services to DON components. NCIS performs its duties under the authority of the Secretary of the Navy. NCIS initiates, conducts, and directs criminal, counterintelligence, terrorism and related investigations and operations as deemed appropriate, regardless of command authorization, pursuant to references (f) and (g). Moreover, NCIS conducts the full range of counterintelligence activities as delineated in references (h), (i), and (j). NCIS shall routinely ensure Navy and Marine Corps component commanders are apprised of NCIS CI activities per reference (j). The Director, NCIS shall advise the CNO and Commandant of the Marine Corps (CMC) on these matters in a timely manner and may provide the CNO and CMC information on such matters directly if necessary. NCIS shall establish and employ Security Training Assistance and Assessment Teams (STAAT) to conduct antiterrorism activities and law enforcement/security training.

b. Relationship with other DON Components and Activities: Successful resolution of criminal investigations and the effective identification of threats to the DON require timely notification and referral to NCIS, the cooperation of DON organizations and the protection of information regarding NCIS activities.

(1) DON commands and activities shall:

(a) Immediately refer to NCIS any incidents of actual, suspected, or alleged major criminal offenses, to include espionage, acts of terrorism, and all instances of suspicious activities or anomalies that might indicate the involvement of a foreign government or terrorist organization, regardless of whether they occur on or off an installation or ship or are being investigated by other authorities. Referrals must be made prior to any substantive investigative steps by the command, to include interrogation of suspects and

SECNAVINST 5430.107

28 DEC 2005

searches where individuals have an expectation of privacy, unless such investigative actions are necessary to protect life or property or prevent the destruction of evidence. The requirement for immediate referral shall not preclude efforts by first responders to safeguard personnel, secure crime scenes, or take other emergency responses in exigent circumstances. In those rare instances when immediate response by NCIS is not feasible, such as a submarine on patrol, commanding officers shall conduct such preliminary investigations as circumstances dictate, preparatory to a full investigation by NCIS. NCIS shall immediately be notified (where security considerations do not dictate otherwise) to facilitate NCIS guidance to commands. Appropriate measures will be taken to ensure the preservation and accounting of possible evidence and to avoid any action that might prejudice investigative possibilities or impair the judicial process. Offenses, incidents, anomalies, and other situations requiring immediate referral to NCIS are further identified in paragraph 7b.

(b) Respond to any NCIS request for information or assistance pursuant to an authorized investigation or operation as if made by the Secretary, including providing access to installations, information and records as specified in paragraph 6e.

(c) Not impede the use of investigative techniques deemed necessary and permissible under law or regulation by NCIS.

(d) Facilitate NCIS use of DON personnel as sources or in other undercover roles in investigations and operations targeting criminal, foreign intelligence, and terrorist activities whenever practicable. NCIS shall obtain initial concurrence of the commander or commanding officer prior to tasking a military member to perform in support of these operations. Use of DON civilian employees and contractors do not require command concurrence. Special considerations may apply in the case of individuals indoctrinated for access to Sensitive Compartmented Information (SCI). Where operational activities present a significant safety risk to other personnel, NCIS shall inform the installation commander, unless specific circumstances dictate otherwise.

(e) Ensure that NCIS information regarding investigations, operations, and related activities is not

SECNAVINST 5430.107

28 DEC 2005

compromised by command personnel, and to the extent possible, is limited to senior command personnel.

(f) Provide required logistical and communications support, within the limits of other operational commitments, when NCIS personnel are deployed with any naval unit.

(2) The Naval Inspector General (NAVINSGEN): Whenever the NAVINSGEN requests investigative assistance from the Director, NCIS on a priority basis, such request will be made in writing. The NAVINSGEN and the Director, NCIS shall, to the extent possible, provide each other the results of investigative activity when such information impacts the mission and functions of the other. Any disagreement between the NAVINSGEN and the Director, NCIS regarding the sharing of information or the conduct of a particular investigation shall be referred to the Secretary of the Navy for resolution. This relationship also applies to the Deputy Naval Inspector General for Marine Corps Matters.

(3) The Director of Naval Intelligence (DNI): The DNI serves as the DON sponsor for National Intelligence Program and Military Intelligence Program resources and is responsible for the development of counterintelligence policy in coordination with the Marine Corps Director of Intelligence (DIRINT) and Director, NCIS. The Director, NCIS shall support the DNI as set forth in reference (j). The Director, NCIS and the DNI shall also ensure the interoperability of intelligence, counterintelligence, and law enforcement related databases, systems, and capabilities to the maximum extent possible.

(4) Marine Corps Counterintelligence Elements: Reference (j) defines the relationship between NCIS and Marine Corps counterintelligence elements.

(5) Command Investigators: Many Navy and Marine Corps commands maintain an organic investigative capability. Use of command investigators for criminal and security investigations shall be limited to minor offenses (punishable by one year or less confinement), purely military offenses as defined herein, or cases that NCIS has declined to investigate. NCIS may enter into agreements with Navy and Marine Corps commands regarding command investigations into offenses meeting the definition of a major criminal offense.

SECNAVINST 5430.107

28 DEC 2005

These agreements, however, shall not prevent NCIS from assuming jurisdiction in the investigation of any offense.

(6) Command Investigations Conducted under the Manual of the Judge Advocate General (JAGMAN): Command investigations conducted under the JAGMAN shall not compromise or otherwise impede any NCIS investigation. If, during the conduct of an NCIS investigation, a commanding officer deems it necessary to proceed with a command investigation, that decision must first be coordinated with NCIS. If NCIS objects to the initiation of a command investigation, it will be suspended and the matter referred for resolution to the officer exercising general court-martial authority.

(7) Assistant General Counsel (Acquisition Integrity) (AGC(AI)): Within the DON, AGC(AI) is responsible for coordinating investigative, inspection-related, and audit-related efforts to assure the integrity of DON acquisition processes. NCIS shall support these efforts and forward matters under AGC(AI) cognizance to that office for action, as appropriate.

c. Relationships with the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA): Joint criminal investigations and counterintelligence activities within the United States conducted with the FBI are governed by Memorandums of Agreement between the Department of Justice (DOJ) and the DOD. Certain counterintelligence activities conducted overseas are conducted in coordination with the Central Intelligence Agency pursuant to Director of Central Intelligence Directive (DCID) 5/1, Espionage and Counterintelligence Activities Abroad, and a Memorandum of Agreement between the CIA and the DOD. These documents designate NCIS as having exclusive responsibility within the DON for coordinating and conducting the activities identified therein. USMC CI elements may conduct CI activities that do not require DCID 5/1 coordination in support of deployed Marine Corps forces, and shall do so in accordance with reference (j). When USMC CI elements conduct liaison with U.S. and foreign officials in support of deployed and deploying forces, they shall apprise the nearest NCIS element of the conduct of this activity.

d. Credentials and Badges: The Director, NCIS is authorized to issue credentials and badges to NCIS personnel accredited to perform investigations and related activities. DON personnel who are not duly accredited by the Director,

SECNAVINST 5430.107

28 DEC 2005

NCIS to perform such activities are prohibited from making any representation that indicates NCIS accreditation.

(1) Special Agents carry out the full range of duties associated with criminal investigations, counterintelligence activities, and other related activities. They are issued standardized credentials and badges identifying them as "Special Agents." Use of this title by any other individuals within the DON is prohibited.

(2) NCIS may seek to have agents from Marine Corps Criminal Investigation Division assigned to NCIS for duty as Special Agents. Marine Special Agents so assigned will carry NCIS credentials and badges, conduct criminal investigations under the authority of NCIS, and fall under the operational control of NCIS. While assigned duties with NCIS, Marine Special Agents may be authorized to undertake official duties in a manner that disassociates them from identification as a military member. Given their military status, Marine Special Agents may not exercise the arrest authorities extended to NCIS civilian Special Agents pursuant to reference (b).

(3) NCIS is supported by the Navy Reserve, which provides personnel to perform investigative and counterintelligence duties. These personnel are issued credentials and badges identifying them as Agents.

(4) NCIS also employs personnel who perform specialized investigative, analytical, and security functions in support of the NCIS mission. These personnel are issued standardized credentials identifying them as Investigators or Operational Representatives.

e. Access to Information and Facilities: Personnel issued NCIS Special Agent credentials have Top Secret security clearances. Special Agents, upon displaying their official credentials, shall be considered as having a need to know and shall be granted access to information, material, or spaces classified up to Top Secret and relevant to the performance of their official duties. This access applies to all types of command files, personnel records, medical records, training records, contract and procurement documents, and computer files and records, without further administrative requirements. As law enforcement officials and as agents of a health oversight agency, Special Agents are authorized to make written investigative demands for medical records in accordance with the requirements of Sections C7.4 and

SECNAVINST 5430.107
28 DEC 2005

C7.6.1.2.3. of reference (k). Access to SCI and Special Access Programs (SAPs) or similarly controlled information, spaces, or material shall be granted to NCIS personnel who have requested such access in advance as part of an authorized investigative, counterintelligence, or security matter and who have been verified as holding the appropriate level security clearance and are indoctrinated for access to SCI or the SAP in question. Prior verification shall be waived in exigent circumstances involving the protection of life or preservation of evidence; however, such verification shall be accomplished as soon as practicable. Consistent with the foregoing, personnel displaying NCIS Special Agent credentials shall be granted full access to Navy and Marine Corps installations, commands, ships, and other naval facilities. NCIS Special Agents who properly identify themselves as such shall, in the course of their official duties, be exempt from all routine searches of their persons, possessions, and materials, as well as vehicles and the occupants therein. Moreover, individuals escorted by a credentialed NCIS Special Agent shall not be required to display identification.

f. Apprehension and Arrest Authority: Reference (l) authorizes NCIS Special Agents, Agents, and Investigators to apprehend persons subject to the UCMJ. Pursuant to reference (b), civilian Special Agents are authorized to execute and serve any warrant or other process issued under the authority of the United States and to make any arrest without a warrant authorized under 10 U.S.C. § 1585a, in accordance with guidelines prescribed by the Secretary of the Navy and approved by the Secretary of Defense and the Attorney General.

g. Weapons: Consistent with reference (m), NCIS Special Agents are authorized to carry NCIS-approved firearms at all times, while on or off duty, and while on and off installations, aircraft, and ships. NCIS Special Agents are required to carry NCIS-approved firearms while on official business, except when in specific "exclusion areas" where special weapons/systems are stored. The need for a Special Agent to carry a firearm in such areas will be left to the discretion of the commander or commanding officer having responsibility for the "exclusion area." In addition, other accredited NCIS personnel may be authorized by the Director, NCIS to carry firearms.

h. Oaths: Those persons accredited by the Director, NCIS as Special Agents, Agents, Investigators, and Operational Representatives are authorized to administer oaths and take

SECNAVINST 5430.107

28 DEC 2005

sworn statements. This authority applies only to official investigative duties in connection with the investigative jurisdiction and responsibilities of NCIS, as set forth in this instruction. This authority is derived from reference (n).

i. Wire, Electronic, and Oral Interceptions for Law Enforcement: Within the DON, NCIS is exclusively authorized to intercept wire, electronic, and oral communications, and to install or use pen register and trap and trace devices for law enforcement in accordance with guidance set forth in reference (o). Within NCIS, only the Director may authorize or deny requests to conduct consensual interceptions of wire, electronic, or oral communications for law enforcement purposes.

j. Law Enforcement Communications: NCIS shall control and manage DON access to and use of the National Law Enforcement Telecommunications System (NLETS), the National Crime Information Center (NCIC), and similar national law enforcement telecommunications systems.

7. Mission and Functions

a. Mission: NCIS is a federal law enforcement agency that protects and defends the DON against terrorism and foreign intelligence threats, investigates major criminal offenses, enforces the criminal laws of the United States and the UCMJ, assists commands in maintaining good order and discipline, and provides law enforcement and security services to the Navy and Marine Corps on a worldwide basis.

b. Functions:

(1) Major Criminal Investigations: Within the DON, NCIS has primary responsibility for investigating actual, suspected, or alleged major criminal offenses, including espionage and acts of terrorism. NCIS shall investigate offenses committed against persons, the U.S. Government, or private property, and attempts or conspiracies to commit such offenses. In addition to all major criminal offenses, NCIS shall investigate the following categories of incidents:

(a) Any non-combat death, on or off naval installations, facilities, vessels, or aircraft, where the cause of death cannot be medically attributable to disease or natural causes. Pursuant to reference (p), NCIS shall

SECNAVINST 5430.107

28 DEC 2005

investigate the circumstances until criminal causality can be reasonably excluded.

(b) Any fire or explosion of unknown origin affecting DON property, or property under DON control.

(c) Incidents involving the loss or theft of ordnance, narcotics, dangerous drugs, or controlled substances.

(d) Missing command members, when foul play cannot be excluded.

(2) Criminal Operations: Within the DON, NCIS shall have exclusive jurisdiction to conduct Criminal Operations as defined herein. Other DON law enforcement elements may conduct activities consistent with their approved authorities and jurisdictional limits.

(3) Fraud Against the Government Offenses: NCIS shall conduct investigations into fraud against the government and has primary jurisdiction within the DON for the investigation of these offenses pursuant to references (q) and (r). The policies, procedures, and responsibilities for determining which DoJ or DOD criminal investigative organization will conduct the investigation of these offenses under the U.S. Code or UCMJ are set forth in reference (s).

(4) Counterintelligence and Counterterrorism Activities:

(a) NCIS shall conduct the full range of counterintelligence activities, as specified in references (i) and (j), to include counterterrorism activities designed to detect, identify and neutralize terrorist planning and activities. NCIS has exclusive investigative jurisdiction into actual, potential, or suspected acts of espionage, terrorism, sabotage, and assassination, or actual, suspected, or attempted defection by DON personnel. This exclusive jurisdiction does not prohibit USMC CI elements from conducting CI preliminary debriefing and reporting while supporting the immediate force protection needs of deployed Marine Corps forces. NCIS shall conduct all counterintelligence activities in accordance with references (j) and (t).

SECNAVINST 5430.107

28 DEC 2005

(b) Reference (t) assigns NCIS the primary responsibility for collecting, processing, storing, and disseminating counterintelligence information regarding U.S. persons, less those activities conducted by Marine Corps counterintelligence elements pursuant to reference (j). All such information obtained by commands will be forwarded to NCIS.

(c) Consistent with references (h) and (j), NCIS has exclusive jurisdiction within the DON to conduct strategic offensive counterintelligence operations (OFCO) designed to counter foreign intelligence or terrorist activities and to support operational commanders, the DON, and national level requirements.

(d) NCIS shall support Research and Technology Protection (RTP) by conducting counterintelligence activities that protect critical program information (CPI), technologies, or systems. The focus of this support is on DON research, development, technology, and evaluation (RDT&E) efforts, designated acquisition programs, and systems currently deployed. NCIS has exclusive jurisdiction within the DON for providing counterintelligence support to RTP, and pursuant to reference (u), commanding officers, program managers, and technical directors responsible for executing program protection plans shall incorporate NCIS Counterintelligence Support Plans when configuring plans for risk mitigation and threat countermeasures.

(5) Threat Warning and Analysis: NCIS shall maintain, direct, and operate the DON Multiple Threat Alert Center (MTAC) to provide Indications and Warning of terrorist, foreign intelligence, cyber, and criminal threats to the DON and to generate related analysis and production on matters of interest to the Department. The MTAC serves as NCIS' fusion center for law enforcement, intelligence, counterintelligence, security, and other threat information required to defeat terrorist, foreign intelligence, criminal, and related threats to DON personnel, installations, facilities, vessels, and aircraft, and it supports the national effort to combat terrorism. In addition, the MTAC serves as NCIS' operational control center, providing direct support to NCIS' investigations and operations as required. MTAC functions include:

(a) Maintaining 24 hour-a-day, 7 day-a-week watch and alert operations to continually monitor national,

SECNAVINST 5430.107

28 DEC 2005

service, theater, and other intelligence and law enforcement information to identify specific threats to DON assets, operations, and activities.

(b) Issuing threat reports, special analyses, intelligence assessments, advisories, and summaries to notify commanders of potential threats.

(c) Providing a centralized capability and locus for coordination of and direct support to NCIS investigations and operations.

(d) Supporting DON's Threat and Local Observation Notice reporting requirements by collecting and reporting this information and serving as the lead component within DON for the distribution of this information.

(6) Internal Security: Reference (u) directs NCIS and local commands to coordinate on the investigation of internal security incidents. The following are among those incidents within the investigative jurisdiction of NCIS:

(a) Loss, compromise or suspected compromise of classified information: Commands shall proceed with a preliminary inquiry, unless the NCIS Special Agent in Charge (SAC) requests that command actions be held in abeyance in order to preserve evidence for a criminal investigation. NCIS shall promptly notify commanders if it will initiate an investigation. NCIS shall document the results of all preliminary inquiries via the NCIS reporting system.

(b) Any request for classified information other than those made through official channels.

(c) Requests for unclassified information by individuals or organizations associated with a foreign government.

(d) Unofficial contacts with officials of a foreign government or members of an international terrorist organization.

(e) Incidents of suicide or attempted suicide by personnel with access to classified information.

SECNAVINST 5430.107

28 DEC 2005

(f) Incidents where DON personnel with access to classified information are missing or are considered an unauthorized absentee.

(7) Cyber Investigations and Operations: Pursuant to reference (v), NCIS shall maintain a staff skilled in the investigation of computer crime and the evaluation of the foreign intelligence threat to information warfare/command and control warfare (IW/C2W), and shall conduct counterintelligence activities in support of IW/C2W. NCIS has primary jurisdiction within the DON for certain cyber-related functions as they apply to DON computer networks, to include:

(a) Infrastructure protection operations.

(b) Cyber-related criminal investigations regarding unauthorized access, intrusion, denial of service, or viruses/malicious code.

(8) Support to Special Access Programs: NCIS shall assign appropriately cleared and qualified personnel to conduct the full range of counterintelligence activities, as delineated in references (w) and (x), to support DON Special Access Programs (SAPs) and other sensitive compartmented programs. NCIS shall also investigate fraud and other major criminal offenses involving these programs. Consistent with reference (y), commands shall identify and provide validated Critical Program Information (CPI) to enable NCIS to conduct specific and accurate threat analysis to support recommended security countermeasures.

(9) Technical Surveillance Countermeasures: Reference (z) designates NCIS as the DON Technical Surveillance Countermeasures (TSCM) Program Manager. NCIS shall manage TSCM counterintelligence investigative and related activities as delineated in references (z) and (aa). Such activities shall include support to DON critical information and infrastructure protection and technical security assurance.

(10) Naval Security Programs: The Director, NCIS shall serve as Special Assistant for Naval Investigative Matters and Security to the CNO (N09N).

(11) Protective Service Operations: Safe and effective Protective Service Operations require specialized expertise and careful operational coordination. Consistent

SECNAVINST 5430.107

28 DEC 2005

with references (bb) and (cc), NCIS shall serve as the executive agent for all Protective Service matters within the DON and shall execute exclusive jurisdiction and authority to conduct and coordinate Protective Service Operations to protect individuals who occupy designated DON High Risk Billets (HRBs) and other designated individuals, except as otherwise authorized by a combatant commander in a JOA. In addition, NCIS shall perform the following related functions:

(a) Participate in the review and validation of DON HRBs as Subject Matter Experts.

(b) Conduct Personal Security Vulnerability Assessments for designated DON HRBs to determine the level of risk and vulnerability to terrorist or criminal activities, and to determine the appropriate level of protection.

(c) Execute primary jurisdiction within the DON for support to the United States Secret Service and to DOD and non-DOD agencies conducting Protective Service Operations for U.S. government and foreign officials.

(12) Liaison: Within the DON, NCIS has exclusive responsibility for liaison with federal, state, local, and foreign law enforcement, security and intelligence agencies on all criminal investigative, counterintelligence, counterterrorism, and security matters assigned to NCIS by this instruction and its references. Commands may pursue interaction with federal, state, local, and foreign law enforcement, security, and intelligence agencies on antiterrorism matters, but shall do so in coordination with NCIS. Execution of this responsibility shall not limit any of the following:

(a) Contact between Navy and Marine Corps judge advocates and federal, state or local officials to determine prosecutorial jurisdiction and grants of immunity, coordinate pretrial agreements, or take any other action consistent with the duties of judge advocates.

(b) Interaction between commands and federal, state, local, or foreign law enforcement and security officials on routine matters involving physical security, minor offenses, purely military offenses, traffic matters, and training.

SECNAVINST 5430.107

28 DEC 2005

(c) Liaison conducted by Marine Corps counterintelligence elements in accordance with reference (j).

c. Initiation, Reporting and Declination of NCIS Investigations and Operations:

(1) Initiation of Investigations:

(a) NCIS may initiate, independent of command request, any investigative action within the purview of this instruction and need not solicit authorization to conduct any investigation. NCIS shall, however, normally apprise the immediate senior in command (ISIC) of the person or organization being investigated that an investigation has been initiated. Any commander, commanding officer or other appropriate command authority within the Navy or Marine Corps may request NCIS assistance.

(b) Only the Secretary of the Navy may direct NCIS to delay, suspend, or terminate an investigation other than an investigation being conducted at the behest of the DOD Inspector General (IG). Only the DOD IG may direct NCIS to delay, suspend, or terminate an investigation being conducted at the behest of the DOD IG. Objections to NCIS investigations, or requests to delay, suspend, terminate, or discontinue NCIS investigations, shall be administered under the procedures of reference (g).

(2) Dissemination and Retention of Reports: NCIS shall:

(a) Provide to each command, prosecutorial authority or other appropriate activity a full report of investigation regarding any offenses or incidents investigated affecting that entity.

(b) Maintain a central repository for reports of investigation, counterintelligence data and security clearance adjudication files created by the DON Central Adjudication Facility (DON CAF).

(c) Maintain a record of disposition of command disciplinary actions or the actions of civilian judicial authorities. This includes the results of courts-martial, nonjudicial punishments, and actions by civilian criminal or civil proceedings. Commands are required to

SECNAVINST 5430.107

28 DEC 2005

provide the disposition of such cases to NCIS within thirty (30) days of the disposition action.

(d) Ensure all files created under the provisions of this instruction are retained and disposed of pursuant to reference (dd). Only the Director, NCIS may modify, destroy or authorize the modification or destruction of any such file.

(e) Promptly notify affected commanders of any information or aspect of investigative, counterintelligence or security activities indicating an actual or suspected threat to naval operations, personnel, facilities or other assets, or any occurrence which warrants the attention of fleet, component or combatant commanders, the DON/DOD leadership or other seat of government officials.

(f) Support, on a reciprocal basis, other federal, state, local or foreign law enforcement, security or intelligence agencies in lawful actions.

(3) Declination of Investigations: NCIS may, at its discretion, decline to undertake the investigation of a case. If this occurs, NCIS shall expeditiously inform the affected command or activity.

8. Effect of Other Regulations, Directives, Instructions, Notices. All SECNAV, Navy, and Marine Corps regulations, directives, instructions and notices pertaining to the assignment of duties to the former Naval Investigative Service Command (NISCOM), or delegating various authorities to NISCOM, remain in effect. All such responsibilities and delegations are transferred to NCIS as the successor to NISCOM.

9. Action. The Under Secretary of the Navy, CNO and CMC shall take appropriate action to ensure the updating of all regulations, directives, instructions and notices, specifically those involving law enforcement, counterintelligence and security, to comply with this instruction. All addressees shall take such action as is required to ensure compliance with this instruction.

Dionel M. Aviles
Under Secretary of the Navy

SECNAVINST 5430.107

28 DEC 2005

Distribution:

Electronic only, via Navy Directives Web site

<http://neds.daps.dla.mil//>

SECNAVINST 5430.107

28 DEC 2005

REFERENCES, continued

- (f) Public Law 99-145, National Defense Authorization Act, Section 1223, November 8, 1985
- (g) DOD Instruction 5505.3 of 21 June 2002
- (h) Executive Order 12333
- (i) DOD Directive 5240.2 of 22 May 1997
- (j) SECNAVINST 3850.2C
- (k) DOD 6025.18-R of 24 January 2003
- (l) Manual for Courts-Martial, RCM 302
- (m) SECNAVINST 5500.29C
- (n) Title 5 USC § 303(b)
- (o) DOD Directive 5505.9 of 20 April 1995
- (p) DOD Instruction 5505.10 of 31 January 1996
- (q) DOD Instruction 5505.2 of 6 February 2003
- (r) SECNAVINST 5430.92A
- (s) DOD Directive 5525.7 of 22 January 1985
- (t) DOD 5240.1-R of December 1982
- (u) SECNAVINST 5510.36
- (v) SECNAVINST 5239.3A
- (w) DOD Directive 5205.7 of 13 January 1997
- (x) SECNAVINST S5460.3C
- (y) DOD Directive 5200.39 of 10 September 1997
- (z) SECNAVINST 3850.4
- (aa) DOD Instruction 5240.5 of 23 May 1984
- (bb) DOD Directive 2000.12 of 18 August 2003
- (cc) DOD O2000.12-H of February 2004
- (dd) SECNAVINST 5212.5D

Enclosure (1)



DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
WASHINGTON, D.C. 20350-1000

SECNAVINST 5520.3B
NCIS
4 January 1993

SECNAV INSTRUCTION 5520.3B

From: Secretary of the Navy
To: All Ships and Stations

Subj: CRIMINAL AND SECURITY INVESTIGATIONS AND RELATED
ACTIVITIES WITHIN THE DEPARTMENT OF THE NAVY

Ref: (a) Executive Order 12333
(b) DoDI 5505.3 of 11 Jul 86 (NOTAL)
(c) SECNAVINST 3820.2D
(d) SECNAVINST 3850.2B (NOTAL)
(e) JAGINST 5800.7B
(f) DoD Directive 5525.7 of 22 Jan 85 (NOTAL)
(g) DoDI 5505.2 of 16 Jul 90 (NOTAL)
(h) SECNAVINST 5430.92A
(i) OPNAVINST 5510.1H
(j) OPNAVINST C8126.1 (NOTAL)

1. **Purpose.** To restate jurisdiction and responsibility in the conduct of criminal and security investigations and related activities within the Department of the Navy.

2. **Cancellation.** SECNAVINST 5520.3A and SECNAVINST 5520.1B.

3. **Discussion.** Good order and discipline are the direct responsibility of command. In the discharge of this responsibility, commanding officers must frequently rely on prompt investigative action by professionally trained personnel, not only for effective resolution of alleged, suspected, or actual criminal and security offenses, but also to preserve facts and construct an evidentiary foundation for subsequent command action. Under the Secretary of the Navy, the Naval Criminal Investigative Service (NCIS) has primary investigative and counterintelligence jurisdiction within the Department of the Navy, except as noted elsewhere in this instruction. This jurisdiction is grounded and documented in Presidential Executive Order, Department of Defense instructions and Secretary of the Navy instructions, (references (a) through (g)). The Marine Corps maintains a cadre of accredited counterintelligence and investigative personnel who exercise jurisdiction as delimited in this instruction and implemented by Marine Corps directives. NCIS maintains a world-wide field structure which provides

1 KAN 3-93

2 APR 93



0579LD0561490

SECNAVINST 5520.3B

4 JAN 1993

criminal investigative and counterintelligence support to the Navy and Marine Corps both ashore and afloat. In a combat or combat contingency environment, the task force commander afloat and landing force commander ashore exercise immediate control over assigned Navy and Marine Corps investigative and counterintelligence assets. Commands maintain a limited investigative capability for resolving minor offenses and those of a purely military character. This Instruction delineates NCIS's responsibilities and limitations regarding utilization of assets and policy applicable to criminal and security investigations, criminal intelligence operations, counterintelligence activities and technical investigative support matters.

4. Command Relationships. The Director, NCIS reports directly to the Secretary of the Navy. Headquarters, NCIS is an Echelon 2 command under the Office of the Under Secretary of the Navy with day-to-day supervision being provided by the Under Secretary of the Navy. In addition, the Director, NCIS reports to the Chief of Naval Operations for physical, personnel and information security as Special Assistant for Naval Investigative Matters and Security (N09N) and, through the Director of Naval Intelligence, to develop policy for the Navy on foreign counterintelligence as Assistant for Foreign Counterintelligence (N2E).

5. Relationship With The Naval Inspector General. When requested by the Naval Inspector General (NIG) to provide the highest priority to a request for criminal investigative assistance, such request will be in writing and the Director NCIS will notify the Secretary/Under Secretary of the Navy. In addition, the NIG and the Director, NCIS will report back to the Secretary/Under Secretary within 2 working days as to the status of the assistance being provided. When directed by the Secretary/Under Secretary of the Navy, the NIG and the Director, NCIS will exchange all criminal investigative material in an expeditious manner.

6. Responsibilities

a. Major Criminal Offenses

(1) Within the Department of the Navy, NCIS is primarily responsible for investigating actual, suspected or alleged major criminal offenses committed against a person, the United States Government, or private property, including the attempts or conspiracies to commit such offenses. A major criminal offense (felony) is defined for purposes of this instruction as one punishable under the Uniform Code of Military Justice by confinement for a term of more than 1 year, or similarly framed federal statutes, state, local or foreign laws or regulations.

SECNAVINST 5520.3B

4 JAN 1993

Incidents of actual, suspected or alleged major criminal offenses coming to command attention must be immediately referred to NCIS whether occurring on or off an installation or ship and regardless of whether they are being investigated by state, local or other authorities. The referral to NCIS should be made before any substantive investigative steps are considered by the command, such as interrogation of suspect(s) or conducting searches of property, as to which individuals have an expectation to privacy, unless such steps are necessary to protect life or property or to prevent the destruction of evidence. Command investigations conducted under the Manual of the Judge Advocate General (reference (e)) must not compromise or otherwise impede the NCIS investigation. When NCIS is conducting an investigation and the officer in command deems it necessary to proceed with an inquiry under reference (e), that decision must first be communicated to the local NCIS office to establish coordination of the investigative effort. If NCIS objects to the initiation of the inquiry by a command fact-finding body, the command inquiry will be suspended and the matter referred for resolution to the officer exercising general court-martial jurisdiction, or the area coordinator via the chain of command. NCIS shall comply with the referral, reporting, and conferral requirements of the Memorandum of Understanding (MOU) between the Department of Justice and the Department of Defense (DoD) relating to the investigation and presentation of certain crimes, as implemented by reference (f) and other sections of this instruction.

(2) In those rare instances when immediate response by NCIS is not feasible, such as a submarine on patrol or a ship at a remote location, commanding officers shall conduct such preliminary investigations as circumstances dictate, preparatory to a full investigation by NCIS. NCIS shall immediately be notified (where security considerations do not dictate otherwise) to facilitate NCIS guidance to commands. Appropriate measures will be taken to ensure the preservation and accounting of possible evidence and to avoid any action which might prejudice investigative possibilities or otherwise impair the subsequent judicial process. NCIS may decline to undertake investigation of certain cases but must comply with fraud investigation and reporting requirements of references (g) and (h). When this occurs, the requesting command will be expeditiously notified. Examples of situations which may be deferred by NCIS to the command for resolution include the following:

(a) When in NCIS judgment, the inquiry would be fruitless and unproductive.

(b) Any instance in which the suspected felonious offense is purely military in nature such as unauthorized absence.

SECNAVINST 5520.3B

4 JAN 1993

(c) When, in accordance with policy issued by the Director, NCIS, certain lesser offenses may be deferred to the command for investigation because of NCIS priorities or resource limitations.

(3) In addition to referral of major criminal offenses, when any of the following circumstances occur, the command shall promptly provide available information to NCIS for investigation:

(a) Any death occurring on a Navy vessel or Navy/Marine Corps aircraft or installation, except when the cause of death is medically attributable to disease or natural causes. When notified, NCIS will investigate the circumstances until criminal causality can reasonably be excluded.

(b) Any fire or explosion of unknown origin affecting Department of the Navy property or property under Navy or Marine Corps control.

(c) Aspects surrounding a nominal or minor incident of a potentially sensitive nature. Such considerations include, but are not limited to, incidents involving loss of ordnance, narcotics, dangerous drugs or controlled substances; incidents of aberrant sexual behavior involving force/coercion or when children are involved or where special circumstances are present and the command authority desires the help of NCIS resources for resolution of such matters.

(d) Incidents involving loss of ordnance, narcotics, dangerous drugs, or controlled substances; incidents of aberrant sexual behavior involving force/coercion or when children are involved.

(e) Thefts of minor amounts of personal property when ordnance, contraband or controlled substances are involved. On Marine Corps installations, guidance is provided by MOU between NCIS and the Commandant of the Marine Corps.

(f) Disappearance of a command member which may suggest foul play.

(g) All information concerning possible significant cases as discussed and required by references (g) and (h).

(4) A major criminal offense, as defined, may constitute a violation of both military and civil law, and may involve both military personnel and civilians. Primary or concurrent jurisdiction may also rest with another agency outside of the Department of the Navy. Only NCIS has the authority to make investigative referrals in these instances. When Department of

SECNAVINST 5520.3B

4 JAN 1993

the Navy commands or personnel are contacted by other law enforcement organizations in connection with investigative matters, the matter must be referred to NCIS for coordination. This policy includes inquiries by federal, state, local and foreign law enforcement or investigative agencies when the matter involves security or major criminal offenses, as previously defined. This does not preclude Department of the Navy commands from conferring with law enforcement organizations on physical security, loss prevention issues and other matters of mutual concern.

(5) When NCIS personnel are embarked upon any naval vessel, commands shall provide appropriate logistical and communications support within the limits of other operational commitments.

b. Minor Criminal Offenses. A minor criminal offense is defined as one punishable under the Uniform Code of Military Justice by confinement of 1 year or less, or carrying similar punishment by federal, state, local or foreign statute or regulation, and lacking any of the considerations enumerated in the discussion of major criminal offenses above.

c. Use of Command Investigators

(1) Many Navy and Marine Corps commands maintain an investigative capability. Use of command investigators for criminal and security investigations shall be limited to minor offenses, as defined in this instruction, except when NCIS has declined jurisdiction. The Director, NCIS, or his/her designee may from time to time enter into agreements with the Marine Corps or Navy commands regarding command-conducted investigations which meet the definition of major criminal offenses, as defined in this instruction. However, such agreements shall never prevent NCIS from conducting any investigation it deems appropriate and in the best interests of the Department of the Navy. This stipulation does not preclude command investigations in those instances where NCIS is not investigating or where the offense is purely military in nature (e.g. unauthorized absence).

(2) Off-base investigative activities by command investigators shall be limited to minor offenses and to the immediate area surrounding the installation and off-base housing areas. This policy shall not in any way restrict their assigned patrol and law enforcement functions such as preventing the escape or loss of identity of suspected offenders, preserving crime scenes and ensuring the integrity of physical evidence.

d. Criminal Intelligence Operations. Criminal intelligence operations are defined as formalized programs targeting persons

SECNAVINST 5520.3B

4 JAN 1993

or organizations whose criminal activity significantly affects the naval establishment, or those activities designed to gain information of a criminal intelligence nature for law enforcement purposes. A high degree of specialized training and experience is necessary for the successful accomplishment of these operations, and, to the extent that they are undertaken within the Department of the Navy, they will be done exclusively by NCIS, regardless of location. Criminal intelligence operations are undertaken at NCIS initiative, in close coordination with senior command authority. During their course, these sensitive operations may disperse over wide geographic areas and extend across multiple command lines. The cooperation of all commanding officers is necessary to insure the integrity of these operations and enhance the probability of success.

e. **Fraud Matters.** References (f) and (g) establish policies, procedures and responsibilities for determining which Department of Justice or DoD criminal investigative agency will conduct investigations of fraud offenses under the United States Code and the Uniform Code of Military Justice. Reference (h) implements these policies, procedures and responsibility for the Department of the Navy. To that end, all instances of suspected fraudulent activity within the Navy or the Marine Corps will be immediately referred to NCIS, whether committed by a military member, a civilian, or a business enterprise. The general term "fraud" includes theft or embezzlement from the government, bribery, receipt or giving of gratuities, conflict of interest, violation of anti-trust laws, as well as false statement and false claims in the following areas: pay and allowances, procurement, property disposal, subsistence, unauthorized services, non-appropriated funds, foreign military sales and personnel matters. Except as noted below, NCIS maintains primary jurisdiction in the investigation of these offenses as they relate to the Department of the Navy, even though NCIS may work jointly with other Department of Justice, DoD, federal or local law enforcement agencies during the term of the investigation. However, notwithstanding reference (h), the Director, NCIS, will execute a Memorandum of Agreement with the DoD Inspector General (IG) establishing the following process for investigating all procurement fraud cases: (1) All new procurement fraud allegations made after the effective date of this instruction will be immediately referred to the DoD IG, who will act as focal controlling point for all such cases; (2) The DoD IG will assign procurement fraud investigations to the military departments, to the Defense Criminal Investigative Service (DCIS), or jointly, based on such factors as size and type of contract, available investigative expertise, vital interest of a particular military department especially in priority situations affecting operating forces; and, (3) the DoD IG will establish a joint service committee comprised of the directors of the appropriate

SECNAVINST 5520.3B

4 JAN 1993

investigative agencies to coordinate procurement fraud investigations, exchange lessons learned, and monitor the process established under the Memorandum of Agreement and to make recommendations for improvements to the DoD IG and the Service Secretaries. If the DoD IG or the DCIS decline a case, the Director, NCIS, with the approval of the Secretary/Under Secretary of the Navy, will assume primary jurisdictional responsibility. Ultimately, NCIS will refer all viable fraud cases, which it investigates, to the appropriate command or U.S. Attorney's office for criminal prosecution, civil litigation or administrative remedies.

f. Security and Counterintelligence Matters

(1) Within the Department of the Navy, NCIS has exclusive investigative jurisdiction in non-combat matters involving actual, potential, or suspected terrorism, sabotage, espionage, and subversive activities. This jurisdiction includes actual, suspected, or attempted defection by Department of the Navy personnel. Prompt command referral of matters in these categories to NCIS is mandatory.

(2) In accordance with reference (i), coordination between commands and NCIS in security matters will be as follows:

(a) When classified information has been, or is suspected of being lost, compromised, or subjected to compromise, NCIS will be notified immediately. The command will conduct a preliminary inquiry, unless otherwise directed by NCIS. NCIS will promptly notify the commander whether investigative action will be taken. Regardless of whether NCIS has declined investigative action, the command may request investigative assistance for the command's investigation. An NCIS investigation does not exempt the command from the responsibility to conduct an investigation in accordance with reference (e), if required in accordance with reference (i).

(b) NCIS will be notified immediately of any requests through other than official channels, for classified national defense information from anyone or for unclassified information from an individual believed to be in contact with a foreign intelligence service. NCIS will then advise what action is to be taken.

(c) When a member with access to classified information commits suicide or attempts to commit suicide, the command will forward available information to NCIS for action. If NCIS assumes investigative jurisdiction, the command investigation will be subordinate.

SECNAVINST 5520.3B

4 JAN 1993

(d) When a member who had access to classified information is an unauthorized absentee, the command will investigate to determine whether there are indications that the absence may be inimical to national security interests. If there are such indications, NCIS will be notified immediately.

(3) Reference (c) delegates to NCIS the primary responsibility for collecting, processing, storing and disseminating counterintelligence information regarding persons or organizations not affiliated with DoD. Therefore, all information regarding these activities obtained by the command will be forwarded to NCIS, less those activities conducted by the Marine Corps counterintelligence in combat and combat contingencies.

(4) Reference (d) designates NCIS as the primary element within the Department of the Navy for the conduct of non-combat related counterintelligence and related activities. These important operations are undertaken at NCIS initiative and will be done exclusively by NCIS within the Department of the Navy. Utilization of Navy and Marine Corps personnel (military or civilian) and property, including classified information and material, is often critical to the success of counterespionage operations designed to thwart the threat posed by certain foreign entities. In that regard, the fullest cooperation of all commanding officers is necessary and directed.

(5) Commands which support, develop or execute sensitive Navy/Marine Corps programs of inherent value to hostile intelligence will, with NCIS assistance, establish passive programs to enhance operational and information security.

g. Special Activities. In addition to the above-noted categories, NCIS facilities may be utilized by the Department of the Navy where unusual circumstances or aspects of sensitivity pertain (such as the protection of senior officials, dignitaries or other persons) and which may require unusual techniques and/or exercising a high degree of discretion or employing extensive investigative resources.

h. Liaison. In the field, NCIS shall be the element exclusively assigned to maintain liaison on all criminal investigative, and counterintelligence and security matters with federal law enforcement, security and intelligence agencies; and shall be the primary agency for liaison in these matters with state, local and foreign law enforcement, security and intelligence agencies, including those of foreign and U.S. military departments. This does not limit contact between appropriate Navy or Marine Corps judge advocates and federal and state agency officials to determine prosecutorial jurisdiction,

SECNAVINST 5520.3B

4 JAN 1993

forward grants of immunity, coordinate pretrial agreements, or take any other prosecution-directed action consistent with reference (f). This does not restrict Department of the Navy commands from conducting normal liaison with federal, state, local or foreign law enforcement officials in routine law enforcement matters such as traffic, physical security, minor crimes and training. Following notification of the local NCIS office, Marine Corps counterintelligence may conduct liaison necessary to accomplish its mission during combat contingencies. If prior notification of NCIS is not possible, notification will be made at the earliest opportunity.

i. **Initiation and Reporting.** To promote effective law enforcement and per reference (b), the following policy is established:

(1) Requests for NCIS support may be initiated by any commander, commanding officer or other appropriate command authority in the Navy or Marine Corps.

(2) Per reference (b), NCIS is authorized, exclusive of command request, to undertake investigative activities within the purview of this instruction and need not solicit authorization or requests to conduct any investigation; however, NCIS shall normally assure that the Immediate Senior In Command (ISIC) of the person or organization being investigated is promptly apprised of the initiation of the investigation.

(3) Should the responsible ISIC not concur with the initiation of an investigation because of operational or other considerations, such officer will report the circumstances immediately to the Secretary of the Navy (SECNAV) via the chain of command and the Chief of Naval Operations (CNO) or the Commandant of the Marine Corps (CMC), as appropriate. SECNAV will make a determination upon receiving the recommendations of the Director, NCIS and the CNO or CMC and will provide the DoD IG with the details of the case and the resolution of the matter. No investigation may be delayed or suspended in these circumstances except by expressed direction of SECNAV.

(4) Only the DoD IG may request the Director, NCIS to delay, suspend or terminate an investigation being conducted at the request of the DoD IG. All requests to delay, suspend, or discontinue such investigations will be promptly referred to SECNAV.

(5) Under normal circumstances, commanders and commanding officers shall not impede the use of investigative techniques permissible under law or regulation which NCIS considers necessary.

SECNAVINST 5520.3B

4 JAN 1993

Examples include undercover criminal operations, to include drug operations and investigations. Commands are encouraged to support recruitment and utilization of naval personnel as cooperating witnesses and confidential sources of information. Command approval for NCIS utilization of Department of the Navy civilian employees is not necessary; however, due to the unique nature of the military chain of command, prior to NCIS tasking any military member, initial concurrence of the commander or commanding officer to utilize the member will be obtained.

(6) Commanders and commanding officers are responsible for ensuring NCIS investigations are not compromised by command personnel. Providing information about ongoing NCIS investigations to persons below the executive officer level should be held to an absolute minimum and is discouraged except under unusual circumstances.

(7) To permit Department of the Navy reporting to the DoD IG, commanders and commanding officers must ensure that any member under their command who is investigated by NCIS, and who is thereby the subject of a court-martial or nonjudicial punishment proceeding, submit to fingerprinting by NCIS. Commands must also forward to NCIS a copy of the court-martial or nonjudicial punishment disposition within 30 days of disposition. Dispositions which are exculpatory in nature (e.g. dismissal of charges or acquittal) must also be forwarded. For purposes of this Instruction, disposition does not include appellate action. For court-martial, disposition means either dismissal of preferred charges by convening authority or, if charges are referred, court-martial findings and sentence, if any. For nonjudicial punishment cases, disposition means the commander's (or commanding officer's) decision to dismiss charges or the imposition of punishment and the specifics thereof.

(8) NCIS is authorized to support, on a reciprocal basis, other federal, state, local or foreign law enforcement, security or intelligence agencies in lawful actions. Such support shall include, but not be limited to, providing information/intelligence and reports of investigations concerning military and civilian personnel who are suspected of committing criminal offenses in the respective jurisdictions of other agencies.

(9) NCIS shall ensure that each command or other prosecutorial authority is provided a full report of offenses occurring within the jurisdiction of that entity. In addition, it is the responsibility of NCIS to:

(a) Assure the maintenance of a central repository for appropriate reports of investigation and pertinent counterintelligence data.

SECNAVINST 5520.3B

4 JAN 1993

(b) Provide statistical reporting required by higher authority on investigative and other matters within its mission responsibility.

(c) Report any aspect of investigative, security or counterintelligence activity indicating actual or potential trend, a threat to operational integrity, or an occurrence which otherwise warrants the attention of fleet and force Commanders in Chief, DoD/Department of the Navy, Commanding Generals, Fleet Marine Force Atlantic and Fleet Marine Force Pacific, and senior officials at the seat of government. This in no way abrogates the responsibility of commands to notify appropriate echelons of significant incidents, investigative action initiated, results thereof, and command actions taken or contemplated. This responsibility cannot be deferred to NCIS.

j. **Investigative Files.** The retention and disposal of all NCIS original investigative files is a matter within the exclusive authority of the Director, NCIS. Accordingly, no Department of the Navy representative may modify or destroy or agree to the modification or destruction of any original investigative file without the prior written approval of SECNAV, UNSECNAV or the Director, NCIS.

k. **Law Enforcement Communications.** NCIS will exercise policy control over Department of the Navy access to and use of the National Law Enforcement Telecommunications System (NLETS), the National Crime Information Center (NCIC) and similar national law enforcement telecommunications systems.

l. **Credentials and Badges.** Individuals accredited by the Director, NCIS, to carry out investigations and other mission related responsibilities are issued standardized credentials and badges designating them as "Special Agents." Certain categories of personnel are also issued credentials identifying them as "NCIS Representatives." No other persons in the Navy and the Marine Corps engaged in investigative, security or counterintelligence matters are authorized to use either title. Personnel issued NCIS Special Agent credentials are cleared for access up to and including Top Secret by the Director, NCIS. They shall be presumed to have a need to know with regard to access to information, material, or spaces relevant to the performance of their official duties. This includes all personnel and medical records, as well as all records relating to procurement or contract matters under the control of the Navy or the Marine Corps. Authority for access to special intelligence and compartmented or similarly controlled spaces, material or information shall be requested by NCIS of the authority controlling access prior to the Special Agent pursuing a matter of official concern. NCIS Special Agent credentials are to be

SECNAVINST 5520.3B

4 JAN 1993

accorded full recognition when presented for purposes of boarding or departing vessels or other naval facilities. NCIS Special Agents, as well as vehicles used by them in the course of official business and all occupants therein, shall be exempt from routine search; persons under escort by NCIS Special Agents will not be required to identify themselves or be impeded in any way.

m. **Weapons.** NCIS Special Agents are required and authorized to carry firearms on and off installations, aircraft and ships with the exception of specific "exclusion areas" where special weapons/systems are stored, as defined in reference (j). The need for a Special Agent to carry a firearm in such areas will be left to the discretion of the commander or commanding officer having responsibility for the "exclusion area."

n. **Investigative and Counterintelligence Policy.** The Director of Naval Intelligence (DNI) in consultation with the Marine Corps Director of Intelligence has overall responsibility for counterintelligence policy. NCIS is the activity responsible, with DNI oversight, for developing counterintelligence policy. NCIS is responsible for formulating investigative policy, as set forth in this instruction, to include policy regarding polygraph examinations, audio surveillance and other investigative or countermeasure aids.

o. **Oaths.** Those persons accredited by the Director, NCIS as Special Agents, agents, and operational representatives are authorized to administer oaths and take sworn statements. This authority applies only to official investigative duties in connection with the investigative jurisdiction and responsibilities of NCIS, as set forth in this instruction. This authority is derived from 5 U.S.C. 303(d). The authority vested in an individual ends when reassignment to duties other than those performed by NCIS or upon withdrawal of authorized credentials.

7. **Limitations.** Except as specifically discussed, nothing here is to be construed as infringing upon, conflicting with, or restricting in any way the legitimate fact-finding functions of the Naval Inspector General, Deputy Naval Inspector general for Marine Corps matters, other inspectors general, courts of inquiry or investigations conducted under the Uniform Code of Military Justice or the Manual of the Judge Advocate General. Examinations and other actions concerning the effectiveness of command procedure for good order and discipline or the effectiveness with which command personnel have carried out their duties are not appropriate for NCIS inquiry and should not be so referred.

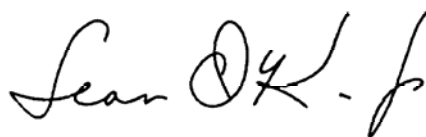
SECNAVINST 5520.3B

4 JAN 1993

8. Effect of Other Regulations, Directives, Instructions, Notices. All SECNAV, Navy and Marine Corps regulations, directives, instructions and notices pertaining to the assignment of duties to the former Naval Investigative Service Command (NISCOM), (now NCIS), or delegating various authorities to NISCOM, remain in effect. All such responsibilities and delegations are transferred to the Director, NCIS as the successor to the Commander, NISCOM.

9. Action. The Under Secretary of the Navy, the Chief of Naval Operations and the Commandant of the Marine Corps shall take appropriate action to ensure the timely updating of all regulations, directives, instructions and notices to comply with this instruction. All addressees shall take such action as is expressed or implicit to ensure compliance with this instruction.

10. Report. The reporting requirements contained in this instruction are exempt from reports control by SECNAV 5214.2B.



Sean O'Keefe

Distribution:

SNDL Parts 1 and 2
MARCORPS Codes PCN 71000000000
and 71000000100

SECNAV/OPNAV Directives Control Office
901 M Street, S.E., Bldg 200
Washington, DC 20374-5074 (20 copies)

Director
Naval Criminal Investigative Service
Washington Navy Yard, Building 111
Washington, DC 20388-5000 (1500 copies)

Stocked:
Naval Aviation Supply Office
Physical Distribution Division, Code 103
5801 Tabor Avenue
Philadelphia, PA 19120-5099 (500 copies)



DEPARTMENT OF THE NAVY

OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

SECNAVINST 5820.7C
N3/N5
26 January 2006

SECNAV INSTRUCTION 5820.7C

From: Secretary of the Navy

Subj: COOPERATION WITH CIVILIAN LAW ENFORCEMENT OFFICIALS

Ref: (a) DoD Directive 5525.5 of 15 Jan 86
(b) DoD Directive 3025.12 of 4 Feb 94
(c) Title 10, U.S. Code, Sections 371-382
(d) SECNAVINST 5211.5D
(e) DoD 4515.13-R, Air Transportation Eligibility, of Nov 94
(f) SECNAVINST 5430.107
(g) SECNAVINST 3820.3E
(h) Title 18, U.S. Code, Section 1385
(i) CJCSI 3121.01B

1. Purpose. This instruction implements reference (a) and Department of the Navy (DON) policy, responsibilities, and procedures for the transfer of relevant information, and the provision of equipment, facilities and personnel to Federal, State, and local civilian law enforcement officials. This instruction has been administratively revised and should be reviewed in its entirety.

2. Cancellation. SECNAVINST 5820.7B.

3. Scope. This instruction applies to all DON commands and activities. This instruction does not apply to cooperation with foreign officials (which follows the guidance of applicable international agreements and the administrative and operational chain of command). Use of DON personnel in civil disturbances and related matters is addressed by reference (b). Assistance to the government of the District of Columbia is addressed by separate Department of Defense (DoD) guidance.

4. Policy. It is DON policy to cooperate with civilian law enforcement officials (employees with the responsibility for enforcement of the laws within the jurisdiction of U.S. Federal, State, or local governmental agency) to the extent practical. The implementation of this policy shall be consistent with the needs of national security and military preparedness, the historic tradition of limiting direct military involvement in

SECNAVINST 5820.7C
26 January 2006

civilian law enforcement activities, and applicable law. Assistance provided under this instruction shall be at the lowest cost practicable. Assistance may not be provided under this instruction if such assistance could adversely affect national security or military preparedness.

5. Procedures for Prompt Transfer of Relevant Information

a. In accordance with reference (c), DON commands and activities are encouraged to provide Federal, State, or local civilian law enforcement officials any information collected during the normal course of military operations that may be relevant to a violation of any Federal or State law within the jurisdiction of such officials. In the event that a system of records maintained by DON to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature arising by general statute (or by rule, regulation, or order issued pursuant to the statute), the relevant records in the system of records may be referred, as a routine use under reference (d), to the appropriate agency, whether Federal, State, or local, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute (or rule, regulation, or order issued pursuant to it). An exception may be made when information is acquired and disseminated to a civilian agency through separate channels established and approved by the Chief of Naval Operations, the Commandant of the Marine Corps, Director, Naval Criminal Investigative Service, or higher authority.

b. The planning, scheduling, and execution of compatible military training or operations may take into account the needs of civilian law enforcement officials when the collection of information is an incidental aspect of training performed for a military purpose. This does not permit the planning, scheduling or execution of military training or operations for the primary purpose of aiding civilian law enforcement officials, or the purpose of routinely collecting information about U.S. citizens. Local law enforcement agents may accompany routinely scheduled training flights as observers for the purpose of collecting law enforcement information. This provision does not authorize the use of DoD aircraft to provide point-to-point transportation and training flights for civilian law enforcement officials (which may be provided only in accordance with reference (e)).

c. The transfer of such information shall be in accordance with reference (f) (providing Naval Criminal Investigative

SECNAVINST 5820.7C

26 January 2006

Service exclusive authority for some matters, and primary authority for other matters). Naval commands are authorized to established local contact points with civilian agencies in routine law enforcement matters; commands shall coordinate with the local Naval Criminal Investigative Service Office for other matters.

d. Nothing in this section modifies DON policies or procedures concerning collection or dissemination of information for intelligence purposes under reference (g).

6. Procedures for Request for Equipment, Facilities, Personnel

a. All requests from civilian law enforcement officials for the use of DON equipment, facilities, or personnel under this instruction will be submitted by the requested command via the chain of command to the designated approval authority (unless approval by higher authority is required by statute or DoD guidance). On Marine Corps installations with Provost Marshals, requests shall be coordinated with the Provost Marshal. Requests requiring DoD approval must be forwarded with a recommendation and justification to approve or deny the request. Requests may be communicated by telephone when time and circumstances require immediate action. When forwarding a request, the command will provide all available relevant information concerning:

(1) The ability to provide the assistance requested without adversely affecting national security or military preparedness, and

(2) The incremental costs DON would incur in providing the requested assistance.

b. Approval Authority for Use of Equipment and Facilities:

(1) Requests for the loan or use of equipment or facilities for more than 60 days (including a permanent disposition) or for arms, ammunition, combat vehicles, vessels, and aircraft must be approved by the Assistant Secretary of the Navy (Manpower and Reserve Affairs) (ASN (M&RA)).

(2) All other requests may be approved by any of the following commands (or superiors to these commands): Naval Component and Fleet Commanders; Commanders and Commanding Officers of major Navy shore commands; Commanding Generals of Marine Corps operating forces; Commanders of Marine Corps bases, camps, aviation installations, logistics installations, and unit

SECNAVINST 5820.7C

26 January 2006

training centers; Commanding Generals of Marine Corps Reserve support activities.

c. Approval Authority for Use of Personnel:

(1) The Secretary of Defense, via the Joint Staff (and Assistant Secretary of Defense (Reserve Affairs) for requests involving reserve personnel), is the approval authority for personnel requests that involve assignment of 50 or more DON personnel, or a period of assignment of more than 30 days, or DON intelligence components.

(2) The ASN (M&RA) may approve requests for the following use of DON personnel, except as provided above, in accordance with reference (a):

(a) To provide training or expert advice;

(b) For equipment maintenance;

(c) To monitor and communicate the movement of air and sea traffic;

(3) The Under Secretary of Defense for Personnel and Readiness, via the Joint Staff (and ASD(RA)) for requests involving reserve personnel) is the approval authority for other requests that involve the assignment of personnel.

d. Delegated Denial Authority: Requests for assistance from civilian law enforcement officials that may be approved at the Secretary of the Navy level or below may be denied by the appropriate Echelon 2 command if appropriate under this instruction.

7. Permissible Forms of Equipment and Facilities Assistance

a. DON activities may make equipment and facilities (base and research) available to Federal, State, or local civilian law enforcement officials for law enforcement purposes when approved as above.

b. Approval authorities shall ensure that assistance provided under this paragraph follows applicable provisions of Title 10, U.S. Code, Sections 372, 2576, 2667, Title 31, U.S. Code, Sections 1535-1536, and other applicable laws and directives (see reference (a)).

8. Permissible and Impermissible Forms of Personnel Assistance

SECNAVINST 5820.7C

26 January 2006

a. DoD policy (reference (a), making the Posse Comitatus Act applicable to the DON) reflects the historic tradition of limiting direct military involvement in civilian law enforcement activities. The Posse Comitatus Act (reference (h)) states:

"Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both."

Pursuant to reference (a), commands must adhere to this paragraph in deciding on the provision of military personnel to civilian law enforcements requests.

b. Restrictions on Direct Assistance: Except as otherwise provided in this instruction, reference (a) prohibits the following forms of direct assistance by military personnel:

(1) Interdiction of a vehicle, vessel, aircraft, or other similar activity.

(2) A search or seizure.

(3) An arrest, apprehension, stop and frisk, or similar activity.

(4) Use of military personnel for surveillance or pursuit of individuals, or as undercover agents, informants, investigators, or interrogators.

(5) With regard to such actions described above that are conducted outside the territorial jurisdiction of the United States, the Secretary of Defense or the Deputy Secretary of Defense will consider for approval, on a case-by-case basis, requests for exceptions to the policy restrictions against direct assistance by military personnel to execute the laws. Such requests for exceptions to policy outside the territorial jurisdiction of the United States should be made only when there are compelling and extraordinary circumstances to justify them.

(6) Further, the Secretary of the Navy may provide exceptions to the limitations contained in this instruction on a case-by-case basis:

SECNAVINST 5820.7C
26 January 2006

(a) Such exceptions shall include requests from the Attorney General for assistance under Title 21, U.S. Code, Section 873(b).

(b) Prior approval from the Secretary of Defense shall be obtained for exceptions that are likely to involve participation by members of the Navy or Marine Corps in an interdiction of a vessel or aircraft, a law enforcement search or seizure, an arrest, apprehension, or other activity that is likely to subject civilians to use of military power that is regulatory, proscriptive, or compulsory. Such approval may be granted only when the head of the civilian agency concerned verifies that:

1. The size or scope of the suspected criminal activity poses a serious threat to the interests of the United States and enforcement of a law within the jurisdiction of the civilian agency would be impaired seriously if the assistance were not provided because civilian assets are not available to perform the missions; or

2. Civilian law enforcement assets are not available to perform the mission and temporary assistance is required on an emergency basis to prevent loss of life or wanton destruction of property.

c. Permissible Direct Assistance. The following activities are permissible:

(1) Primary Purpose Military or Foreign Affairs: Actions that are taken for the primary purpose of furthering a military or foreign affairs function of the United States, regardless of incidental benefits to civilian authorities. This provision must be used with caution, and does not include actions taken for the primary purpose of aiding civilian law enforcement officials or otherwise serving as a subterfuge to avoid the restrictions of the instruction. Actions under this provision may include the following, depending on the nature of the DoD interest and the authority governing the specific action in question:

(a) Investigations and other actions related to enforcement of the Uniform Code of Military Justice (UCMJ).

(b) Investigations and other actions that are likely to result in administrative proceedings by the Department of Defense, regardless of whether there is a related civil or criminal proceeding.

SECNAVINST 5820.7C

26 January 2006

(c) Investigations and other actions related to the commander's inherent authority to maintain law and order on a military installation or facility.

(d) Protection of classified military information or equipment.

(e) Protection of DoD personnel, equipment and official guests.

(f) Such other actions that are undertaken primarily for a military or foreign affairs purpose.

(2) Department of Defense Inspector General (DoD IG): Audits and investigations conducted by, under the direction of, or at the request of the DoD Inspector General. This includes drug investigations conducted by Naval Criminal Investigative Service under DoD IG Criminal Investigations Policy Memorandum Number Five on Criminal Drug Investigative Activities of 1 October 1987.

(3) Preserve Public Order: Actions that are taken under the inherent right of the U.S. Government under the Constitution to ensure the preservation of public order and to carry out governmental operations within its territorial limits, or otherwise in accordance with applicable law, by force, if necessary. This authority is reserved for unusual circumstances, and will be used only under reference (b), which permits use of this power in two circumstances:

(a) The emergency authority authorizes prompt and vigorous Federal action, including use of military forces, to prevent loss of life or wanton destruction of property and to restore governmental functioning and public order when sudden and unexpected civil disturbances, disasters, or calamities seriously endanger life and property and disrupt normal governmental functions to such an extent that duly constituted local authorities are unable to control the situation.

(b) The emergency authority authorizes Federal action, including the use of military forces, to protect Federal property and Federal Government functions when the need for protection exists and duly constituted local authorities are unable or decline to provide adequate protection.

(4) Insurgency: Actions taken pursuant to DoD responsibilities under Title 10, U.S. Code, Sections 331-334 and

SECNAVINST 5820.7C
26 January 2006

reference (b), relating to the use of the military forces with respect to insurgency or domestic violence or conspiracy that hinders the execution of State or Federal law in specified circumstances.

(5) Assistance to Executive Officials. Actions taken under express statutory authority to assist officials in executing the laws, subject to applicable limitations. The laws that permit direct military participation in civilian law enforcement, include, but are not limited to, the following:

(a) Protection of national parks and certain other Federal lands. Title 16, U.S. Code, Sections 23, 78 and 593.

(b) Enforcement of the Fishery Conservation and Management Act of 1976. Title 16, U.S. Code, Section 1861(a).

(c) Assistance in the case of crimes against foreign officials, official guests of the United States, and other internationally protected persons. Title 18, U.S. Code, Sections 112 and 1116.

(d) Assistance in the case of crimes against members of Congress. Title 18, U.S. Code, Section 351.

(e) Assistance in the case of crimes involving nuclear materials. Title 18, U.S. Code, Section 831.

(f) Protection of the President, Vice President, and other designated dignitaries. Title 18, U.S. Code, Section 1751 and the Presidential Protection Assistance Act of 1976.

(g) Actions taken in support of the neutrality laws. Title 22, U.S. Code, Sections 408 and 461-462.

(h) Removal of persons unlawfully present on Indian lands. Title 25, U.S. Code, Section 180.

(i) Execution of quarantine and certain health laws. 42 U.S.C. § 97.

(j) Execution of certain warrants relating to enforcement of specified civil rights laws. 42 U.S.C. § 1989.

(k) Removal of unlawful inclosures from public lands. 43 U.S.C. § 1065.

SECNAVINST 5820.7C
26 January 2006

(l) Protection of the rights of a discoverer of a guano island. Title 48, U.S. Code, Section 1418.

(m) Support of territorial governors if a civil disorder occurs. Title 48, U.S. Code, Sections 1422 and 1591.

(n) Actions in support of certain customs laws. Title 50, U.S. Code, Section 220.

(6) Expert Advice. DON activities may provide expert advice to Federal, State, or local law enforcement officials in accordance with Title 10, U.S. Code, Section 373. This does not permit regular or direct involvement of military personnel in activities that are fundamentally civilian law enforcement operations, except as otherwise authorized in this instruction.

(7) Training. DON activities may provide training to Federal, State, and local civilian law enforcement officials in the operation and maintenance of equipment made available under this instruction. This does not permit large scale or elaborate training, and does not permit regular or direct involvement of military personnel in activities that are fundamentally civilian law enforcement operations, except as otherwise authorized by this instruction. Any such training shall be provided under the following guidance:

(a) It shall be limited to situations when the use of non-DoD personnel would be unfeasible or impractical from a cost or time perspective and would not otherwise compromise national security or military preparedness.

(b) It shall not involve DON personnel in a direct role in law enforcement operations, except as otherwise authorized by law.

(c) The performance of such assistance by DON personnel shall be at a location where there is not a reasonable likelihood of a law enforcement confrontation, except as otherwise authorized by law.

(8) Use of DON Personnel to Operate or Maintain Equipment. The use of DON personnel to operate or maintain or to assist in operating or maintaining equipment shall be limited to situations when the training of non-DoD personnel would be unfeasible or impractical from a cost or time perspective and would not otherwise compromise national security or military preparedness concerns. In general, the head of the civilian law enforcement agency may request DON activities to provide

SECNAVINST 5620.7C
26 January 2006

personnel to operate or maintain or assist in operating or maintaining equipment for the civilian agency. This assistance shall be subject to the following guidance:

(a) It shall not involve DON personnel in a direct role in law enforcement operations, except as provided by this instruction or as otherwise authorized by law.

(b) It shall be at a location where there is not a reasonable likelihood of a law enforcement confrontation, except as otherwise authorized by law.

(c) The use of military aircraft to provide point-to-point transportation and training flights for civilian law enforcement officials may be provided only under reference (c).

(d) Additional provisions concerning drug, customs, immigration, and certain other laws: A request under this provision for DON personnel to operate or maintain or to assist in operating or maintaining equipment made available under this instruction may be made by the head of a civilian agency empowered to enforce the following laws:

1. The Controlled Substances Act (Title 21, U.S. Code, Sections 801 et seq.) or the Controlled Substances Import and Export Act (Title 21, U.S. Code, Sections 951 et seq.);

2. Immigration and Nationality Act (Title 8, U.S. Code, Sections 1324-1328);

3. Law relating to the arrival or departure of merchandise, as defined in the Tariff Act of 1930 (Title 19, U.S. Code, Section 1401), into or out of the customs territory of the United States, as defined in the Tariff Schedules of the United States (Title 19, U.S. Code, Section 1202), or any other territory or possession of the United States;

4. Any other law that establishes authority for DON personnel to provide direct assistance to civilian law enforcement officials.

(e) DON personnel may be assigned to operate or assist in operating equipment to the extent the equipment is used for monitoring and communicating to civilian law enforcement officials the movement of air and sea traffic with respect to any criminal violations specified in paragraph 8(c)(5) of this instruction. This includes communicating

SECNAVINST 5820.7C
26 January 2006

information concerning the relative position of civilian law enforcement officials and other air and sea traffic.

(f) In an emergency circumstance, equipment operated by or with the assistance of DON personnel may be used outside the land area of the United States (or any commonwealth, territory, or possession of the United States) as a base of operations by Federal law enforcement officials to facilitate the enforcement of such laws, and to transport such officials in connection with such operations, subject to the following limitations:

1. Equipment operated by or with the assistance of DON personnel may not be used to interdict or interrupt the passage of vessels or aircraft, except when DON personnel are otherwise authorized to take such action with respect to a civilian law enforcement operation.

2. There must be a joint determination by the Secretary of Defense and the Attorney General that an emergency circumstance exists under Title 10, U.S. Code, Section 374(c) (2). An emergency circumstance may be determined to exist under this subparagraph only when the size and scope of the suspected criminal activity poses a serious threat to the interests of the United States, and enforcement of laws in paragraph 8(c)(5) of this instruction would be impaired seriously if the assistance described in this subparagraph were not provided.

3. The emergency authority in this subparagraph applies only to large-scale criminal activity at a particular point in time or over a fixed period. It does not permit use of this authority on a routine or extended basis.

(9) Nothing in these subparagraphs restricts the authority of military personnel to take immediate action to save lives or property or to protect a Federal function as provided in this paragraph.

(10) When DON personnel are otherwise assigned to provide assistance, the participation of such personnel shall be consistent with the limitations in such laws, if any, and such restrictions as may be established by the chain of command.

d. Other Permissible Indirect Assistance:

(1) Transfer of information acquired in the normal course of military operations. See paragraph 5 above.

SECNAVINST 5820.7C

26 January 2006

(2) Such other actions approved by the Secretary of the Navy that do not subject civilians to use of military power that is regulatory, proscriptive, or compulsory.

e. Exceptions based on status. The restrictions in this paragraph do not apply to the following persons:

(1) A member of a Reserve Component when not on active duty, active duty for training, or inactive duty for training.

(2) A member of the National Guard when not in the Federal Service.

(3) A civilian employee of the Department of Defense. If the civilian employee is under the direct command and control of a military officer, assistance will not be provided unless otherwise permissible under paragraph 8.

(4) A member of a DON when off duty and in a private capacity. A member is not acting in a private capacity when assistance to law enforcement officials is rendered under the direction or control of DoD authorities.

9. Reimbursement and Accounting Procedures

a. As a general rule, reimbursement is required when equipment or services are provided to agencies outside DoD. When DON resources are used in support of civilian law enforcement efforts, the costs to DON shall be limited to the incremental or marginal costs.

b. As a part of the normal administrative control procedures, a copy of the civilian law enforcement agency request or a statement of the requested support and the official approval should be retained for two years by the command providing the assistance. The date(s) and location(s) of the support and the DON resources employed shall be included in the documentation.

c. The system used to account for the cost of support to civilian law enforcement agencies need be no different from that deemed adequate and sufficient for normal administration and control of resources. If the accounting system used by a command has the capability to accumulate and distribute the indirect costs incurred in providing the support, including the indirect costs for the overall management of the command, that system shall be used. Where such a system is not in use, but

SECNAVINST 5040.7C
26 January 2006

the existing accounting system can be easily modified to provide for a systematic and rational indirect costing process which would also be beneficial to the day-to-day operations of the command, such modification shall be effected. Where such a system is not in use and the command has no other recurring or substantial need for an accounting system which separately identifies direct and indirect costs, the command will use a memorandum costing or cost-finding system established by the Assistant Secretary of the Navy (Financial Management and Comptroller).

d. Requests for waivers of reimbursement shall be forwarded to the Chief of Naval Operations (N3/N5) or the Commandant of the Marine Corps (Code PS), as appropriate with a copy to Assistant Secretary of the Navy (Financial Management and Comptroller). Budgetary resources of the requesting civilian law enforcement agency and past practices with respect to similar types of assistance will be considered in evaluating such requests. The Under Secretary of Defense for Personnel and Readiness is the approval authority to waive reimbursement. Waivers of reimbursement will normally be appropriate in the following circumstances:

(1) When assistance under this instruction involves use of DON personnel in an activity that provides training or operational benefits that are substantially equivalent to the benefit of normal training or operations.

(2) When reimbursement is not otherwise required by law, and assistance is provided as an incidental aspect of the activity that is conducted for military purposes.

10. Responsibilities

a. The Chief of Naval Operations (N3/N5) and the Commandant of the Marine Corps (Code PS) shall:

(1) Respond to the Joint Staff in the formulation of data to evaluate the impact of requests for assistance on national security and military preparedness.

(2) Advise the ASN(M&RA) on the impact on national security and military preparedness of specific requests for assistance when the Assistant Secretary of the Navy or higher authority acts as the approving authority.

(3) Review training and operational programs to determine how assistance can be provided to civilian law

SECNAVINST 5820.7C
26 January 2006

enforcement officials, consistent with the policy in this instruction, with a view towards identification of programs that would not involve any incremental costs or that would permit waiver of reimbursement.

b. Naval Component and Fleet Commanders; Commanders and Commanding Officers of major Navy shore commands; Commanding Generals of Marine Corps operating forces; Commanders of Marine Corps bases, camps, aviation installations, logistics installations, and unit training centers; Commanding Generals of Marine Corps Reserve support activities shall:

(1) Review training and operational programs to determine how assistance can be provided to civilian law enforcement officials, consistent with the policy in this instruction, with a view towards identification of programs that would not involve any incremental costs or that would permit waiver of reimbursement.

(2) Establish operational procedures for rendering assistance to civilian law enforcement officials to include as applicable:

(a) Establishment of ocean surveillance and reporting programs.

(b) Provision of towing or escort services for vessels seized by the U. S. Coast Guard.

(c) Provision of transportation for arrested persons in custody of civilian law enforcement officials.

(d) Provision of logistic support for law enforcement operational units.

(e) Embarkation of civilian law enforcement officials on selected Navy vessels and aircraft for law enforcement purposes.

(f) Use of force in civilian law enforcement activities in accordance with reference (i).

(3) Establish contact points in subordinate commands for purposes of coordination with civilian law enforcement officials.

c. Naval Criminal Investigative Service field offices shall normally serve as the primary point of contact between Navy and Marine Corps commands and Federal, State and local civilian law enforcement officials in connection with investigative requests for assistance under this instruction.

11. Release of Information. Information provided for public affairs purposes that concerns law enforcement operations is the primary responsibility of the civilian agency that is performing the law enforcement function. DON activities may provide information on DON support when approved by the Chief of Information.



Dionel M. Aviles
Under Secretary of the Navy

Distribution:

Electronic only, via Navy Directives Website
<http://neds.daps.dla.mil/>