An Introduction to Intelligence Oversight and Sensitive Information: The Department of Defense Rules for Protecting Americans' Information and Privacy

Kevin W. Kapitan[*]

I. Introduction: The Issue(s)

The Department of Defense (DoD) conducts intelligence activities. While not a grand revelation, what most people (including judge advocates) do not realize is that most of these activities are conducted only overseas. While some are conducted within the homeland, the focus of military intelligence is limited by presidential executive orders (EOs) and DoD policy to only two mission sets: defense-related foreign intelligence and counterintelligence.[1]

These limitations may, however, be a grand revelation to military personnel returning from combat zones, Iraq and Afghanistan in particular. Using intelligence assets to develop information on just about anything pertaining to environmental, socio-cultural, or political situations in the region is perfectly acceptable and often desirable. All information developed in the war zone may have foreign intelligence or counterintelligence value directly affecting strategic military operations, decision-making, and force protection. Such is not the case in the homeland.

In this era of impending drawdowns, furloughs, and other force-reduction measures, the use of military forces within the United States is becoming directed at homeland defense and defense support of civil authorities (DSCA) missions.[2] While functionally logical and fiscally feasible, the transition from combat operations to domestic support activities requires a significant shift in paradigm. Uses of intelligence assets that were routine in theater generally require approval from the Secretary of Defense (SecDef) or a service secretary in the homeland.[3] The objective of military support activities during, say, a natural disaster is not to identify and eliminate the enemy; it is to assist other federal agencies (usually the Federal Emergency Management Agency (FEMA)), who in turn are helping disaster victims within the United States.

Yet DoD personnel cannot provide domestic assistance in a vacuum. They must develop adequate information to protect both their own forces *and* the privacy rights of the victims being aided. The need to do so often creates tension between the government's need for information and Americans' concern for their civil and privacy rights. The challenge confronting military decision makers becomes inherent: national intelligence and force protection interests must be balanced against constitutional and privacy rights of the populace. Intelligence oversight (IO) programs come into play now more than ever. Since DoD intelligence activities are already self-limiting to foreign intelligence and counterintelligence, by providing processes and procedures designed to permit the capture of requisite military intelligence and information demands while ensuring that these persons' privacy rights are not violated, IO provides an extensive interlocking system of safeguards that has been in place for over thirty years to address these concerns.

Precious little has been written about intelligence oversight for those who do *not* practice in intelligence law or national security legal fields, by those who do. For that reason, while this article will enlighten any judge advocate or DoD legal advisor, it will be of greatest benefit to those who practice operational law, since it will be those attorneys who will most likely be advising commanders and intelligence component personnel on intelligence law and

---

[*] Legal Advisor, U.S. Army North, Fort Sam Houston, Texas. He received his J.D. from the Dedman School of Law, Southern Methodist University, Dallas, Texas, in 1988; an M.A. in Forensic Studies (Criminal Justice), from Indiana University at Bloomington, in 1977; and a B.A. from Indiana University at Bloomington, in 1976. He is admitted to the Texas Bar, and is licensed to practice before the U.S. Supreme Court, the U.S. Court of Appeals for the Armed Forces, the U.S. Air Force Court of Criminal Appeals, the U.S. Court of Appeals for the Fifth Circuit, the U.S. District Court for the Northern District of Texas, and the U.S. District Court for the Western District of Texas . He is a retired U.S. Air Force (USAF) Reserve Assistant Staff Judge Advocate. Retiring as a lieutenant colonel, he served on active and reserve duty from May 1977 until April 2004. He was called to active duty in support of Operations Noble Eagle and Enduring Freedom to Headquarters, Air Intelligence Agency (AIA, now the Air Force Intelligence Surveillance and Reconnaissance Agency), and was awarded the USAF Meritorious Service Medal, Second Oak Leaf Cluster and the Global War on Terrorism (non-combat) Medal for his efforts while serving as the first embedded judge advocate supporting the AIA Information Operations Center at Lackland AFB, Texas. Prior to serving as a military lawyer, Mr. Kapitan was assigned as a USAF Security Police officer, and also a Special Agent for the USAF Office of Special Investigations (OSI). During his non-legal military career, he held two commands: USAF OSI Detachment, Fort George G. Meade, Maryland, and the 301st Security Police Squadron, Carswell AFB, Texas.

[1] *See* Exec. Order No. 12,333, United States Intelligence Activities, 3 C.F.R. 200 (1981) [hereinafter EO 12,333], *as amended by* Exec. Order No. 13,284, 68 Fed. Reg. 4075 (Jan. 23, 2003); Exec. Order No. 13,355, 69 Fed. Reg. 53593 (Aug. 27, 2004); and Exec. Order No. 13,470, 73 Fed. Reg. 45325 (July 30, 2008) [hereinafter E.O. 13,470]; *see also* U.S. DEP'T OF DEF., DIR. 5240.01, DOD INTELLIGENCE ACTIVITIES encl. 2, para. E2.7 (27 Aug. 2007).

[2] *See* CHAIRMAN, JOINT CHIEFS OF STAFF, JOINT PUB. 3-37, HOMELAND DEFENSE (12 July 2007); U.S. DEP'T OF DEF., DIR. 3025.18, DEFENSE SUPPORT OF CIVIL AUTHORITIES (29 Dec. 2010) (C1, 21 Sept. 2012) [hereinafter DoDD 3025.18] (superseding U.S. DEP'T OF DEF., DIR. 3025.1, MILITARY SUPPORT OF CIVIL AUTHORITIES para. 1 (15 Jan. 1993) [hereinafter DoDD 3025.1]).

[3] For example, the use of unmanned aerial systems (UAS) in theater frequently accompanied many if not most large scale operations due to their value as surreptitious intelligence gathering assets. However, in the Defense Support to Civil Authorities (DSCA) domain, domestic use of UAS capabilities is highly restricted due to safety and policy considerations, and requires the direct approval of the Secretary of Defense (SecDef). *See* DoDD 3025.18, *supra* note 2, para. 4.0.

related matters. While prospects for a demonstration of knowledge of intelligence and national security law in the courtroom will be quite rare for military attorneys, the transition from combat operations to domestic support activities will afford military lawyers in the field, as well as those serving on headquarters' staffs, new opportunities to develop more than mere awareness of IO. The following article is designed to facilitate that endeavor.

In the wake of 9/11, Congress recognized the need for all federal, state, and local entities involved in homeland security to share threat-related information "to the maximum extent practicable."[4] The President later issued Executive Order 13,470, reinforcing the existing mandate of federal agencies to acquire and provide the highest levels of the Executive Branch with useful intelligence, using "[a]ll means . . . consistent with applicable United States law . . . and with full consideration of the rights of United States persons," in such a manner as "to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law," and treating state, local, and tribal governments as "critical partners" in the process.[5]

When the military is called upon to render disaster support to the civilian populace, the process is referred to as Defense Support of Civilian Authorities, or "DSCA." Formerly known as Military Support to Civilian Authorities (MSCA),[6] DSCA specifically pertains to support provided by U.S. federal military forces, DoD civilians, DoD contract personnel, DoD Component assets, and National Guard forces (when the SecDef, in coordination with the Governors of the affected States, elects and requests to use those forces in either Title 10 or Title 32, U.S.C., status) in response to requests for assistance from civil authorities for domestic support during emergencies, law enforcement assistance and indirect support, and other domestic activities, or from qualifying entities seeking assistance during special events.[7] Domestic incidents arising from terrorist threats or attacks, major disasters, and other emergencies are the focus of DSCA operations.[8] During the course of these events, the acquisition, evaluation, retention, and distribution of information and intelligence may be necessary to ensure the effective rendering of assistance, while assuring the protection of military forces engaged in consequence management and disaster assistance.

This article is designed to provide the practitioner with an overview of the history and the legal, regulatory, and policy restrictions that characterize the dusky domain of domestic military intelligence activities during consequence management and disaster support operations.

II. A Brief History of Intelligence Oversight[9]

Formalized national intelligence oversight programs began with the passage of the National Security Act of 1947.[10] The Act created the national intelligence framework of the United States, establishing the Central Intelligence Agency (CIA)[11] and the responsibilities of the DoD in the national intelligence framework.[12] Even then, Congress saw the need to provide oversight of intelligence activities, and as part of the Act required that its own intelligence committees be kept "fully and currently informed" about significant intelligence activities.[13] Despite these provisions, for decades Congress maintained a "hands-off" approach to intelligence oversight, assuming all intelligence activities conducted were legal and necessary; from 1945 to 1975, it declined to pass more than two hundred bills that were designed to enhance non-intelligence supervision and accountability of Executive Branch intelligence activities.[14]

However, with the turbulent 1960s and 1970s came new and widespread allegations of CIA and military intelligence abuses and improprieties, including alleged violations of American citizens' privacy and constitutional rights.[15] Some of these allegations found their way into federal courtrooms when plaintiffs claimed illegal surveillance of one kind or

[4] Homeland Security Information Sharing Act, 6 U.S.C. § 481(c) (2012).

[5] EO 12,333, *supra* note 1, § 1.1(a), *as amended by* EO 13,470, *supra* note 1, at 45325. The order requires agencies to provide information to the President, the National Security Council, and the Homeland Security Council, and to share information "on which to base decisions concerning the development and conduct of foreign, defense, and economic policies, and the protection of United States national interests from foreign security threats," with a special emphasis on espionage, terrorism, and weapons of mass destruction. *Id*.

[6] DoDD 3025.1, *supra* note 2, para. 1.

[7] DoDD 3025.18, *supra* note 2, at glossary; *see also* U.S. DEP'T OF HOMELAND SEC., NATIONAL RESPONSE PLAN 41 (Dec. 2004) [hereinafter DHS NATIONAL RESPONSE PLAN] (recently reissued as U.S. DEP'T OF HOMELAND SEC., NATIONAL RESPONSE FRAMEWORK (Mar. 2008)).

[8] DHS NATIONAL RESPONSE PLAN, *supra* note 7, at 41.

[9] For a more extensive history, see William C. Banks & M. E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 2–76 (2000).

[10] National Security Act of 1947, 50 U.S.C. §§ 401–442b (2011).

[11] *Id.* §§ 403–04.

[12] *Id*. § 403–05.

[13] *Id*. §§ 413, 413a, 413b(b), 413c (requiring the executive branch to keep congressional intelligence committees informed about intelligence activities, especially covert actions).

[14] 1 REPORT OF THE SENATE SELECT COMM. ON GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, S. REP. No. 765, 94th Cong., 2d Sess. 4 (1976).

[15] *See* Seymour M. Hersch, *Huge CIA Operation Reported in U.S. Against Antiwar Forces*, N.Y. TIMES, Dec. 22, 1974, at A1; *see also* Seymour Hersch, *Underground for the CIA in New York: An Ex-agent Tells of Spying on Students*, N.Y. TIMES, Dec. 29, 1974 at A1.

another.[16] In the 1972 case of *United States v. U.S. District Court* (*Keith*), Justice Powell delivered the powerful opinion of the Court addressing alleged abuses perpetrated by the CIA and other members of the intelligence community:

> History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.' Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent. . . . The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society. . . .[17]

In 1975, a congressional commission, Commission on CIA Activities Within the United States (chaired by Vice President Nelson Rockefeller), concluded that the CIA had in fact exceeded its statutory authority by conducting illegal mail searches, engaging in illegal wiretaps, conducting illegal break-ins, and so on, in the process collecting staggering amounts of information on the lawful activities of U.S. persons (USPs).[18] The following year, a Senate committee examined all U.S. agencies' activities even tangentially related to the U.S. intelligence community.[19] Chaired by Senator Frank Church, this committee found myriad abuses, including plots to overthrow or assassinate foreign leaders, the opening of private mail without warrants, the infiltration of the news media and publishing industry, and the distribution of propaganda to the American public.[20] Alarmingly, the committee found that a major perpetrator of these abuses was the DoD, either acting on its own or under the direction of the CIA.[21]

In response to these concerns, Congress in 1974 passed the Hughes-Ryan Act, amending the Foreign Assistance Act of 1961,[22] and placing limits on CIA activity in foreign countries:

> No funds appropriated under the authority of this or any other Act may be expended by or on behalf of the Central Intelligence Agency for operations in foreign countries, other than activities intended solely for obtaining necessary intelligence, unless and until the President finds that each such operation is important to the national security of the United States and reports, in a timely fashion, a description and scope of such operation to the appropriate committees of Congress . . . .[23]

---

[16] *See, e.g.*, Laird v. Tatum, 408 U.S. 1, 3 (1973) (existence of Army surveillance program that could include peaceful political activity, without more, did not grant standing to plaintiffs who alleged no specific wrong against them); Halkin v. Helms, 690 F.2d 977, 981–85, 990–92 (D.C. Cir. 1982) (antiwar activists claimed unlawful CIA surveillance; court upheld trial court's refusal to allow discovery of documents related to surveillance programs as state secrets; case includes an extensive unclassified analysis of CIA domestic operations); Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144, 153–63 (D.C. Cir. 1976) (Americans living in West Berlin and West Germany sued, alleging warrantless electronic surveillance by the U.S. Army; the court held that warrants were required under the circumstances and damages could be recovered for unlawful surveillance); 2 JAMES G. CARR & PATRICIA L. BELLIA, LAW OF ELECTRONIC SURVEILLANCE § 8.38 (2012), *available at* Westlaw, ELECTRSURV 8:38 (discussing civil remedies for illegal electronic surveillance by government).

[17] United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 314 (1972).

[18] COMM'N ON CIA ACTIVITIES WITHIN THE UNITED STATES, REPORT TO THE PRESIDENT (1975) (also known as "The Rockefeller Commission"); *see also* Exec. Order No. 11,828, Establishing a Commission on CIA Activities Within the United States, 40 Fed. Reg. 1219 (Jan. 4, 1975) (enumerating President Ford's two core objectives of the commission: to "[a]scertain and evaluate any facts relating to activities conducted within the United States by the Central Intelligence Agency which give rise to questions of compliance with the provisions of 50 U.S.C. 403"; and to "[d]etermine whether existing safeguards are adequate to prevent any activities which violate the provisions of 50 U.S.C. 403").

[19] At roughly the same time, the House of Representatives also formed its own committees to examine potential CIA and Intelligence Community abuses. The first was the Nedzi Committee, under the leadership of Lucien Nedzi (D–MI), Chairman of the Armed Services Subcommittee on Intelligence, the House Select Committee on Intelligence was short lived, created on 19 February 1975 by H.R. 138, but then dissolved on 17 July 1975, with no final report issued. Its successor, created on 17 July 1975, was a new House Select Committee on Intelligence known as the Pike Committee, chaired by Otis Pike (D–NY), and met a somewhat similar demise in that the Committee was dissolved without final publication of its report. Nonetheless, journalist Daniel Schorr acquired and provided a copy of the entire Pike Committee report to the Village Voice, which published it on 16 February 1976. *See* Gerald K. Haines, *Looking for a Rogue Elephant: The Pike Committee Investigations and the CIA*, STUD. IN INTELLIGENCE, Winter 1998-99, at 81, *available at* https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/winter98_99.

[20] S. REP. No. 94-755 (1976).

[21] *Id*. at 84–85, 289–98.

[22] Pub. L. No. 93-559, § 32, 88 Stat. 1804 (1974).

[23] *Id*.; *see* STEPHEN DYCUS, ARTHUR L. BERNEY, WILLIAM C. BANKS, & PETER RAVEN-HANSEN, NATIONAL SECURITY LAW 390 (4th ed. 2007) (providing a compilation of information on the Hughes-Ryan Amendment and its effects on CIA accountability).

As observed by one set of commentators, "[o]ne clear purpose of Hughes-Ryan was to end the practice of 'plausible deniability' for the President, at least in his relations with Congress" when dealing with intelligence matters.[24] Congress also indirectly restricted governmental collection activities by passing the Privacy Act of 1974,[25] which allowed individuals to access governmental records about themselves, and was designed to "prevent the secret gathering of information on people or the creation of secret information systems or data banks on Americans . . . ."[26]

Congress then passed the Foreign Intelligence Surveillance Act of 1978 (FISA),[27] which, as an extension and expansion of the Federal Wiretap Statute,

> generally allows a federal officer, if authorized by the President of the United States acting through the Attorney General . . . to obtain from a judge of the specially created FISA Court . . . an order "approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information."[28]

Simply, FISA was designed to regulate the domestic collection of foreign intelligence and counterintelligence information for national security purposes. Its original focus was electronic surveillance, although in 1994 it was amended to include physical searches.[29] As the First Circuit Court of Appeals observed, "[a]lthough evidence obtained under FISA subsequently may be used in criminal prosecutions, the investigation of criminal activity cannot be the primary purpose of the surveillance."[30] Ultimately, FISA reflected a compromise of sorts, balancing national security requirements with personal privacy protection.[31]

A succession of Presidents issued EOs to increase accountability for intelligence activities within the Executive. In February 1976, President Ford signed EO 11,905,[32] which defined the Intelligence Community,[33] placed restrictions on surveillance of USPs, and established the Intelligence Oversight Board to review reports from intelligence organizations' inspectors general and general counsel. In 1979, President Carter issued EO 12,036, which increased the restrictions on collecting intelligence against USPs.[34]

Then, in 1983, President Reagan issued EO 12,333. This established the core structure for intelligence oversight that (with minor modifications over the years) has prevailed ever since. As a part of Executive Branch oversight responsibilities, the EO imposed specific obligations upon the President's Intelligence Oversight Board to conduct: periodic reviews of the practices and procedures of each agency's inspector general (IG) and general counsel (GC) within the Intelligence Community in discovering and reporting intelligence activities to the Board that raised questions of legality or propriety; periodic reviews of the internal guidelines of each agency within the Intelligence Community concerning the legality or propriety of intelligence activities; quarterly reporting to the President of its findings; unscheduled yet timely reporting to the President of any intelligence activities that raised serious questions of legality or propriety; and investigations of the intelligence activities of agencies within the Intelligence Community as the Board deemed necessary to carry out its functions under the EO.[35] This expansion of "oversight" and reporting requirements laid the framework for national intelligence oversight programs which were to become the basis of the current intelligence process.

Consistent with the intelligence oversight framework that was now evolving, Congress passed the Intelligence Oversight Act of 1980,[36] which essentially mirrored the safeguards implemented in earlier EOs.[37] Still lacking, however, were congressional controls over U.S. intelligence activities. The one exception was the new section 501 of the National Security Act of 1947, which required the Executive to report certain activities to the Senate Intelligence

[24] DYCUS ET AL., *supra* note 23, at 392.

[25] 5 U.S.C. § 552a (2012).

[26] DYCUS ET AL., *supra* note 23, at 1017–18.

[27] 50 U.S.C. §§ 1801–1862 (2011).

[28] United States v. Duggan, 743 F.2d 59, 69 (2d Cir. 1984); *see also* 50 U.S.C. § 1802(b).

[29] *In re* Sealed Cases, 310 F.3d 717, 722 (FISA Ct. Rev. 2002).

[30] United States v. Johnson, 952 F.2d. 565, 572 (1st Cir. 1991) (citations omitted). *See also* ELIZABETH B. BAZAN, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: OVERVIEW AND MODIFICATIONS, at vii (2008).

[31] BAZAN, *supra* note 30, at vii.

[32] Exec. Order No. 11,905, United States Foreign Intelligence Activities, 41 Fed. Reg. 7703 (Feb. 19, 1976) [hereinafter EO 11,905].

[33] *Id*. § 2.

[34] Exec. Order No. 12,036, United States Intelligence Activities, 43 Fed. Reg. 3674 (Jan. 26, 1978), *amended by* Exec. Order No. 12,139, Foreign Intelligence Electronic Surveillance, 44 Fed. Reg. 30311 (May 25, 1979), *revoked by* EO 12,333, *supra* note 1.

[35] *Id*. § 3-1.

[36] Pub. L. No. 96-450, § 407(b)(1), 94 Stat. 1975, 1981 (1980).

[37] DYCUS ET AL., *supra* note 23, at 395–96.

Committee.[38] Otherwise, intelligence oversight was left to the dominion of the President.[39]

Executive Order 12,333 clearly identified who and what constitutes the Intelligence Community and gave it specific direction and responsibilities by agency, designed specific processes associated with the conduct of intelligence activities, and provided for their reporting to, and oversight by, Congress.[40] Its Purpose and Effect provision made clear its objective: "This Order is intended to *control and provide direction and guidance to* the Intelligence Community. Nothing contained herein or in any procedures promulgated hereunder is intended to confer any substantive or procedural right or privilege on any person or organization."[41]

The most sweeping change effected by EO 12,333 was mandating a radical change in the paradigm set: while national security interests remained paramount, the constitutional and privacy rights of USPs were directed to be considered of equal importance, and all intelligence activities were required to not only consider impacts upon these rights, but also established procedures to ensure this. In so doing, the EO established a "balancing" requirement "between the acquisition of essential information and protection of individual interests . . ."[42] It then placed the responsibility for promulgating procedures for collection, retention and dissemination of information upon the heads of agencies comprising the Intelligence Community. Further, the EO required these procedures to fully comply with the EO's general principles, by instituting a "narc" provision, requiring all members of the intelligence community to report "questionable intelligence activities," regardless of who the perpetrators were.[43]

In overview, Part 1 of the EO 12,333 established the goals, directions, duties, and responsibilities of the Intelligence Community membership. Part 2 laid out the processes and procedures for the conduct of national intelligence activities. Part 3 covered aspects of congressional oversight, National Security Council operations review responsibilities, and specific definitions, including a definition of "United States persons," which is central to intelligence oversight.

The Order details, with great specificity, the types of information about United States persons that may be collected, retained, or disseminated by members of the Intelligence Community.[44] It authorizes Intelligence Community members to cooperate with law enforcement to protect personnel and resources of the Intelligence Community and prevent clandestine intelligence activities by foreign powers and international terrorist or narcotics groups.[45] It prohibits members of the Intelligence Community from unauthorized infiltration—that is, from joining or participating in any organization in the United States on behalf of any Intelligence Community agency without disclosing their intelligence affiliations to appropriate officials of the organization, except in accordance with procedures established by the heads of their agencies and approved by the Attorney General.[46] It also forbids assassination.[47]

---

[38] *Id*. *See* Pub. L. No. 96-450, § 407(b), 94 Stat. 1975, 1981 (1980).

[39] DYCUS ET AL., *supra* note 23, at 393–94.

[40] EO 12,333, *supra* note 1 (defining the intelligence community as consisting of the following agencies and departments of the U.S. Government: Central Intelligence Agency, § 1.8; Department of State, § 1.9; Department of the Treasury, § 1.10; the Department of Defense (DoD), § 1.12, to include the Defense Intelligence Agency (DIA), the National Security Agency (NSA), military offices for the collection of specialized intelligence through reconnaissance programs, and the foreign intelligence and counterintelligence elements of the Army, the Air Force, the Navy, and the Marine Corps; the Department of Energy, § 1.13, and the Federal Bureau of Investigation, § 1.14).

[41] EO 12,333, *supra* note 1, § 3.5 (emphasis added).

[42] *Id*. § 2.2. The order also recognized that in the conduct of intelligence activities, "[c]ollection of . . . information is a priority objective and will be pursued in a vigorous, innovative and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded." *Id*. § 2.1.

[43] *Id.* § 2.3. A ("United States person" was defined by Executive Order (EO) 12,333 as "a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments." *Id*. §3.4(i).

[44] *Id.* § 2.3(a)–(j). The types of information that can be collected are publicly available information; information obtained by consent of the individual; information pertaining to foreign intelligence and counterintelligence; information obtained during the course of investigations into foreign intelligence, counterintelligence, international narcotics, or international terrorist activities; information necessary for the protection of persons who are targets, victims or hostages of international terrorist organizations; information needed to protect foreign intelligence and counterintelligence collection sources and methods; information concerning persons reasonably believed to be potential sources or contacts to determine their suitability and credibility; information arising out of lawful personnel, physical or communications security investigations; information acquired through the use of overhead reconnaissance when it is not specifically directed at United States persons; information that is incidentally obtained that may indicate violations of U.S. or foreign laws; and information necessary to accomplish administrative purposes. Intelligence community members may disseminate this information (except when derived through signals intelligence processes) to each other so that they may determine if the information is relevant to their respective responsibilities and should therefore be retained.

[45] *Id*. § 2.6. *Compare*, U.S. DEP'T OF DEF., REG. 5240.1-R, procedure 12 (Dec. 1982) [hereinafter DoD 5240.1-R], and U.S. DEP'T OF DEF., DIR. 5525.5, DoD COOPERATION WITH CIVILIAN LAW ENFORCEMENT OFFICIALS (15 Jan 1986) (C1, 20 Dec. 1989) [hereinafter DoDD 5525.5] (recently cancelled, and recodified as U.S. DEP'T OF DEF., INSTR. 3025.21, DEFENSE SUPPORT OF CIVILIAN LAW ENFORCEMENT AGENCIES (27 Feb. 2013), [hereinafter DoDI 3025.21]. Note also that pursuant to §§1.14(a) and (c) of the Order, the Federal Bureau of Investigation (FBI) is the primary federal agency responsible for *investigating and conducting* foreign intelligence and counterintelligence operations *within* the United States.

[46] EO 12,333, *supra* note 1, § 2.9.

Although EO 12,333 has undergone minor modifications,[48] it has withstood the test of time. It remains the foundation of all DoD intelligence oversight policies and procedures, which are implemented through DoD Regulation 5240.1-R. The remainder of this paper will examine authorities and processes for collecting information on USPs by DoD entities, first the intelligence oversight processes that apply to DoD intelligence components, then the sensitive information processes that apply to all other DoD components.

III. Department of Defense Intelligence Oversight Basics

A. The Intelligence Oversight Process

The current intelligence oversight, or "IO"[49] program, results from efforts to balance the constitutional and privacy interests of United States persons (USPs) against the need to conduct national foreign intelligence activities. In doing so, it establishes which techniques are permissible to obtain information for foreign intelligence or counterintelligence purposes.[50]

As the underlying purpose of the IO program is to ensure the sanctity of constitutional and privacy rights, the primary beneficiary is the USP. A USP is a U.S. citizen; a lawful permanent resident alien; an unincorporated association substantially composed of U.S. citizens or permanent resident aliens; or a corporation incorporated in the United States, unless it is directed and controlled by a foreign government.[51] The DoD intelligence oversight program establishes presumptions about possible USPs. A person or organization outside the United States is presumed not to be a USP, unless specific information to the contrary is in the possession of the government; in practice, a person inside the United States is presumed to be a USP, unless there is information to the contrary.[52] An (illegal) alien in the United States is presumed not to be a USP unless specific information to the contrary is obtained.[53]

PRACTICE TIP: The United States Person (USP)

• Consists of: U.S. Citizens, lawful permanent resident aliens, unincorporated associations composed of U.S. citizens or permanent resident aliens, and corporations incorporated in the United States and under U.S. control

• Basic Presumptions:
Persons and Companies located in United States = USPs;
Located outside of United States ≠ USPs

The DoD IO program applies to personnel and units that have the authority and mission requirements to conduct intelligence activities.[54] Intelligence oversight therefore applies to all Active Army, Army Reserve, and Army National Guard *intelligence* personnel.[55]

But IO is much more than asking "Whom does it apply to?" and "Is there a USP in the mix?" Intelligence oversight review must be viewed as a process; a series of questions must be asked to even initiate the analysis. The legality formula facilitates this analysis: Lawful Mission + Authority = Lawful Intelligence Activity.

PRACTICE TIP: Legality Formula

Lawful Mission (D-FI/D-CI) + Authority = Lawful Intelligence Activity

The first question is "Are the intelligence tasks undertaken consistent with, and pursuant to, a lawfully assigned mission set?" There are *only* two: defense-related foreign intelligence (D-FI) or defense-related counterintelligence (D-CI)?"[56] In short, there must be a clear

[47] *Id*. § 2.11. This prohibition dates back to President Ford's Executive Order 11,905 in 1976. EO 11,905, *supra* note 32.

[48] *See supra* note 9.

[49] Not to be confused with the "other IO," Information Operations. *See* CHAIRMAN JOINT CHIEFS OF STAFF, JOINT PUB. 3-13, INFORMATION OPERATIONS (13 Feb. 2006) [hereinafter JP 3-13].

[50] DOD 5240.1-R, *supra* note 45, paras. C1.1.1, C1.2.

[51] *Id*. para. DL.1.1.25.

[52] *Id*. para. DL1.1.25.2.

[53] *Id*. paras. DL1.25.2 and DL1.25.3.

[54] DOD 5240.1-R, *supra* note 45, para. C1.1. The DoD has identified these organizations as: the NSA/Central Security Service; the DIA; offices within the DoD for the collection of specialized national foreign intelligence through reconnaissance programs; the Assistant Chief of Staff for Intelligence, Army General Staff; the Office of Naval Intelligence; the Assistant Chief of Staff, Intelligence, United States Air Force; the Army Intelligence and Security Command; the Naval Intelligence Command; the Naval Security Group Command; the Director of Intelligence, U.S. Marine Corps; the Air Force Intelligence Service (now dissolved); the Electronic Security Command, USAF (now dissolved and reorganized as the Air Force Intelligence Surveillance and Reconnaissance Agency); the counterintelligence elements of the Naval Investigative Service; the counterintelligence elements of the Air Force Office of Special Investigation; and the 650th Military Intelligence Group, SHAPE. *Id.* para. DL1.1.8.

[55] *See* U.S. DEP'T OF ARMY, REG. 381-10, U.S. ARMY INTELLIGENCE ACTIVITIES paras. 1-1, 1-4m, 1-4n (3 May 2007) [hereinafter AR 381-10]; CHIEF, NAT'L GUARD BUREAU, MANUAL 2000.01, NATIONAL GUARD INTELLIGENCE ACTIVITIES (2012).

[56] *See* EO 13,470, *supra* note 1, § 1.5 (f); U.S. DEP'T OF DEF., DIR. 5240.01, DOD INTELLIGENCE ACTIVITIES (27 Aug. 2007) [hereinafter DoDD 5240.01]. The current Chairman, Joint Chiefs of Staff (CJCS), DSCA Execution Order (EXORD) requires that even when military intelligence capabilities are used to support DSCA-authorized incident awareness and assessment (IAA), intelligence oversight, and sensitive information program restrictions will still apply, and be carefully followed. CHAIRMAN, JOINT CHIEFS OF STAFF, DEFENSE SUPPORT OF CIVIL AUTHORITIES EXORD, para.

DoD *and foreign* nexus to proceed with the mission set. If not, the question is, "Why do it?" This mission constraint has been reinforced by EO 13,470.[57] A tiny sliver of exceptions exist in the Defense Support for Civil Authorities (DSCA) domain in support of Incident Awareness and Assessment. These are extremely limited and are not technically "intelligence activities."[58]

The next question to be asked is, "Is there lawful authority to conduct these missions?" Core authority to conduct intelligence activities comes from presidential orders (pursuant to his authority as commander-in-chief), the Constitution (Articles I and II), and statutory mandates (found in titles 10 and 50 of the U.S. Code). These assign authority to the SecDef or to the military secretaries, and such authority may be further delegated to combatant commands or to service commanders through directives, instructions, regulations, policies or other formalized documentation and orders.[59]

The third and final question is "Since these missions are occurring inside the United States, will they conflict with current or pending FBI operations?"[60] In short, has the unit G2/S2 (Intelligence) staff coordinated with the local field office of the FBI? This is not to say that every domestic defense-related intelligence or counterintelligence mission must be coordinated with or approved by the FBI, but coordination is important to ensure operational de-confliction and avoid a duplication of effort. A vital but oft-forgotten point is that domestic military intelligence activities *must* have a foreign element: DoD has no authority to conduct domestic intelligence activities on its own, in the absence of a DoD nexus. Such activities are also being conducted in the FBI's "front yard"; EO 13,470 makes the Bureau primarily responsible for domestic intelligence and counterintelligence.[61] To avoid needless conflict, coordination and approval of the activity by higher military headquarters is strongly encouraged.

In any military operation, the commander will rely heavily on his intelligence team to provide timely and accurate information. Providing emergency disaster assistance or aiding in consequence management inside the United States poses similar information requirements, although acquisition of this information is much trickier. An operation in Dubuque, Iowa, will impact and involve far more USPs than an operation occurring in Tikrit, Iraq. While intelligence oversight rules are the same in both places, but they will apply far more often in the domestic setting. Thus, military intelligence personnel must take extra care to comply with intelligence oversight programs when operating within the United States.

Toward this end, the Constitution, the National Security Act, FISA, and EO 12,333 operate in concert to establish the baseline policy for protecting the privacy and civil rights interests of USPs from unwarranted invasions by members of the Intelligence Community. Department of Defense Directive 5240.01 applies the requirements of these authorities, and so serves as "the primary authority used as guidance by the Defense Intelligence Components and those performing [a defense-related foreign] intelligence or counterintelligence (CI) function to collect, process, retain, or disseminate information concerning U.S. persons."[62] It is implemented by DoD Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons.*[63] This regulation specifies how and when information on USPs may be collected, retained and disseminated, and its Procedures provide the "sole authority" by which DoD intelligence components may do so.[64] The military services have implemented these requirements through their own regulations.[65] A useful guide to IO is the Defense Intelligence Agency's *Defense HUMINT Service Intelligence Law Handbook* (DIA Handbook).[66] It is frequently referred to as the "Bible of Intel Oversight." It originally covered only human

4.B.8, 4.D.7.A., 9.L.2.A. (2010) [hereinafter CJCS DSCA EXORD] Pursuant to the EXORD, any non-traditional use of DoD intelligence capabilities must be approved by SecDef.

[57] *See supra* note 9.

[58] The DoD standard practice dictates that intelligence assets and capabilities will only be used for traditional intelligence activities, except by express authorization of the SecDef to use such assets otherwise. The IAA constitutes a "quasi-exception," since in support of DSCA operations, otherwise traditional intelligence activities may be conducted to support SecDef approved information gathering missions. These are described in the CJCS DSCA EXORD, *supra* note 56. *See also infra* note 96, and U.S. NORTHERN COMMAND, INSTR. NNCI 14-3, DOMESTIC IMAGERY (5 May 2009). During the course of IAA operations, intelligence oversight rules *still* apply, and United States Persons (USPs) may ***not*** be targeted nor may personal identifying information or *images* be captured. .

[59] *See* U. S. NORTHERN COMMAND, INSTR. 14-103, INTELLIGENCE OVERSIGHT para. 2.6 (16 Apr. 2007).

[60] *Id*. para. C2.5.3.

[61] EO 13,470, *supra* note 1, § 1.5(g).

[62] DODD 5240.01, *supra* note 56.

[63] *Supra* note 2.

[64] The particular procedures detailed in DoD 5240.1-R will hereafter be referred to as the "Procedures."

[65] For example, see AR 381-10, *supra* note 55; U.S. DEP'T OF AIR FORCE, INSTR. 14-104, OVERSIGHT OF INTELLIGENCE ACTIVITIES (23 Apr. 2012); U.S. DEP'T OF NAVY, SECNAVINST 3820.3E, OVERSIGHT OF INTELLIGENCE ACTIVITIES WITHIN THE DEPARTMENT OF THE NAVY (21 Apr. 2005); and, U.S. MARINE CORPS, MCWP 2-1, INTELLIGENCE OPERATIONS (10 Sept. 2003).

[66] U.S. DEF. INTELLIGENCE AGENCY, HUMINT SERVICE INTELLIGENCE LAW HANDBOOK (1995) [hereinafter DIA HANDBOOK]. For practitioners who are new to the intelligence oversight world, perhaps this is the best and most comprehensive guide for understanding and applying basic as well as advanced intelligence oversight concepts.

intelligence (HUMINT)[67] activities conducted by DIA, but its guidance has found DoD-wide applicability in military intelligence operations.

PRACTICE TIP: Know your Key Authorities, and have them readily available, preferably in a "Battle Book"

- EO 12,333. United States Intelligence Activities (4 Dec 1981); amended by EO 13,470 (30 Jul 2008)
  - Establishes parameters, procedures and responsibilities for obtaining National Intelligence
- DoDD 5240.01, DoD Intelligence Activities, (27 Aug 2007, 25 Apr 1988)
  - Implements EO 12,333 and establishes baseline policy to protect USP rights
- DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons (7 Dec 1982, 30 Nov 1979)
  - Implements DoDD 5240.01, establishes specific procedures for collection, retention and dissemination of USP information; for special collection techniques; and for reporting violations of the regulation
- AR 381-10, U.S. Army Intelligence Activities (3 May 2007, 22 Nov 2005, 1 Jul 1984)
  - Implements Intel Oversight program for the U.S. Army

B. Intelligence Oversight Procedures

While each member of the Intelligence Community has its own intelligence oversight regulations or policies that apply to its own respective function or mission set, all are based on these core authorities, and framed in terms of compliance with EO 12,333. The military services, as noted, were no different, as all DoD IO programs are based on DoD 5240.1-R.

Department of Defense Regulation 5240.1-R contains fifteen "procedures" which address intelligence techniques as they directly or indirectly affect the rights and privacy of USPs.[68] These may be grouped into three basic categories. The first, the "General Provisions," consist of Procedures 1-4. These deal with intelligence collection, retention and dissemination. The second group, Procedures 5–10, are the "Special Collection Techniques," and focus on special and technical methods of collection supporting operational intelligence and counterintelligence activities of the DoD.[69] The final group, loosely known as "Administrative Procedures," consist of Procedures 11–15. These address intelligence community conduct and administrative activities.

Procedure 1 (General Provisions) sets the ground rules and scope for intelligence oversight within the DoD. Procedures 2 (collection), 3 (retention), and 4 (dissemination) provide the authority and basic processes by which DoD intelligence components may collect, retain, and disseminate information about USPs.[70] Procedures 5-10 (including electronic and physical surveillance), are extremely complex, and usually require higher HQ or SecDef approval.[71] Procedure 11 deals with contracting practices to ensure compliance with IO programs.[72] Procedure 12 establishes requirements for the DoD Intelligence Community to provide assistance to law enforcement agencies.[73] Procedure 13 prohibits DoD Intelligence Community experimentation on human subjects for intelligence purposes except by informed consent.[74] Procedure 14 addresses DoD Intelligence Community employee conduct.[75] Procedure 15 establishes procedures for identifying, investigating, and reporting questionable activities.[76]

PRACTICE TIP: DoD 5240.1-R Procedures

Procedures 1-4 provide basic information on collection, retention, and dissemination.

Procedures 5-10 are the specialized collection techniques.

Procedures 11-14 are administrative and address conduct.

Procedure 15 is the procedure with the greatest impact: it establishes the procedures and responsibilities for dealing with Questionable Intelligence Activities.

DON'T GET FAMOUS WITH A PROCEDURE 15! This is *not* a way for your higher HQ, SecDef, and Congress to get to know you or your commander.

Remember, the focus of the procedures is on protecting the rights and privacy of USPs; if USP issues are not

[67] "Human Intelligence," or HUMINT, is defined as "[a] category of intelligence derived from information collected and provided by human resources." *See* U.S. DEP'T OF DEF., INSTR. 3305.15, DOD HUMAN INTELLIGENCE (HUMINT) TRAINING (25 Feb. 2008) (certified current through 25 February 2015).

[68] Since many of the concepts involved in intelligence oversight are quite different from those used elsewhere, either in law or military doctrine, a careful review of the definitions in section DL1 of DOD 5240.1-R is highly recommended. Within the intelligence realm, the definitions and processes discussed pertain *only* to intelligence applications, and are presented and applied here with *only* this in mind.

[69] DIA HANDBOOK, *supra* note 66, para. 8-2.

[70] DOD 5240.1-R, *supra* note 45, paras. C2.1, C3.1, and C4.1.

[71] *Id*. paras. C5.1, C6.1, C7.1, C8.1, C9.1, and C10.1.

[72] *Id*. para. C11.1.

[73] *Id*. para. C12.1.

[74] *Id*. paras. C13.1, C13.3.1.

[75] *Id*. para. C14.1.

[76] *Id*. para. C15.1.

involved, there may not be an IO issue.[77] Likewise, the Procedures apply *only* to DoD intelligence components conducting defense-related foreign intelligence or counterintelligence. They do *not* apply to "law enforcement activities, including civil disturbance activities, that may be undertaken by DoD intelligence components . . . ."[78] As noted by the Center for Law and Military Operations (CLAMO),

> [T]he lines between counterintelligence and force protection information are now blurred. Whereas one typically dealt with foreign information and the other domestic, both now involve elements of foreign and domestic information. Military commanders' need for information and intelligence within the homeland is on the rise—they expect force protection information and counterintelligence to be integrated into domestic and domestic support operations due to a heightened awareness of potential terrorist threats. . . DoD intelligence components are subject to one set of rules referred to as intelligence oversight. Everyone else in DoD, except the MCIO's (military criminal investigations organizations), are subject to a different set of rules governed by DoD[] [Directive] 5200.27. Therefore, the commander must direct his need for information or intelligence to the right component. . . . Figuring out the nature of the data and the right unit to gather it are areas that often require [legal] input.[79]

Thus, any intelligence oversight analysis begins with the question, "What is the mission of the DoD Intelligence Community element concerned?" The question is self-limiting, since the DoD Intelligence Community carries out intelligence activities, defined as "[t]he collection, analysis, production, and dissemination of [defense-related] foreign intelligence and [counterintelligence] . . . ."[80] Pursuant to DoD policy, these are the only authorized DoD Intelligence Community missions, regardless of the situation. As CLAMO also points out,

> These authorities establish the operational parameters and restrictions under which DoD intelligence components may collect, produce, and disseminate FI (foreign intelligence) and CI (counterintelligence). Implicit in this authorization, by the definition of FI and CI, is a requirement that such intelligence relate to the activities of international terrorists or foreign powers, organizations, persons, and their agents. Moreover, to the extent that DoD intelligence components are authorized to collect FI or CI within the United States, they may do so only in coordination with the Federal Bureau of Investigation (FBI), which has primary responsibility for intelligence collection within the United States.[81]

Once the DoD Intelligence Community mission parameters have been clearly established, an in-depth analysis may be undertaken to determine what intelligence or information may be collected and why, and whether the collection will be legally appropriate.

Procedures 2 (collection), 3 (retention), and 4 (dissemination) of DoD Regulation 5240.1-R are the integral "process" for collection, retention and dissemination of information about USPs.[82] The linchpin of the IO procedures is Procedure 2 (collection).

1. The Concept of "Collection" Under Procedure 2

To determine whether information may be collected, one must first understand what "collection" is for IO purposes. Procedure 2 states that information is considered collected

---

[77] In many instances, the accurate identification of USPs can be the most difficult aspect of determining if intelligence oversight rules apply to the given situation. Similarly, even if the rights of a USP are neither implicated nor violated, the intelligence activity may still be questionable or illegal, thereby placing it squarely with the restrictions of intelligence oversight. *See, e.g,. id.* procedures 14 and 15.

[78] *Id*. para. C1.1.3.

[79] CTR FOR LAW & MILITARY OPERATIONS, DOMESTIC OPERATIONS HANDBOOK 182–83 (18 July 2006) [hereinafter 2006 DOPLAW HANDBOOK]. *See also* U.S. DEP'T OF DEF., DIR. 5200.27, ACQUISITION OF INFORMATION CONCERNING PERSONS AND ORGANIZATIONS NOT AFFILIATED WITH THE DEPARTMENT OF DEFENSE (7 Jan. 1980) [hereinafter DODD 5200.27].

[80] DODD 5240.01, *supra* note 62, encl. 2, para. E2.7. *"Foreign intelligence"* means information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on international terrorist activities. Executive Order 12,333 defined *"[c]ounterintelligence"* as information gathered and activities conducted to protect against espionage, other 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. EO 12,333, *supra* note 1, para. 3.4(a). *See supra* note 8 and accompanying text.

[81] 2006 DOPLAW HANDBOOK, *supra* note 79, at 183–84; *see also* EO 12,333, *supra* note 1, § 1.14(a); Memorandum Between the FBI and the DoD, Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation (5 Apr. 1979); and Memorandum Between the FBI and the DoD, Supplement to 1979 FBI/DoD Memorandum of Understanding: Coordination of Counterintelligence Matters Between the FBI and DoD (20 June 1996).

[82] DOD 5240.1-R, *supra* note 45, paras. C2.1, C3.1, and C4.1.

"only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties."[83] "Thus, information volunteered to a DoD intelligence component by a cooperating source would be 'collected' under this procedure when an employee of such component *officially accepts*, in some manner, such information for use within that component. Data acquired by electronic means is 'collected' only when it has been processed into intelligible form."[84]

The DIA Handbook further describes "collection" as "gathering plus":

> So, we see that "collection of information" for DoD 5240.I-R purposes is more than "gathering"—it could be described as "gathering, plus . . . ." For the purposes of DoD 5240.1-R, "collection" is officially gathering or receiving information, plus an affirmative act in the direction of use or retention of that information. For example, information received from a cooperating source (e.g., the FBI) about a terrorist group is not "collected" unless and until that information is included in a report, entered into a data base, or used in some other manner which constitutes an affirmative intent to use or retain that information.[85]

This being so, acquiring information to determine if it *can* be collected is also permissible, as long as the collection is consistent with authorized mission sets. The DIA Handbook refers to such actions as "Collectability Determinations":

> Information held or forwarded to a supervisory authority, solely for the purpose of making a determination about its collectability (as described in DoD 5240.1-R, Procedure 1), and which has not been otherwise disseminated, is not "collected." Information may be held for up to 90 days pending such a determination from a higher authority, and if that higher level authority finds it necessary to hold the same information and seek still higher-level advice, an additional period of 90 days will begin to run from the date of the second request. Only when some additional affirmative action is undertaken in the direction of retention or dissemination will such information be considered "collected." In addition, data acquired by electronic means is "collected" only when it is processed into intelligible form.[86]

2. Permissible Collection under Procedure 2

Procedure 2 establishes the baseline for collecting information about USPs. Specifically, the procedure "identifies the kinds of information about United States persons that may be collected by DoD intelligence components and sets forth general criteria governing the means used to collect such information."[87] Before wandering through that analytical maze, it is important to remember that there is no need for intelligence oversight analysis unless: (1) the information being assessed was collected as part of the collecting unit's mission, *and* (2) the information identifies a USP.[88] If collecting the information is not part of the collecting unit's mission, it may not be collected at all, and further analysis is unnecessary. If the information does not *identify* a USP, intelligence oversight restrictions do not apply, and further analysis is unnecessary.

For example, in the aftermath of a major hurricane, which has left hundreds of thousands of people homeless or without food, water, or electricity, the affected states may request federal assistance through FEMA. Suppose FEMA then turns to DoD for specialized airborne capabilities to find people buried in the rubble.[89] Certain search and rescue (SAR) capabilities have been authorized for use during DSCA events.[90] In this situation one of the most useful capabilities is forward looking infrared sensors or "FLIR." While infrared capabilities are usually considered "traditional intelligence capabilities," SecDef has authorized their limited general use for DSCA purposes solely to assist civilian authorities in rescue operations.[91] While such

[83] *Id.* para. C2.2.1.

[84] *Id*. (emphasis added).

[85] DIA HANDBOOK, *supra* note 66, para. 3-7b.

[86] *Id*. para. 3-8; *see also* DOD 5240.1-R, *supra* note 45, procedures 2 and 5 (rules governing the inadvertent interception of conversations of USPs). *Compare* AR 381-10, *supra* note 55, glossary, at 34.

[87] DOD 5240.1-R, *supra* note 45, para. C2.1.

[88] "Information that identifies a USP may be collected by a DoD intelligence component only if it is necessary to the conduct of a function assigned the collecting component." *Id.* para. C2.3.

[89] *See* DODD 3025.18, *supra* note 2, para. 1.d.

[90] *See, e.g.*, CJCS DCSA EXORD, *supra* note 56, paras. 4.B.6, 4.D.

[91] *Id.* para. 4.D.7.A.4. These capabilities are traditional intelligence, surveillance and reconnaissance (ISR) assets, and if employed outside the contiguous United States (OCONUS) would be referred to as "ISR". When such capabilities are utilized in the United States for DSCA purposes, they are referred to as Incident Awareness and Assessment (IAA) packages. SecDef has approved seven such capabilities for DSCA use. Since these are intelligence capabilities, intelligence oversight rules still apply, although collection for traditional intelligence purposes is not being conducted. The rationale is simple: Information on, and the images of, USPs may be collected, even if unintentionally, and so USP's rights must still be protected. This is covered extensively in the CJCS DSCA EXORD, which

assistance is clearly neither a foreign intelligence nor counterintelligence mission, SecDef has approved this highly limited use for the purpose of saving lives, preventing human suffering, or mitigating great property damage within the United States during catastrophic events.[92] Because the mission seeks to employ specialized intelligence capabilities for a use other than foreign intelligence or counterintelligence, it requires specific approval by SecDef.[93]

a. Types of Information

Under EO 12,333, various types of information may be collected about USPs. Subject to special limitations, information constituting foreign intelligence may be collected[94] as long as the intentional collection of foreign intelligence about USPs is limited to persons who are reasonably believed to be acting on behalf of a foreign power;[95] involved in, or constituting an organization which is reasonably believed to be owned or controlled, directly or indirectly, by a foreign power;[96] reasonably believed to be engaged in or about to engage in international terrorist or international narcotics activities;[97] reasonably believed to be prisoners of war or missing in action; or are the targets, the hostages, or victims of international terrorist organizations.[98] Information may be collected about corporations or other commercial organizations if they are believed to be involved in some relationship with foreign powers, organizations, or persons.[99]

Military counterintelligence agents[100] may collect information about a USP if the information actually constitutes counterintelligence. The intentional collection of counterintelligence about USPs must be limited to persons reasonably believed to be engaged or about to engage in intelligence activities on behalf of a foreign power or international terrorist organizations,[101] and persons in contact with such persons.[102]

Information may be collected on USPs if they are reasonably believed to be potential sources of intelligence or assistance to intelligence activities, but only to assess their credibility or suitability to render such assistance.[103] In other words, information may be gathered for the sake of recruiting or assessing sources of intelligence.

Information may also be collected by the DoD to protect defense intelligence sources and methods. That is to say, it may also be collected about USPs who have had access to or possess information that reveals foreign intelligence and counterintelligence sources or methods, when the collection is reasonably believed to be necessary to protect against the unauthorized disclosure of such information.[104] Within the United States, intentional collection of this type of information is limited to present and former DoD employees, present or former DoD contractors' employees; or applicants for DoD or DoD contractor employment.[105] In short, the DoD nexus must be clearly established.

While foreign intelligence and counterintelligence are the mainstays of military intelligence programs, additional collection activities may include assessments of physical security of DoD installations and facilities, during which information may be collected about a USP who is reasonably believed to threaten the physical security of DoD employees, installations, operations, or official visitors.[106] Information may be collected in the course of a lawful physical security investigation.[107] Information may also be collected on USPs during personnel security investigations[108] or while conducting communications security activities or

---

is issued annually in most years. For that reason, review of the most current DSCA EXORD is necessary to determine *which* capabilities are available for DSCA applications.

[92] *See id.* para. 9.J.

[93] While the capabilities may exist to support a given situation, the question remains, "Can they be used in this way?" Because the use of intelligence assets to support DSCA operations is so complex, practitioners are urged to carefully read DoDD 3025.18 and the CJCS DSCA EXORD for a better understanding of how and when such assets may be used. After doing so, if questions remain, please contact us the Office of the Staff Judge Advocate for U.S. Army North or U.S. Northern Command regarding specific questions.

[94] DoD 5240.1-R, *supra* note 45, para. C2.3.3.

[95] *Id.* para. C2.3.3.1.

[96] *Id.* para. C2.3.3.2.

[97] *Id.* para. C2.3.3.3.

[98] *Id.* para. C2.3.3.4.

[99] *Id.* para. C2.3.3.5.

[100] For DoD intelligence oversight purposes, "counterintelligence" is defined as "[i]nformation gathered and activities conducted to protect against espionage, other 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." *Id.* para. DL1.1.5.

[101] *Id.* para. C2.3.4.1.

[102] *Id.* para. C2.3.4.2.

[103] *Id.* para. C2.3.5.

[104] *Id.* para. C2.3.6.

[105] *Id.*

[106] *Id.* para. C2.3.7.

[107] *Id.*

[108] *Id.* para. C2.3.8.

investigations.[109] Also, information on USPs may be collected in support of DoD administrative functions.[110]

When a USP is reasonably believed to be engaged in international narcotics activities, information may be collected on this individual as part of the military effort to assist in the "War on Drugs."[111] Information may also be collected on USPs suspected of engaging in or are about to engage in international terrorism.[112] In support of hostage situations, information may be collected about a USP when the information is needed to protect the safety of any person or organization, including targets, victims, or hostages of international terrorist organizations.[113]

PRACTICE TIP: Intelligence Collection

As a general rule information which identifies a USP may be collected by a DoD intelligence component only if the information is necessary to a function assigned to that component, and if it falls under an authorized category for collectable information, IAW DoD 5240.1-R, Procedure 2.

b. Means of Collection

Information may be obtained with consent.[114] "Consent" is defined as "[t]he agreement by a person or organization to permit DoD intelligence components to take particular actions that affect the person or organization."[115] Consent may be oral or written unless a specific form of consent is required by a particular procedure. It may be implied if adequate notice is provided that a particular action presumes consent to an accompanying action.

Two simple examples may assist in understanding the concept. Both deal with entry into classified physical locations. Entry into a Sensitive Compartmented Information Facility (SCIF) requires requisite security clearances. Personnel seeking to enter or work in the SCIF not only give consent for their background investigations to be conducted, but they also provide extensive family and professional information about themselves of their own accord. This is done consensually since no one is forcing the individuals to access a SCIF; it is their choice as part of their efforts to gain the clearances necessary to work in the facility. Upon accessing a SCIF, all personnel and their belongings are subject to search. Consenting to such search requirements is a prerequisite to gaining access; individuals consent to such searches if they desire entry to the facility. Failure to consent to searches will preclude access.

If DoD intelligence elements must target a USP for collection purposes, they must exhaust the least intrusive means available for collection.[116] Thus, to the extent feasible, any such information should be collected from publicly available information or with the consent of the person concerned.[117] If this cannot be done or will not suffice, collection from cooperating sources (such as law enforcement or other governmental entities) may be a next resort.[118] Failing these methods, pertinent information may be collected using appropriate, lawful investigative techniques that do not require a judicial warrant or the approval of the Attorney General.[119] Finally, when all else fails, DoD Intelligence Community elements may seek approval for use of investigative techniques that require a judicial warrant (usually under FISA) or the approval of the U.S. Attorney General.[120]

Note that all of these collection efforts must be based on a reasonable belief that a USP is somehow involved; such activities may not be taken on mere hunches or "mere suspicion."

So far we have looked at the basics of collecting intelligence that pertains to, or affects the interests and privacy rights of, USPs. In general, if information on a USP can be legally collected, then it can usually be legally retained and disseminated.

3. Retention of Collected Information: Procedure 3

Once it has been determined that information of intelligence value may be collected about a USP, the next step is to decide if the information can be retained by the

[109] *Id.* para. C2.3.9.

[110] *Id.* para. C2.3.13.

[111] *Id.* para. C2.3.10. When violations of law are indicated, these types of collections will also be governed by DOD 5240.1-R, *supra* note 45, procedure 12, and DODI 3025.21, *supra* note 45, para. 4 & encl. 7, requiring that the information be turned over to local law enforcement as soon as possible. Pursuant to the Posse Comitatus Act, 18 U.S.C. § 1385 (2006), DODI 3025.21 (formerly DODD 5525.5) restricts certain forms of direct assistance while and permitting limited indirect assistance to civilian law enforcement. *See* DODI 3025.21, *supra* note 45, para. 4 & encl. 3 (providing a complete listing of permitted and prohibited DoD assistance).

[112] DOD 5240.1-R, *supra* note 45, para. C2.3.3.3.

[113] *Id.* para. C2.3.11.

[114] *Id.*, para. C2.3.1.

[115] *Id.* para. DL1.1.4.

[116] *Id.* para. C2.4.2.

[117] *Id.* para. C2.4.2.1.

[118] *Id.* para. C2.4.2.2.

[119] *Id.* para. C2.4.2.3.

[120] *Id.* para. C2.4.2.4.

DoD Intelligence Community without that person's consent. Retention is covered by DoD 5240.1-R, Procedure 3.[121]

a. The Meaning of "Retention"

The key to retention is the process of retrieval: the term "retention," as used in Procedure 3, refers to the maintenance of information about USPs that can be retrieved by reference to the person's name or other identifying data.[122]

The DIA Handbook provides some clarification of the process:

> The term "retention" means more than merely retaining information in files—it is retention plus retrievability. As stated in DoD 5240.I-R . . . "[t]he term 'retention,' as used in this procedure, refers only to the maintenance of information about United States persons which can be retrieved by reference to the person's name or other identifying data." . . . A very limited view must be taken of this retrievability element. Accordingly, if "nonretainable" information can be retrieved by any means, it must be destroyed. From a policy perspective, it is also important to recognize that information that never should have been collected in the first place must also be destroyed, regardless of whether or not it is retrievable. You may not file unauthorized information about US persons just because it is not retrievable by reference to a person's name or other identifying data. That would not be within the spirit and intent of . . . [EO 12,333] and DoD 5240.I-R, which is to allow collection and retention only when necessary to the performance of a lawful function of the particular intelligence agency involved. The initial lawful function threshold test must always be met.[123]

b. Retainable Information

Information collected properly and lawfully (consistent with authorized mission sets) under Procedure 2 may be retained.[124]

Information collected *incidentally* to authorized collection activities may be retained if it *could* have been collected under Procedure 2.[125] It may also be retained if it is necessary to understand or assess foreign intelligence or counterintelligence;[126] if it constitutes foreign intelligence or counterintelligence which was collected from authorized electronic surveillance measures;[127] or if it "may indicate involvement in activities that may violate [f]ederal, [s]tate, local, or foreign law."[128] However, if the information pertains only to civilian law enforcement or some other non-DoD function, the information may be retained only long enough to transfer it to the agencies whose business it is.[129]

For example, if during the conduct of an authorized DoD foreign intelligence collection activity, a DoD intelligence component identifies a verifiable USP who is a former DoD employee as being complicit in terroristic acts that will have a direct impact on military operations in Kabul, at a minimum, temporary collection will be appropriate. The USP has been identified through foreign intelligence information, and while he may not have been the target, he was nonetheless identified. The information has been collected incidentally. It may be retained because it was properly collected under Procedure 2, it indicates information of a foreign intelligence nature, it possibly implicates DoD foreign and domestic activities, it was incidental to an authorized collection, and it indicates violation of federal, state, or foreign and international laws.[130]

Continuing the example, let us say a DoD intelligence component also determines that the USP has provided security plans to U.S. facilities as well as DoD facilities overseas, intended as targets of terrorism by the terrorist groups he is supporting. Further research reveals he is on the FBI's Watch List and has been assigned a Terrorist Identities Datamart Environment (TIDE) number,[131] which tends to validate a suspected terrorist affiliation. DoD intelligence component analysts may retain the information on the USP for up to ninety days to determine its collectability, and also to identify the most appropriate agencies to receive it. In this case, the FBI would be the most appropriate recipient, especially concerning the domestic threats. However, since

---

[121] *Id.* para. C3.1.

[122] *Id.* para. C3.2.

[123] DIA HANDBOOK, *supra* note 66, para. 3-21.

[124] DOD 5240.1-R, *supra* note 45, para. C3.3.1.

[125] *Id*. para. C3.3.2.1.

[126] *Id*. para. C3.3.2.2.

[127] *Id*. para. C3.3.2.3.

[128] *Id*. para. C3.3.2.4.

[129] *Id.* para. C3.3.3.

[130] *See* DIA HANDBOOK, *supra* note 66, para. 3-22, tbl. 3-3.

[131] Terrorist Identities Datamart Environment (TIDE) is the U.S. Government's (USG) central repository of information on international terrorist identities. TIDE supports the USG's various terrorist screening systems or "watchlists" and the U.S. Intelligence Community's overall counterterrorism mission.

there is a very strong DoD nexus, and the information indicates espionage and related activities are present, the DoD has a strong justification to retain this information for its own counterintelligence and force protection purposes, pending the development of additional information. If retention is not feasible or not recommended, it may be appropriate for the DoD intelligence component to encode the USP's name with a symbol, and as appropriate, include a "hot link" or citation to the originating database.[132]

Retention rules are not absolutely inflexible. Properly collected information may be retained temporarily to determine whether it can be retained longer than ninety days or even permanently as long as "collectability" can be validated.[133] This process is referred to as "temporary retention for determination purposes." Unfortunately a practice has developed of placing non-collectible information or intelligence in a "temporary retention for determination" status for ninety days, and making "interim" use of the information in the meanwhile. This avoidance of the rule is an inappropriate use of the "temporary retention" status. Procedure 3 states that information regarding a USP may be retained for up to ninety days to determine *if* it can be permanently retained and not to use it freely before that determination is made.[134] What is not stated is the obvious: if information regarding a USP is *prima facie* non-collectable or non-retainable, then it *cannot* be retained for ninety days, or any other length of time. Once that determination is made, even if it is made at the outset, the information must be destroyed or immediately transferred to appropriate law enforcement agencies under Procedure 12.[135]

In short, USP information should never be retained "just in case" it might be useful in the future.

PRACTICE TIP: Retention of USP Information

As a general rule, USP information should not be knowingly retained by DoD intelligence components without the consent of the person concerned, except solely for administrative purposes, or in accordance with the specific retention criteria of Procedure 3. Information properly collected under Procedure 2 may usually be retained. Incidentally collected information may only be retained IAW DoD 5240.1-R, Procedure 3, para, C3.3.2.

4. To Disseminate or Not to Disseminate: Procedure 4

In the post-9/11 era, information sharing is a stated objective among governmental agencies of varying U.S. sovereigns.[136] However, neither supporting intelligence oversight law nor DoD policy dealing with information collection and dissemination has kept pace with current legislation. Consequently, despite the stated need to share information, policy restrictions on doing so remain in effect. Information on USPs is no exception.

In military consequence management operations, DoD personnel and commanders often find themselves barraged with requests for information or intelligence regarding USPs in a declared disaster area. The rationales range from force protection to risk amelioration while rendering assistance to non-governmental organizations (NGOs) such as the American Red Cross. Despite the well-intentioned nature of the requestors (or the severity of their needs), great care must be exercised before any USP information can be released.[137]

Information on a USP that has been properly collected and retained can be disseminated without the USP's consent as long as certain criteria are met.[138] Procedure 4 of DoD 5240.1-R lays out the recipients to whom such information may be disseminated.[139] It does not apply to information collected solely for administrative purposes or disseminated pursuant to law or court order that otherwise imposes controls upon such dissemination.[140]

[132] *See* DIA HANDBOOK, *supra* note 66, para. 3-22.

[133] DOD 5240.1-R, *supra* note 45, para. C3.3.4.

[134] *Id.*

[135] *See id*. para. 12.1.; *see supra* note 65; *see also* DODI 3025.21, *supra* note 45, encl. 7.

[136] *See, e.g*., *supra* note 2; *see also* The White House Memorandum on the Terrorism Information Sharing Environment (2 June 2005); United States Attorney General's Memorandum, Section 203 Guidelines Regarding Disclosure of Information Identifying United States Persons (Sept. 23 2005); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272,278-81, § 203 (2001).

[137] Sometimes, during major DSCA operations in response to catastrophic events, civilian law enforcement agencies and related authorities become overwhelmed. While civilian authorities are attempting to regain control of the situation, criminal activity may rise at an alarming rate, ranging from looting of food and water to more extensive serious crimes, involving aggravated rape, assault, and even murder. During these periods of unrest, civil authorities may seek DoD assistance, the Posse Comitatus Act notwithstanding. One of the most frequent requests will be to assist in identifying criminal elements, such as gangs or specific actors, under the mistaken assumption that DoD has such data, or at least the capabilities to acquire it. The tightrope DoD personnel, especially intelligence component members, walk during disaster support is thin, and in the absence of a clear and articulable military purpose (per DODD 3025.18, *supra* note 2), specific assistance in the form of directed collection is prohibited. *See* DODI 3025.21, *supra* note 45, encl. 7.

[138] DOD 5240.1-R, *supra* note 45, para. C4.2.1.

[139] *Id*. para. C4.2.2.

[140] *Id.*

Information may be disseminated only if it was properly collected and retained under Procedures 2 and 3.[141] In addition, the intended recipient must be reasonably believed to have a need to receive the USP information to accomplish a lawful governmental function,[142] *and* must be one of the following: (1) an employee of DoD or a DoD contractor with need for the information in the course of his official duties;[143] (2) a law enforcement entity of federal, state, or local government, that requires the information because it may indicate criminal involvement;[144] (3) an agency within the Intelligence Community (as long as the information has not been derived from signals intelligence);[145] (4) a federal agency authorized to receive this information in the performance of a lawful governmental function;[146] or (5) a foreign government, when dissemination is undertaken pursuant to an agreement or other understanding with that government.[147]

Department of Defense policy requires that any dissemination that does not meet the above criteria be approved by the releaser's legal office *after* consultation with the Department of Justice and DoD General Counsel. It also requires that the decision to release be based on the legal conclusion that the proposed dissemination complies with applicable laws, executive orders, and regulations.[148]

Despite current mandates and trends to ensure that law enforcement and the Intelligence Community share information, complications prevail. When releasing information, especially USP information, to state or local governments, additional care should be taken to determine whether Procedure 12 and the new DoDI 3025.21 apply. Military intelligence personnel should consider the effects of the receiving entities' state laws regarding freedom of information and public access to information held by the state. Some states are quite restrictive while others are far less so, and consider information received from other governmental entities, such as the DoD, to be releasable under their own public information laws.[149] In short, great care should be exercised when releasing information and especially intelligence to civilian authorities, since the recipients may not be able to prevent further release to the public and the media; despite well-intentioned efforts, DoD personnel may inadvertently violate several DoD regulatory authorities by doing so if proper procedures for release are not followed.[150] Keep in mind also that release of information or intelligence to National Guard personnel who are not in title 10 (active duty) status may also be an improper or prohibited release.

PRACTICE TIP: Dissemination of USP Information

DoD intelligence components may disseminate information about US persons without their consent ***only*** IAW DoD 5240.I-R, Procedure 4. This rule also applies to law enforcement information, so be sure to consult Procedure 12, and DoDI 3025.21 before disseminating any of this type of information. Better yet, ***know the rules ahead of time!***

5. The Special Collection Techniques, Procedures 5-10

In this era of mandated intergovernmental information sharing,[151] military intelligence personnel and judge advocates alike must consider not only what information may be collected, retained, and disseminated, but *how* that

[141] *Id*. para. C4.2.1.

[142] *Id*. para. C4.2.2

[143] *Id*. para. C4.2.2.1.

[144] *Id*. para. C4.2.2.2.

[145] *Id*. para. C4.2.2.3. The information may be disseminated to another intelligence agency *without* the disseminating agency having to determine if it is relevant to the receiving agency's mission; information may be disseminated with the express purpose of letting the receiving agency make that determination. *Id.*

[146] *Id*. para. C4.2.2.4.

[147] *Id*. para. C4.2.2.5.

[148] *Id*. para. 4-2*d*. Recalling that the information under consideration is intelligence, and may very well be "raw intelligence", very careful consideration of the necessity for release must be made, and made by senior commanders. Before local judge advocates call the Office of the Secretary of Defense-Office of the General Counsel (OSD-OGC), they should be contacting their higher headquarters for guidance and coordination. Local legal personnel should not be calling OGC; they should always coordinate through command higher headquarters (HQs) and Office of The Judge Advocate General first. *Never* surprise your higher HQ.

[149] *See, e.g.*, Texas Open Records Act, TEX. GOV'T CODE, §§ 552.001-552.118 (2012); The Honorable Kathryn J. Whitmire, Tex. Atty. Gen. Open Records Decision No. 366 (Mar. 24, 1983) (holding that names, addresses, and charges of persons booked in city jail must be disclosed to reporter under the Texas Open Records Act); Ms. Kimberly R. Lafferty, Tex. Atty. General Informal Letter Ruling OR2008-08010 (June 12, 2008) (holding that police report on child custody issue had to be released under the same Act). In short, check the receiving state's laws first and avoid a lawsuit for injunctive relief.

[150] Since there is no composite regulatory material which deals with generic information release, several regulatory authorities should be consulted, *after* a careful review of DoDI 3025.21. *See* U.S. DEP'T OF DEF., DIR. 5230.09, CLEARANCE OF DOD INFORMATION FOR PUBLIC RELEASE (22 Aug. 2008); U.S. DEP'T OF DEF., DIR. 5210.50, UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION TO THE PUBLIC (22 July 2005); U.S. DEP'T OF DEF., DIR. 5230.11, DISCLOSURE OF CLASSIFIED MILITARY INFORMATION TO FOREIGN GOVERNMENTS AND INTERNATIONAL ORGANIZATIONS (16 June 1992); U.S. DEP'T OF DEF., DIR. C-5230.23, INTELLIGENCE DISCLOSURE POLICY (U) (18 Nov. 1983); U.S. DEP'T OF DEF., INSTR. 5230.29, SECURITY AND POLICY REVIEW OF DOD INFORMATION FOR PUBLIC RELEASE (8 Jan. 2009); U.S. DEP'T OF DEF., DIR. 5230.25, WITHHOLDING OF UNCLASSIFIED TECHNICAL DATA FROM PUBLIC DISCLOSURE (6 Nov. 1984).

[151] *See* Exec. Order No. 13,549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, 75 Fed. Reg. 51609 (Aug. 18, 2010); Exec. Order No. 13,556, Controlled Unclassified Information, 75 Fed. Reg. 68675 (Nov. 4, 2010); Exec. Order No. 13,526, Classified National Security Information, 75 Fed. Reg. 707 (Dec. 29, 2009); Exec. Order No. 13,587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, 76 Fed. Reg. 63811 (Oct. 7, 2011).

information may be obtained. Procedures 5 through 10 address methods (such as physical and electronic surveillance) that are often the subject of search warrants under the FISA. Within the DoD, these techniques frequently require approval from the SecDef. The DIA Handbook cautions,

> [A]ll special collection techniques, must be based upon a proper function . . . and must be preceded by a determination that the selection of one of these techniques amounts to the employment of the least intrusive lawful investigative means reasonably available to collect the required information.[152]

For this reason, the DIA Handbook continues,

> "Special collection techniques"—electronic surveillance, concealed monitoring, physical searches, searches and examinations of mail, physical surveillance and undisclosed participation in organizations—are all so potentially intrusive that the policy announced by the President in . . . [EO 12,333] mandates their use on only a limited basis.[153]

There are several specialized techniques which require intense legal scrutiny to ensure compliance with intelligence oversight procedures. Prior coordination by judge advocates with intelligence component personnel to ensure awareness of all missions' parameters is the key. However, from a practical point of view, this seldom happens. Close coordination with senior G2 and S2 personnel may at least increase awareness, particularly when difficult issues may arise. The following is a discussion of the most sensitive, and conceivably problematic, of specialized collection techniques.

a. Electronic Surveillance and Concealed Monitoring: Procedures 5 and 6

Procedure 5 is the most complex of all of the IO procedures. It implements the FISA[154] and applies to seven DoD intelligence activities:

1. All electronic surveillance conducted within the United States to collect "foreign intelligence information," as defined by the FISA;[155]

2. All electronic surveillance conducted by DoD intelligence components against USPs outside the United States for foreign intelligence and counterintelligence purposes;[156]

3. Signals intelligence activities, by elements of the United States Signals Intelligence System, that involve collection, retention, and dissemination of foreign communications and military tactical communications;[157]

4. DoD intelligence use of electronic equipment for technical surveillance countermeasures purposes;[158]

5. Developing, testing, and calibration, by DoD intelligence components, of electronic equipment, that can be used to intercept or process communications and non-communications signals;[159]

6. Training of personnel by DoD intelligence components in the operation and use of electronic communications and surveillance equipment;[160] and

7. The conduct of vulnerability and "hearability" surveys by DoD intelligence components.[161]

All of these activities, if undertaken by intelligence component personnel, must be directly linked to specifically authorized foreign intelligence or counterintelligence mission sets employing these capabilities. Most judge advocates are unlikely to encounter any of these activities unless they are assigned to National Security Agency (NSA) or DIA, or a service-level intelligence headquarters. For this reason, this article will provide only a general overview of Procedure 5.

Since Procedure 5 is designed to ensure the FISA is properly followed by military intelligence when conducting operations in the United States, a little background is in order. The FISA of 1978 was an expansion (to some, or a refinement for others) of Title III of the Omnibus Crime

---

[152] DIA HANDBOOK, *supra* note 66, para. 5-2.

[153] *Id.* para. 6-22.

[154] 50 U.S.C. §§ 1801–62 (2011). For an outstanding summary of what the FISA is, what it does and how it works, see JAMES G. MCADAMS, FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA): AN OVERVIEW (n.d.), *available at*http://www.fletc.gov/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf; *see also* DIA HANDBOOK, *supra* note 66, ch. 4, § II; *see also* ELIZABETH B. BAZAN, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT—OVERVIEW AND MODIFICATIONS (2008) (providing an in-depth review of the Act and discussions of relatively recent updates to it).

[155] DoD 5240.1-R, *supra* note 45, para. C5.1.

[156] *Id*. para. C5.2.

[157] *Id*. para. C5.3.

[158] *Id*. para. C5.4.

[159] *Id*. para. C5.5.

[160] *Id*. para. C5.6.

[161] *Id*. para. C5.7.

Control and Safe Streets Act of 1968, also known as the Federal Wiretap Statutes.[162] When dealing with the concept of wiretaps, we are really discussing nonconsensual electronic eavesdropping or surveillance of USPs' communications. Electronic surveillance, under Procedure 5, consists of "the acquisition by an electronic . . . or other surveillance device of the contents of any wire or radio communication" to or from a USP, but under circumstances where the USP has a reasonable expectation of privacy, and has not given consent.[163] Procedure 5 comes into play when such surveillance is conducted against USPs by DoD intelligence components in pursuit of "foreign intelligence information."[164]

This distinction is important since Procedure 5 has nothing to do with law enforcement activities. Procedure 5 covers only electronic surveillance by DoD intelligence components for foreign intelligence and counterintelligence purposes, and to certain technical aspects of electronic surveillance which are closely allied with specific foreign intelligence collection and counterintelligence activities.[165]

Procedure 5 is divided into three general categories: non-emergency and emergency situations; situations which occur within and outside the United States; and finally, activities which affect USPs and non-USPs.[166] Perhaps the most important point to note is that for purposes of DoD intelligence operations, *absolutely no* electronic surveillance activity may be carried out within the United States, whether against USPs or non-USPs, without U.S. Attorney General approval. Procedure 5 requires a strong evidentiary showing to secure approval of electronic surveillance in the United States. Even in emergency situations, all requests must be cleared through the DoD General Counsel and approved by the U.S. Attorney General.[167]

Inside the United States, such surveillance may only be conducted under warrant issued by the Foreign Intelligence Surveillance Court.[168] Within the DoD, only the SecDef, the Deputy SecDef, the secretary of a military department, or the undersecretary of a military department may even request approval of electronic surveillance from that court, and the request must be made through the Attorney General after consultation with the DoD General Counsel. Outside the United States, this kind of surveillance requires approval from the Attorney General, who must be provided sufficient information to make a probable cause determination that the person being surveilled is a proper target, that the surveillance is necessary to obtain "significant foreign intelligence or counterintelligence," and that less intrusive means would not suffice to obtain it.[169] In emergency situations, the Attorney General may approve electronic surveillance of USPs inside the United States,[170] and under limited circumstances a service secretary or even a general officer may approve some forms of surveillance outside the United States.[171]

PRACTICE TIP: Electronic Surveillance Approval

A DoD intelligence component may ***not*** conduct electronic surveillance directed against a U.S. person without first securing approval from a properly designated approval authority. Know your approval authorities and the procedures to coordinate and request authority to conduct electronic surveillance.

[162] Title III of the Act is codified at 18 U.S.C. § 2510 to § 2522. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 211–23 (1968).

[163] Specifically, "electronic surveillance" is defined as

> [a]cquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction finding equipment solely to determine the location of a transmitter.

DOD 5240.1-R, *supra* note 45, para. DL.1.1.9; *see also id.* para. C5.1.1; 50 U.S.C. § 1804(f)(1), (3), (4) (2011) (surveillance in the United States); DOD 5240.1-R, *supra* note 45, para. C5.2.1 (surveillance outside the United States).

[164] DOD 5240.1-R, *supra* note 45, paras. C5.1.1 and C5.1.2.1. "Foreign intelligence information" is defined in the Foreign Intelligence Surveillance Act as information "that relates to, and if concerning a United States person is necessary to" the ability of the United States to protect against hostile acts by foreign powers, sabotage, international terrorism, the proliferation of weapons of mass destruction, or clandestine intelligence activities by foreign powers; and also information "that relates to, and if concerning a United States person is necessary to," the national defense, the security, or the conduct of the foreign affairs of the United States. 50 U.S.C. § 1804(e). Obviously, this definition includes counterintelligence.

[165] DIA HANDBOOK, *supra* note 66, para. 4-3.

[166] *Id*. para. 4-18.

[167] Signals intelligence activities are coordinated through the NSA and its Office of General Counsel to the Attorney General. *Id.* para. 4-19.

[168] DOD 5240.1-R, *supra* note 45, para. C5.1.2.1.

[169] *Id.* para. C5.2.3.2. The regulation details various proper targets for electronic surveillance of USPs outside the United States, including persons engaged in clandestine intelligence or terrorism and corporations controlled by foreign powers. *Id.* para. C5.2.3.2.1. The entity seeking approval must also provide information showing that any physical intrusion necessary to effect the monitoring will be the least amount necessary to accomplish the objective, a statement of the period of time (not to exceed 90 days) that the monitoring will take place, and a description of the intended dissemination of the intelligence. *Id.* para. C.5.2.3.5-7.

[170] *Id.* para. C5.1.2.3.1.

[171] *Id.* para. C5.2.5. However, the general officer must be one "at the overseas location in question, having responsibility for either the subject of the surveillance, or responsibility for the protection of the persons, installations, or property that is endangered." *Id.* para. C5.2.5.2.1. For specific criteria and limitations, *see id.* para. C5.2.4.

Compared to Procedure 5, concealed monitoring under Procedure 6 is much less complex in application and process. "Concealed monitoring" is defined as

> . . . targeting by electronic, optical, or mechanical devices a particular person or a group of persons without their consent in a surreptitious and continuous manner. Monitoring is surreptitious when it is targeted in a manner designed to keep the subject of the monitoring unaware of it. Monitoring is continuous if it is conducted without interruption for a substantial period of time.[172]

While this description may sound similar to a Procedure 5 scenario, the most important factor in distinguishing concealed monitoring from electronic surveillance is the USP subject's reasonable expectation of privacy[173]—if the surveillance violates a reasonable expectation of privacy, it should be handled as a form of electronic surveillance in accordance with Procedure 5.[174] If it does not, then it may be processed under the less rigorous standards of Procedure 6. The DIA Handbook goes so far as to make this *the* distinction: if there is no reasonable expectation of privacy, then the issue is one of concealed monitoring; but if there is a reasonable expectation of privacy, then the issue becomes one of electronic surveillance.[175] "While this may be somewhat of an over–generalization, it is true most of the time, at least where electronic devices are involved."[176]

The issue of whether the subject of concealed monitoring possesses a reasonable expectation of privacy must be evaluated by the legal office responsible for advising the DoD intelligence component that intends to conduct the monitoring.[177] This is best accomplished *prior* to seeking approval for the activity; we recommend that requests for approval include an already-complete legal review addressing the issue of reasonable expectation of privacy, and legal justification supporting the activity.

Another general rule of Procedure 6 is that concealed monitoring may be conducted by DoD intelligence components within the United States, or outside the United States against USPs, but *only* for foreign intelligence and counterintelligence purposes, and only *after* approval has been obtained for the activity.[178] Approval must come from the Deputy Under Secretary of Defense (Policy); the Director, Defense Intelligence Agency; the Director, NSA; or, at service levels, the Assistant Chief of Staff for Intelligence, Department of Army; the Director, Naval Intelligence; the Director of Intelligence, U.S. Marine Corps; the Assistant Chief of Staff, Intelligence, U.S. Air Force; the Commanding General, Army Intelligence and Security Command; the Director, Naval Investigative Service; and the Commanding Officer, Air Force Office of Special Investigations.[179] Approval at these levels also requires a legal review by the senior servicing legal office.[180] To approve a concealed monitoring operation, the official must find that such monitoring is necessary to conduct assigned foreign intelligence or counterintelligence functions, and *does not* constitute electronic surveillance.[181]

In addition to requiring approval, concealed monitoring is subject to other limitations. Within the United States, a DoD intelligence component may conduct concealed monitoring only on a facility owned or leased by the DoD, or else in the course of an investigation conducted pursuant to the Agreement Between the Deputy SecDef and the Attorney General.[182] Outside the United States, it may be

---

[172] *Id.* para. C6.2.1.

[173] In the context of Procedure 6, reasonable expectations of privacy exist when a reasonable person in the particular circumstances involved is entitled to believe his actions are not subject to monitoring by electronic, optical, or mechanical devices. *Id.* para. C6.2.1. However, the analytical template for determining whether a "reasonable expectation of privacy" serves as the sole determinant for unreasonable searches and seizures may be significantly altered as a "new" standard has emerged in *United States v. Jones*, 132 S. Ct. 945, 950 n.3 (2012), where the U.S. Supreme Court held that the Government's physical intrusion on a constitutionally protected area (including an "effect" as that term is used in the Fourth Amendment) for the purpose of obtaining information constitutes a search under the Fourth Amendment. In this case, law enforcement officials attached a GPS tracking device to the vehicle of a suspected drug dealer while it sat in a public parking lot. The Court expanded the concept of a "reasonable expectation of privacy" (Katz v. United States, 389 U.S. 347, 351 (1967)) to include a requirement to determine whether the government "trespassorily inserted an information-gathering device" onto the subject's property. *Jones*, 132 S. Ct. at 952. The GPS device was planted by federal agents with an expired and limited geographic jurisdictional warrant in hand. However, the Court did not reach the decision as to whether a warrant would have been required, or even relevant to the search. The implications of *Jones* for foreign intelligence and counterintelligence activities are wide-reaching, and will hopefully be considered in the current rewrite of DOD 5240.1-R. For an excellent summary of the findings of the Supreme Court in *Jones*, see Emily Johnson-Liu, *So Tell Us Already! Do We Have to Get a Warrant or Not?*, 42 PROSECUTOR (TEXAS), Mar.–Apr. 2012, at 1, *available at* http://www.tdcaa.com/journal/so-tell-us-already-do-we-have-get-warrant-or-not.

[174] DOD 5240.1-R, *supra* note 45, para. C6.1.2.

[175] DIA HANDBOOK, *supra* note 66, para. 5-8.b.

[176] *Id*.

[177] DOD 5240.1-R, *supra* note 45, para. C6.2.3. For example, a person walking out of his or her residence into a public street ordinarily would not have a reasonable expectation that he or she is not being observed or even photographed; however, the same person ordinarily would have a reasonable expectation of privacy inside his or her residence. *Id*.

[178] *Id.* para. C6.3.2.

[179] *Id.* para. C6.3.3.

[180] *Id.* para. C6.2.3.

[181] *Id*. para. C6.3.2.

[182] *Id*. para. C6.3.1.1; *see also* Agreement Between the Deputy SecDef and Attorney General (Apr. 5, 1979).

conducted only on a facility owned or leased by the DoD, or else after coordination with the CIA.[183]

PRACTICE TIPS: Concealed Monitoring

- Concealed Monitoring vs. Electronic Surveillance
  - If no Reasonable Expectation of Privacy exists → Concealed Monitoring rules apply;
  - If a Reasonable Expectation of Privacy exists → Electronic Surveillance rules apply
- Concealed monitoring by DoD intelligence components within the United States, or outside the United States may ***only*** be conducted against US persons for foreign intelligence (FI) and counterintelligence (CI) purposes IAW DoD 5240.1-R, Procedure 6, and only ***after*** appropriate approval has been received.

b. Physical Searches and Opening Mail: Procedures 7 and 8

Procedure 7 pertains to nonconsensual physical searches of persons and property for foreign intelligence or counterintelligence purposes.[184] It is divided into two categories: nonconsensual physical searches within the United States, and nonconsensual physical searches outside of the United States.[185] Just as such these searches are limited in purpose, they are limited in targets as well. Within the United States, counterintelligence special agents may *only* search the persons and property of active duty military personnel, and only when authorized by a military commander empowered to approve physical searches in accordance with Rule for Court-Martial 315(d).[186] This authorization must be based on a finding of probable cause to believe such persons are acting as agents of foreign powers.[187]

If DoD intelligence components need searches to be conducted within the United States, they may request the assistance of the FBI to do so.[188] Outside the United States, they may themselves conduct such searches of active duty military personnel, again only upon a finding of probable cause by a commander authorized to issue search authorizations.[189] Non-military USPs may be subjected to nonconsensual searches outside the United States only with approval of the Attorney General.[190] Whether within or outside of the United States, the probable cause findings must establish that the subject of the search is a proper target (that is, an "agent of a foreign power"),[191] that the search is necessary to obtain significant foreign intelligence, and that less intrusive means would not suffice to obtain it. Requests to the FBI or Attorney General must include information to support these findings,[192] and be submitted through the SecDef or Deputy SecDef, the secretary or the undersecretary of a military department, the Director of the NSA, or the Director of the DIA.[193]

PRACTICE TIP: Physical Searches

Unconsented physical searches of persons or property may be conducted by DoD intelligence components only for foreign intelligence or counterintelligence purposes, but only after receiving approval by a properly designated approval authority. Know your search limitations regarding purpose, persons and property, IAW DoD 5240.1-R, Procedure 7.

Procedure 8 is simple in scope as it applies to all mail opening and mail covers in U.S. postal channels for foreign intelligence and counterintelligence purposes. In general, three basic rules must be followed to comply with this Procedure:

1. Mail covers must be requested, and if used within the United States, must be undertaken in accordance with U.S. Postal Service (USPS) regulations;[194] mail covers outside the United States may only be accomplished in accordance with the law of the host country or Status of Forces Agreement;[195]

2. Opening mail sealed against inspection (i.e., first class mail) in United States postal channels, including APO and FPO channels, requires a judicial warrant or search authorization issued pursuant to law;[196] and

[183] DOD 5240.1-R, *supra* note 45, para. C6.3.1.2. Coordination with the host nation government is also required if the governing Status of Forces Agreement says so. *Id.*

[184] *Id.* para. C7.1.

[185] *Id.* para. C7.3.

[186] *Id*. para. C7.3.1.

[187] *Id.*

[188] *Id.* para. C7.3.1.2.

[189] *Id*. para. C7.3.2.1.

[190] *Id*. para. C7.3.2.2.

[191] The language in Procedure 7 is identical to that used in Procedure 5 for identifying proper targets for electronic surveillance. It includes persons engaged in clandestine intelligence activities or terrorism on behalf of a foreign power, an officer or employee of a foreign power, a corporation controlled by a foreign power, and persons acting unlawfully under the direction of a foreign power.

[192] Just like requests for electronic surveillance under Procedure 5, requests for searches under Procedure 7 require information sufficient to support a finding that any physical intrusion is the least necessary to accomplish the mission, and the intended dissemination of the information.

[193] DOD 5240.1-R, *supra* note 45, paras. C7.3.1.2, C7.3.2.3.

[194] *Id*. para. C8.3.3.; *see also* U.S. Postal Service Regulations, 39 C.F.R. § 233.3 (2002).

[195] DOD 5240.1-R, *supra* note 45, para. C8.3.2.

[196] *Id*. para. C8.3.1.

3. Opening of mail to or from U.S. persons found *outside* United States postal channels, including APO and FPO channels, is permitted only with the approval of the Attorney General of the United States.[197]

For purposes of Procedure 8, a "mail cover" refers to the process by which a record is made of any data appearing on the outside cover of any class of mail as permitted by law, other than that necessary for the delivery of mail or administration of the USPS.[198]

If the mail in question is in U.S. postal channels, DoD intelligence components may request a mail cover for first class mail, for counterintelligence purposes.[199] Otherwise, DoD intelligence components are prohibited from detaining or opening first-class mail within U.S. postal channels for foreign intelligence and counterintelligence purposes, or from requesting such action by the U.S. Postal Service.[200] However, if mail is second, third, or fourth class, DoD counterintelligence agents may request postal authorities to inspect the contents for these purposes, or to detain mail that may become subject to search.[201] When mail is outside United States postal channels, DoD intelligence components may request mail covers from the host nation government.[202] If the mail is to or from a USP, the Attorney General may approve a request to open the mail, and the request shall be processed and treated as a request for a physical search under Procedure 7.[203] If the mail is not to or from a USP, then the head of a DoD intelligence component may authorize its opening as a search conducted pursuant to applicable Status of Forces agreements.[204]

PRACTICE TIP: Searches and Examinations of Mail

Searches of mail and mail covers may only be conducted or requested by DoD intelligence components upon approval by a properly designated approval authority, and only for counterintelligence purposes IAW DoD 5240.1-R, Procedure 8. Know your approval authorities based on the type and location of the activity sought.

c. Physical Surveillance and Undisclosed Participation: Procedures 9 and 10

Procedures 9 (Physical Surveillance) and 10 (Undisclosed Participation in Organizations) involving USPs within in the United States may be related activities at different points on a time-line. From an operational standpoint, the process of surveillance may lead to, or best be accomplished by, intermingling with or infiltrating an organization to gain a better vantage point. Activities covered by Procedure 9 may evolve into broader operations that are restricted by Procedure 10. Both procedures concern the development of information which may be processed into intelligence. Both are potentially intrusive, and must be restricted in their employment, especially when conducted in the United States and when USPs are involved.[205]

Procedure 9 applies only to the physical surveillance of USPs by DoD intelligence components for foreign intelligence and counterintelligence purposes.[206] It does not apply to law enforcement and criminal investigatory surveillances. "Physical surveillance" means "a systematic and deliberate observation of a person by any means on a continuing basis, or the acquisition of a nonpublic communication by a person not a party thereto or visibly present thereat through any means not involving electronic surveillance."[207]

This definition thus covers two distinct targets of activities: (1) persons being observed and (2) nonpublic communications being acquired, through other than electronic surveillance.[208] This becomes even more complex when considering that the standards for application between the two are different, and also differ from those used in other Procedures.[209] Specifically, surveillance of a person involves observation that is methodical or done with purposeful regularity, and must be intentional or premeditated.[210] Surveillance may only be of a natural person; abstract entities such as entire organizations or corporations cannot be accomplished in their entireties; only specific (human) members of organizations or corporations may be surveilled.[211] The surveillance may be conducted "by any

[197] *Id*. para. C8.3.2.1.

[198] *Id*. para. C8.2.3.

[199] *Id.* paras. C8.3.3.1, C8.2.3.

[200] *Id*. para. C8.3.1.1.

[201] *Id.* para. C8.3.1.2.

[202] *Id.* para. C8.3.3.2.

[203] *Id.* para. C8.3.2.1. *See* DIA HANDBOOK, *supra* note 66, tbl.6-1 for specific checklists required for probable cause showings.

[204] DOD 5240.1-R, *supra* note 45, para. C8.3.2.2.

[205] Note also that Procedure 10 may represent a form of activity which may be similar to that covered by Procedure 11, Contracting for goods and services, since both may involve cover operations in support of clandestine aspects of assigned activities. This concept will be addressed more extensively of our discussion of Procedure 11. *See also* the DIA HANDBOOK, *supra* note 66, para. 7-2.

[206] DOD 5240.1-R, *supra* note 45, para. C9.1.

[207] *Id.* para. C9.2.

[208] DIA HANDBOOK, *supra* note 66, para. 6-15.

[209] *Id*. para. 6-16.

[210] *Id.* para. 6-17.

[211] *Id.*

means," but what is unstated is that if any sort of electronic capability is used to augment the surveillance, such as use of a GPS tracking device,[212] then Procedure 6 procedures must also be followed.[213] Finally, "on a continuing basis" simply means uninterrupted observation.[214]

As to the second facet of the Procedure, acquisition of nonpublic communications, the situation becomes a bit more challenging. The problem is definitional: Procedure 9 does not define what a "nonpublic communication" is.[215] The DIA Handbook suggests that the definition is "communication that is neither available for general public consumption, nor lawfully available to the casual observer."[216] The magic words are "not lawfully available to the casual observer."

From a criminal law perspective, myriad possibilities come to mind, so an illustration may assist in understanding the finer points of this second aspect of the Procedure. If a U.S. Army undercover operative overhears conversation of a DoD Civilian employee who is a USP target at a public restaurant in Dubuque, Iowa, she is *not* conducting physical surveillance because the target's discussions are available to any casual listener in earshot. Conversely, if the operative has been coming to the same restaurant for six months at the same time the target has, knows the target always uses the same booth, and with permission from the restaurant owner, she secretes herself in the hollow space of the wall adjacent to the booth in order to hear the whispers between the target and his foreign handling agent, then the operative *is* conducting physical surveillance, and will require approval from her DoD intelligence component's leadership.[217]

Here lie the distinctions between Procedure 9 and the law enforcement domain. Since the conversations are taking place in a space open to the public, the target and his handler have no reasonable expectation of privacy.[218] A judicial warrant or search authorization would not be required to get this information for a criminal prosecution (unless of course the restaurant owner is not informed).[219] But since we are talking about DoD intelligence component personnel surveilling a USP, the regulatory requirements of IO will apply.[220]

Under Procedure 9, DoD intelligence components may conduct nonconsensual physical surveillances only for foreign intelligence and counterintelligence purposes within the United States, against military USPs.[221] Surveillance of civilian USPs in the United States who are not within the investigative jurisdiction of DoD intelligence components is prohibited.[222] However, surveillances may be conducted of civilians who are present or former employees of the DoD, present or former contractors of the DoD, their present or former employees, and applicants for such employment or contracting.[223] In short, a DoD jurisdictional nexus must exist. Physical surveillance within the United States that occurs off a DoD installation must be coordinated with the FBI and other law enforcement agencies, to ensure mission deconfliction.[224] Outside the United States, DoD intelligence components may conduct surveillance of non-DoD USPs provided the surveillance is done in the course of a lawful intelligence or counterintelligence investigation,[225] is consistent with host country laws and policies and any status of forces agreements,[226] and is being done to collect significant information that cannot be obtained by other means.[227]

---

[212] *See* United States v. Karo, 468 U.S. 705, 715–19 (1984) (The Supreme Court held the Fourth Amendment's protection from unreasonable searches and seizures applied where law enforcement agents used an electronic beeper device to monitor a can of ether without a warrant). *Karo*, along with *Kyllo v. United States*, 533 U.S. 27, 33–40 (2001), remain the core standards against which the intelligence community evaluates Procedures 5, 6 and 9 activities.

[213] DIA HANDBOOK, *supra* note 66, para. 6-17c.

[214] *Id.* para. 6-17d.

[215] DOD 5240.1-R, *supra* note 45, para. DL1.1.9 (addressing "nonpublic communication" in the context of Procedure 5 with a focus on electronic surveillance)

> Electronic Surveillance. Acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction finding equipment solely to determine the location of a transmitter. (Electronic surveillance within the United States is subject to the definitions in the Foreign Intelligence Surveillance Act of 1978 (reference (b)).)

Since Procedure 9 specifically deals with non-electronic surveillance, there is a gap in definitions. However, additional cautions must be used in light of *United States v. Jones*, which focused not on communications of the parties involved, but rather on a transmission of GPS signals identifying the movement and locations of a transmitter placed on a subject's vehicle. *See* Johnson-Liu, *supra* note 166.

[216] DIA HANDBOOK, *supra* note 66, para. 6-18c.

[217] *Id.*

[218] *Id*. para. 6-18b and c.

[219] *Id.*

[220] *Id.*

[221] DOD 5240.1-R, *supra* note 45, para. C9.3.1.

[222] DIA HANDBOOK, *supra* note 66, tbl.6-2.

[223] DOD 5240.1-R, *supra* note 45, para. C9.3.1.

[224] *Id.*

[225] *Id.* para. C9.3.2.

[226] *Id.* para. C9.3.2.1.

[227] *Id.* para. C9.3.2.2.

Physical surveillances must be approved prior to commencement; approval may come from the head of a DoD intelligence component (or his designees) if the person under surveillance is inside the United States or is within the investigative jurisdiction of the DoD.[228] Otherwise, the Deputy Under Secretary of Defense (Policy) is the approval authority.[229]

PRACTICE TIP: Physical Surveillance

Physical surveillance may only be conducted by DoD intelligence components on USPs for foreign intelligence and counterintelligence purposes, and only pursuant to the appropriate approval authority IAW DoD 5240.1-R, Procedure 9. Remember to ***always*** deconflict off-base activities with the FBI.

Procedure 10 pertains to undisclosed participation by employees of any DoD intelligence component in any organization located within the United States, or any organization outside the United States that is a USP, when that participation is undertaken on behalf of any DoD intelligence component organization, even in some small part.[230] "Participation" means "any action undertaken within the structure or framework of the organization," including serving as a representative or agent of the organization; acquiring membership; attending meetings not open to the public, including social functions for the organization as a whole; carrying out the work or functions of the organization; and contributing funds to the organization other than in payment for goods or services[231]

Participation occurs on "behalf of an entity of the intelligence community", when the participant is *tasked* or *requested* to take some action within an organization for the benefit of the requesting intelligence agency.[232] Circumstances requiring authorized concealment of a person's intelligence affiliation for reasons of operational cover, or joining an organization in order to enhance cover, will still fall within the purview of Procedure 10.[233]

Procedure 10 is organization-focused, and applies to undisclosed participation in: (1) Any organization located within the United States; and, (2) Any organization located outside the United States which constitutes a USP.[234]

An "organization" is "any group whose existence is formalized in some manner or otherwise functions on a continuing basis," including business entities, professional societies, and political organizations.[235] An organization is "within the United States" if it is physically located there, even if it is not a USP. A branch of a U.S. organization located elsewhere is not "within the United States" (though it may still be a USP).[236]

Procedure 10 forbids employees of DoD intelligence components to participate secretly in organizations that are either USPs or located within the United States on behalf of the DoD Intelligence Community. They may only participate if they disclose their affiliation with the intelligence component to an appropriate official of the organization.[237] In other words, surreptitious infiltration for official purposes is generally forbidden.

It is important to note that there is a clear distinction between participation *on behalf* of an intelligence agency and acting as a *cooperating source* for the agency. While participation on behalf of an intelligence agency is restricted by Procedure 10, acting as a cooperating source is not.[238] For example, a military intelligence (MI) officer's spouse may voluntarily give her information about a target organization and it may be utilized by the DoD Intelligence Community, as long as neither she nor her husband has been requested to provide that information.[239] Procedure 10 does not restrict the legitimate cooperation of persons with U.S. intelligence components' activities. For this reason, any information of potential intelligence value may be received from cooperating sources by DoD intelligence components. This

---

[228] *Id.* para. C9.3.3.1. *See also*, DIA HANDBOOK, *supra* note 66, tbl.6-2.

[229] DOD 5240.1-R, *supra* note 45, para. C9.3.2.2.

[230] *Id*. para. C10.1. Participation in an organization for primarily personal purposes at outset, but ultimately shift to official collection activities at some later point in time, will be subject to Procedure 10 restrictions. *See also* the DIA HANDBOOK, *supra* note 66, para. 7-3.

[231] DOD 5240.1-R, *supra* note 45, para. C10.2.4.

[232] DIA HANDBOOK, *supra* note 66, para. 7-6c.

[233] DOD 5240.1-R, *supra* note 45, para. C10.2.2.2.6. *But see* DIA HANDBOOK, *supra* note 66, para. 7-6c. This apparent inconsistency, is essentially interpretative, and arises in part due to slight variations which occurred in earlier iterations of DoD 5240.1-R, upon which the DIA Handbook was based. *See also* AR 381-10, *supra* note 55, para. 10-3 (classifying "participation" as either general or specific. Developing or maintaining an authorized cover falls within the purview of Procedure 10, but requires approval from Deputy Chief of Staff G–2, the Commander of Intelligence & Security Command (INSCOM), or the Commander of U.S. Army Special Operations Command, in accordance with paragraph 10-4).

[234] DOD 5240.1-R, *supra* note 45, para. C10.1. *See also* DIA HANDBOOK, *supra* note 66, para. 7-3.

[235] DOD 5240.1-R, *supra* note 45, para. C10.2.2. Note also that "organizations" within the cyberlaw context may also constitute organized and centrally managed chatrooms, or chatrooms requiring membership and access privileges. These concepts will be addressed further in future articles.

[236] *Id.* para. C10.2.3.

[237] *Id.* para. C10.3.

[238] DIA HANDBOOK, *supra* note 66, para. 7-6e.

[239] In short, information of this nature may be *voluntarily* provided, and thus acted on by a DoD Intelligence Component, as long as no *tasking* to develop or provide this information has been made to either the MI officer or her husband in this case. As in a criminal setting involving informants, neither may be operating as an agent for the government *with regard to the particular information provided*.

principle applies to family members, members of organizations or associations, and to walk-in sources at DoD intelligence offices. When the information does not fall within the jurisdiction of the DoD, then it may be passed to an appropriate agency, and not retained in DoD intelligence component files.[240]

However, DoD intelligence components *may* undertake undisclosed participation if their participation is accomplished for a lawful foreign intelligence or counterintelligence purpose, and has been approved *in advance* by an authorized senior intelligence official.[241] If authorization is granted, the period of participation may not exceed twelve months.[242] Further participation that needs to last longer than twelve months must be re-approved on an annual basis, and must continue to meet all the requirements of Procedure 10.[243]

In general, even an approved undisclosed participation may *not* be undertaken for the purpose of *influencing* the activities of the organization or its members.[244] Undisclosed participation activities are undertaken to gather information, *not* to influence an organization composed of USPs. No participation under Procedure 10 may be authorized for the purpose of influencing the activities of an organization, or its members, unless the participation is undertaken on behalf of the FBI in the course of a lawful investigation, or the organization concerned is composed primarily of individuals who are not USPs and is reasonably believed to be acting on behalf of a foreign power.[245]

A DoD intelligence component that desires to undertake participation for the purpose of influencing an organization or its members must request authority for these activities, first through U.S. Army channels, then from the Deputy Under Secretary of Defense (Policy), and must present all relevant facts justifying the participation, and explaining the nature of contemplated activity. Participation may be approved by the Deputy Under Secretary of Defense (Policy), but only with the concurrence of the DoD General Counsel.[246]

PRACTICE TIP: Undisclosed Participation

DoD intelligence personnel may only participate in organizations for official purposes without disclosing their DoD intelligence component affiliation only under limited circumstances and ***only*** after receiving approval from a properly designated approval authority, IAW DoD 5240.1-R, Procedure 10. Remember that this restriction also applies to cyber-activities; depending on the facts and circumstances, an "organization" may very well include web sites and chat rooms. ***Always*** coordinate with your servicing legal advisor prior to any participation activity.

6. Administrative and Enforcement Procedures: Procedures 11-15

There are five intelligence oversight administrative and enforcement procedures. Each can affect missions under the procedures already discussed.

a. Contracting for Goods and Services: Procedure 11

Procedure 11 pertains to procurement of goods and services by DoD intelligence components within the United States, and when the component may buy goods or services without revealing the sponsorship of the purchases or the contract.[247] It does not apply to contracting with other governmental entities or to the enrollment of individual students in academic institutions.[248]

---

[240] *Id*. *See also* DOD 5240.1-R, *supra* note 45, Procedure 12.

[241] DOD 5240.1-R, *supra* note 45, para. C10.3.2.2. Authorizing officials include the Director, DIA, the Deputy Chief of Staff for Intelligence, Department of Army, the Commanding General, U.S. Army INSCOM, the Director of Naval Intelligence, the Director of Intelligence, U.S. Marine Corps, the Assistant Chief of Staff, Intelligence, USAF, the Director, Naval Investigative Service, the Commanding Officer, Air Force OSI, and their designees. For the Army, the designees are listed in AR 381-10, *supra* note 55, para. 10-4b. These are the Deputy Chief of Staff for Army G-2, the Commander of the U.S. Army INSCOM, and the Commander of the U.S. Army Special Operations Command.

[242] *Id.* para. C10.3.1.3. *See also* AR 381-10 *supra* note 55, para. 10-2d (providing specific U.S. Army procedures for re-approval or extensions of periods of undisclosed participation).

[243] DOD 5240.1-R, *supra* note 45, para. C10.3.1.3.

[244] *Id*. para. C10.3.1.4. However, note that AR 381-10, *supra* note 55, does not address influence activities in Procedure 10. It does address it as a *part* of "Special Activities" that occur *outside* of the United States:

> Special activities [are activities] conducted in support of national foreign policy objectives abroad, planned and executed so that the role of the U.S. Government is not apparent or publicly acknowledged. These activities are not intended to influence United States political processes, public opinion, or media, and do not include diplomatic activities or the collection and production of intelligence.

See AR 381-10, *supra* note 55, Glossary, Section II, and paragraph 1-5g, which states, "MI elements are prohibited from conducting or providing support to special activities (see glossary) unless approved by the President and directed by the Secretary of Defense in time of congressionally declared war, or during a period covered by a presidential report/finding and as the Secretary of Defense directs." *See also* JP 3-13, *supra* note 49; U.S. DEP'T OF ARMY, FIELD MANUAL 3-13, INFORM AND INFLUENCE ACTIVITIES (25 Jan. 2013).

[245] DOD 5240.1-R, *supra* note 45, para. C10.3.1.4.

[246] *Id.*

[247] *Id*. para. C11.1.

[248] *Id*.

There are times when cover arrangements are critical to the effective performance of foreign intelligence and counterintelligence missions.[249] However, the government must limit its clandestine interaction with its own citizens to circumstances where there exists a compelling state interest.[250] The intelligence oversight programs discussed thus far are designed to ensure it goes no farther. Undisclosed contracting for goods and services is no different. Procedure 11 is straightforward in its approach: in general, it requires a clear statement of the compelling reason for surreptitious conduct, and provision a reasonable means for control of the conduct to minimize the potential chilling effect on personal freedom.[251]

When contracting with academic institutions, intelligence components may purchase goods or contract services only if they first advise appropriate school officials that they are, in fact, contracting with a DoD intelligence component.[252] This restriction does not apply to the enrollment of individual students.[253] So an intelligence component may enroll one of its members in school without telling the school what the student does or by whom she is employed; however, if the intelligence component wants to pay the school to conduct specialized research, the component must disclose its identity.

When intelligence components are not dealing with academic institutions, they may sometimes contract with private entities or individuals without revealing what they are. They may do so if they are contracting for published material available to the general public or routine goods and services needed for approved activities, such as credit cards, car rentals, travel, lodging, meals, and rent.[254] Intelligence components may also enter into contracts without revealing themselves if an appropriate senior official makes a written determination that the sponsorship of a DoD intelligence component must be concealed to protect that component's intelligence activities.[255]

The Department of the Army has imposed additional requirements on MI personnel seeking to participate in undisclosed contractual relationships. Specifically, MI personnel *shall*:

> a. Not enter into contracts with U.S. Government employees without the approval of the head of the contracting activity;
>
> b. Coordinate with the servicing legal advisor and the contracting office prior to acquiring intellectual property, patent, software, or data rights. MI employees will also comply with all applicable law and policy, including AR 25–2 and Defense Federal Acquisition Regulation Supplement (DFARS), subpart 227;
>
> c. Comply with the Joint Ethics Regulation, DoD 5500.7–R, and, when required, complete Office of Government Ethics (OGE) Form 450 (Executive Branch Confidential Financial Disclosure Report) and appropriate training;
>
> d. Comply with all pertinent fiscal law and policy. MI employees will not split purchases to avoid procurement or construction thresholds;
>
> e. Comply with major acquisition rules requiring legal review under the provisions of DoD Instruction (DoDI) 5000.2;
>
> f. Ensure that secure environment contracts or acquisitions that are protected under the purview of special access programs allow access to appropriately cleared auditor personnel, legal counsel, inspectors general, and intelligence oversight personnel in accordance with DoD Directive (DoDD) 5205.7;
>
> g. Ensure that statements of work do not outsource inherently governmental activities as defined by Federal Acquisition Regulation (FAR) part 7.5 and Office of Federal Procurement policy; and,
>
> h. Ensure that statements of work do not specify requirements for personal services, and that contracts are not

---

[249] DIA HANDBOOK, *supra* note 66, para. 7-2.

[250] *Id*. para. 7-2b. The "compelling interest" is that unless the Government protects its capacity to function and preserve the security of the nation, society could become so disordered that all rights and liberties would be endangered. *Id.* Or so the theory goes.

[251] *Id*. para. 7-2d.

[252] DOD 5240.1-R, *supra* note 45, para. C11.2.1.

[253] *Id.* para. C.11.1.

[254] *Id*. para. C11.2.2.1.

[255] *Id*. paragraph C11.2.2.2. The appropriate approving officials are the Secretaries and Under Secretaries of the military departments, the Director of the NSA, the Director of the DIA, and the Deputy Under Secretary of Defense (Policy). In accordance with AR 381-10 *supra* note 55, para. 11-2b(3), U.S. Army MI personnel must seek written sponsorship concealment determinations from the Secretary of the Army or Under Secretary of the Army that sponsorship must be concealed to protect an the integrity or security of an intelligence activity.

administered as personal services contracts (see FAR part 36.104).[256]

Because these requirements are so extensive, coordination between supporting legal offices and higher headquarters' legal advisors is highly encouraged.

PRACTICE TIP: Cloaked Contracting for Goods and Services

DoD intelligence components that need to contract for goods and services, without revealing the sponsorship of that component, may do so ***only*** under certain circumstances, unless a ***determination*** has been made ***in writing*** by a designated official that such sponsorship must be concealed to protect the activities of the DoD intelligence component concerned, IAW DoD 5240.1-R, Procedure 11. Remember, AR 381-10, Chapter 11, imposes additional requirements and restrictions.

Thus far, we have seen that the first eleven procedures in DoD 5240.I-R are concerned with information collection, dissemination, retention, and the various modus operandi which may be employed in those activities. The primary focus of those procedures is on the operational intelligence, counterintelligence, and security activities of DoD intelligence components. The focus of Procedures 12, 14, and 15 is broader and encompasses *all* personnel affiliated with DoD intelligence components. These procedures concern conduct in with which *all* intelligence personnel could become involved, and should be aware of.[257]

b. Cooperation with Law Enforcement: Procedure 12

Procedure 12 applies to DoD intelligence components assisting civilian law enforcement authorities. It incorporates specific limitations imposed by EO 12333[258] along with statutory and policy restrictions and approval requirements.[259] These provisions apply to DoD intelligence support to any federal, state, or local civilian law enforcement agency.[260] They are applicable not only during DSCA events, but also in this era of "wind-down," as military units return from Iraq and Afghanistan and must confront domestic challenges that they otherwise dealt with routinely and reactively in combat zones. In domestic settings, responses and reactions must be skillfully crafted to conform to current intelligence oversight restrictions imposed by law and policy.

Deriving from the passage of the Posse Comitatus Act of 1879[261] (which prohibited the use of the Army in law enforcement roles), Procedure 12 has undergone some significant evolution. Department of Defense Directive 5525.5 provided the baseline DoD policy to implement the Posse Comitatus Act. This directive has recently been incorporated and canceled by DoDI 3025.21, which is slightly more restrictive, and much more detailed about how and when DoD intelligence components can assist civilian law enforcement agencies. Due to recent events involving Army units allegedly improperly assisting civilian law enforcement officials, judge advocates are *strongly* urged to secure and carefully review DoDI 3025.21.[262]

Procedure 12 covers DOD intelligence components providing assistance to civilian law enforcement authorities. This Procedure serves as the DoD policy implementing the Posse Comitatus Act and the restrictions of EO 12,333 while also providing general guidance regarding *some* of the exceptions to the Act that currently exist.[263]

---

[256] AR 381-10 *supra* note 55, para. 11-3. This expanded "checklist" of requirements has been augmented over and above previous editions of the regulation.

[257] DIA HANDBOOK, *supra* note 66, para. 8-2b.

[258] EO 12,333, *supra* note 2, § 2.6, provides that agencies within the intelligence community are authorized to cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property and facilities of any agency within the intelligence community. Unless otherwise specifically precluded by law (including EO 12,333), such agencies may also participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorists or narcotics activities; provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency; or when lives are endangered, to support local law enforcement agencies. The provision of assistance by expert personnel must be approved in each case by the General Counsel of the providing agency. Agencies within the intelligence community may also give any other assistance and cooperation to law enforcement authorities not precluded by applicable law, such as the Posse Comitatus Act. *See also* DIA HANDBOOK, *supra* note 66, para. 8-3 & n.222.

[259] DIA HANDBOOK, *supra* note 66, para. 8-3. Procedure 12 was originally based on DODD 5525.5, *supra* note 47, which has been replaced by DODI 3025.21, *supra* note 45, which in turn implements the Posse Comitatus Act, 18 U.S.C. § 1385 (2011).

[260] DIA Handbook, *supra* note 66, para. 8-3.

[261] 18 U.S.C. § 1385.

[262] On 10 March 2009, active duty U.S. Army Military Police personnel were deployed from Fort Rucker, Alabama, to Samson, Alabama, in response to a murder spree, purportedly at the request of local law enforcement officials. City officials confirmed that the soldiers assisted in traffic control and in securing the crime scene. The problem was that the governor of Alabama had not requested military assistance under a Stafford Act or related request, and neither had President Obama authorized their deployment. The ensuing investigations disclosed that the Posse Comitatus Act had been violated. As a result, several administrative actions were taken affecting those personnel involved.

[263] DOD 5240.1-R, *supra* note 45, para. C12.1. Enclosure 3 to DODI 3025.21, *supra* note 45, implements the requirements of the Posse Comitatus Act, along with other restrictions. It generally forbids direct assistance to civilian law enforcement by military personnel (including personnel in intelligence components) for interdiction of vehicles, vessels, or aircraft; search and seizure; arrest and apprehension; surveillance, undercover work, or as investigators, or interrogators, evidence collection or the manning of traffic checkpoints, to name but a few. The new instruction provides a clear checklist of permissible direct assistance activities, along with discussions of permissible indirect assistance, such as provision of training and maintenance of equipment, consistent with 10 U.S.C. §§ 331–34, 371–82 (2012). Further, the Use of Information Collected During DoD Operations has been further clarified in Enclosure 7, along with the addition of Domestic Terrorist Incident Support in Enclosure 6.

Compliance with Procedure 12 is critical to the effective flow of information between the DoD Intelligence Community and civilian law enforcement.[264] Operating in concert with DoDI 3025.21 and the Posse Comitatus Act, Procedure 12 permits the DoD Intelligence Community to cooperate with civilian law enforcement authorities to investigate or prevent clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities;[265] to protect DoD employees, information, property, and facilities;[266] and to prevent, detect, or investigate other violations of law within the DoD's investigative jurisdiction.[267]

Pursuant to DoDI 3025.21, DoD Intelligence Components are encouraged to provide information (and intelligence) collected during military operations to federal, state, or local civilian law enforcement officials that may indicate a violation of state or federal law.[268] They are also urged to provide such information if it may be relevant to drug interdiction or other civilian law enforcement matters, unless sharing the information is determined to be inconsistent with national security by the head of that DoD component.[269] Similarly, the needs of civilian law enforcement should be considered when routine military training missions are being planned and executed.[270]

Defense intelligence components may provide specialized equipment and facilities to federal law enforcement authorities[271] and, when lives are endangered, to state and local law enforcement authorities, when approved as authorized by Enclosures 3 and 7 of DoDI 3025.21.[272] Similarly, DoD personnel may be assigned to assist federal law enforcement authorities and, when lives are endangered, state and local law enforcement authorities consistent with approvals required by Enclosures 3, 4, and 7 of DoDI 3025.21, and upon concurrence of the General Counsel's Office of the assisting DoD intelligence component.[273]

PRACTICE TIPS: Assisting Civilian Law Enforcement Agencies

- DoD may ***only*** provide indirect assistance to civilian law enforcement agencies, IAW DoDI 3025.21, and the Posse Comitatus Act, 18 U.S.C. §1385.
- DoDI 3025.21 does not apply to intelligence and counterintelligence components ***except*** when providing assistance to civilian law enforcement activities in accordance with paragraph 2.6. of EO 12,333 and Procedure 12 of DoD 5240.1-R.
- Procedure 12 permits incidentally acquired information reasonably believed to indicate violations of federal, state, local or foreign law to be provided to appropriate civilian law enforcement officials IAW §1.7(a) of EO 12,333 and AR 381-10, paragraph 12-3, and as consistent with DoDI 3025.21, Enclosure 7.
- Procedure 12 also permits specialized equipment and facilities to be provided to federal law enforcement authorities, and, when lives are endangered, to state and local law enforcement authorities, as long as the assistance is consistent with DoDI 3025.21, Enclosure 8, has been approved by an appropriate authority listed in paragraph 4 of that Enclosure.
- Finally, Procedure 12 permits DoD intelligence component personnel to be assigned to assist Federal law enforcement authorities, and, when lives are endangered, to state and local law enforcement authorities, consistent with the restrictions of DoDI 3025.21, Enclosures 3 and 4, and upon approval by SecDef, pursuant to DoDD 5240.01.
- In short, Procedure 12 and DoDI 3025.21 ***together***, should always be consulted ***prior*** to providing any DoD intelligence component assistance to civilian federal or state law enforcement agencies.

c. Human Experimentation—Procedure 13

The historically contentious issue of human experimentation is addressed in DoD 5240.1-R, Procedure 13. This procedure applies to experimentation on human subjects conducted by or on behalf of a DoD intelligence component. It does not cover experiments on animals.[274]

But what exactly constitutes "human experimentation"? Human experimentation is any research or testing activity involving human subjects in which the subjects are exposed to more than a minimal risk.[275] A "minimal risk" is a risk of permanent or temporary injury (including physical or psychological damage and damage to reputation) beyond the risks to which that person is ordinarily exposed in his daily life.[276]

[264] *See* DoDD 5240.01, *supra* note 62, para. 4.5.

[265] DOD 5240.1-R, *supra* note 45, para. C12.2.1.1.

[266] *Id*. para. C12.2.1.2.

[267] *Id*. para. C12.2.3. *Compare* AR 381-10 *supra* note 55, para. 12-2.

[268] DODI 3025.21, *supra* note 45, encl. 7, para. 1.

[269] *Id*. para. 1.g.

[270] *Id*. para. 1.e.

[271] DOD 5240.1-R, *supra* note 45, para. C12.2.2.3.

[272] *Id.*

[273] *Id.* para. C12.2.2.4. In general, to assign military personnel from the intelligence components to assist law enforcement is subject to approval by the SecDef. DODD 5525.5, *supra* note 47, para. E4.5.3.4.

[274] DOD 5240.1-R, *supra* note 45, para. C13.1.

[275] DIA HANDBOOK, *supra* note 66, para. 8-12a.

[276] *Id*.

Current DoD policy is concise and unambiguous: the DoD may *not* engage in or contract for experimentation on human subjects without approval of the SecDef, Deputy SecDef, or the secretary or under secretary of a military department.[277] Furthermore, any experimentation on human subjects conducted by or on behalf of a DoD may be undertaken only with the informed consent of the subject, in accordance with U.S. Department of Health and Human Services guidelines.[278]

d. Employee Conduct and Preventing Intelligence Community Misconduct—Procedure 14

Procedures 14 and 15 pertain to DoD employee misconduct and reporting requirements. Procedure 14 has two simple requirements:

> 1. That all members of the Intelligence Community shall conduct all intelligence activities IAW . . . [EO 12,333], and related Intelligence Program requirements; and,
>
> 2. That all Intelligence Community components ensure that their respective members are properly trained so that they are aware of the limits of the authority under which intelligence activities are conducted, as well as the procedures that apply to each of those activities, whether they involve collection of intelligence information, retention of intelligence information, control and dissemination of that information, or specific collection techniques.[279]

Procedure 14 requires each member of the DoD to ensure all of its employees are trained and familiar with the provisions of EO 12,333, DoDD 5240.1-R, applicable service regulations, and any other applicable intelligence oversight rules.[280] To ensure this, the components must conduct familiarization courses to include orientation and training on Procedures 1 through 4;[281] a summary of other procedures pertaining to whichever collection techniques may be used by the component concerned;[282] and the requirement that they report questionable activity under Procedure 15.[283]

The DIA Handbook identifies six core general principles which support the requirements of Procedure 14 and intelligence oversight. They consist of:

> 1. Unlawful conduct: Any proposal involving activities that may be unlawful or contrary to policy shall be referred to the servicing Inspector General and Staff Judge Advocate offices.
>
> 2. Adverse actions: Adverse action shall not be taken against any person who reports questionable activity pursuant to DoD 5240 .l-R, Procedure 15.
>
> 3. Sanctions: Sanctions shall be imposed on any civilian or military employee who violates intelligence directives or instructions based on those directives.
>
> 4. Breaches of security: Serious or continuing breaches of security shall be referred to the intelligence component Director, or Commanding general.
>
> 5. Access to information: Intelligence oversight officials shall have access to all information about intelligence activities necessary to carry out their oversight responsibilities. Special arrangements for such access may be required in the case of sources and methods.
>
> 6. Employee cooperation: Employees shall cooperate fully with the Intelligence Oversight Board and its representatives.[284]

[277] DOD 5240.1-R, *supra* note 45, para. C13.3.2.

[278] *Id*. para. C13.3.1.

[279] *Id*. paras. C14.2.1, C14.2.2; *see also* DIA HANDBOOK, *supra* note 66, para. 8-14.

[280] DOD 5240.1-R, *supra* note 45, para. C14.2.2.

[281] *Id*. para. C14.2.2.1.1.

[282] *Id*. para. C14.2.2.1.2.

[283] *Id*. para. C14.2.2.1.3.

[284] DIA HANDBOOK, *supra* note 66, tbl.8-1. The responsibility for maintaining these principles and punishing violations rests with the commanding officer of the unit concerned. AR 381-10 *supra* note 55, para. 14-3:

> Commanders will ensure—
> *a.* Personnel are protected from reprisal or retaliation because they report allegations in chapters 15 and 16. If personnel are threatened with such an act, or if an act of reprisal occurs, they will report these circumstances to the DoD Inspector General.
>
> *b.* Appropriate sanctions are imposed upon any employee who violates the provisions of this regulation or applicable USSIDs.
>
> *c.* The field IG; the DCS, G–2; TIG; the AGC; the DoD General Counsel; and ATSD–IO (or the representatives of those officials) who have the appropriate security clearances are provided access to

To avoid problems, the Army sets specific timeframes for training. Army's intelligence components must provide tailored unit training within thirty days of assignment or employment and periodic refresher training.[285]

> ***PRACTICE TIP*: Preventing Misconduct**
>
> The simple key to preventing Intelligence Component employee misconduct is training, of subordinate personnel and supervisors—
>
> - Tailored unit training within 30 days of arrival
> - Recurrent refresher training
> - Familiarization training of supervisors
> - Specialized training for all personnel working under Procedures 5-13

Procedure 14 is designed to ensure intelligence misconduct does not occur. However, when it does, Procedure 15 comes into play.

e. Dealing with Intelligence Community Misconduct: Procedure 15

Despite this system of safeguards, buttressed by extensive preparation and training, violations of the intelligence oversight rules still occur. Procedure 15 applies when they do. It requires the identification, investigation, and reporting of questionable intelligence activities.[286]

In this context, "questionable activity" means *any* conduct that constitutes, or is related to, an intelligence activity, and that may violate the law, any EO or presidential directive, or any applicable DoD policy or regulation.[287] Simply put, Procedure 15 specifically obligates every employee of the DoD to report *any* activity to responsible inspectors general (IGs) or to general counsel offices, including staff judge advocate (SJA) offices,[288] if that conduct may violate the DoD Intelligence Oversight program.[289] The IGs, along with the supporting legal offices, have the responsibility to determine whether such violations have occurred. If questionable intelligence activities occurred, but were not reported in advance, then they must also determine *why* the failure to report occurred.[290]

Army Regulation (AR) 381-10, Chapter 15, details extensively what constitutes "questionable activities," with examples grouped under four headings: improper collection, retention, or dissemination of USP information; misrepresentation; questionable intelligence activity constituting a crime; and misconduct in the performance of intelligence duties. It states what must be reported, and when, how, and by whom.[291] A commander may choose to conduct a AR 15–6 investigation or direct the issue to the appropriate IG. Depending on the investigative vehicle used, each report of questionable activity must be investigated to the extent necessary to determine the facts and to assess whether the activity was legal and consistent with applicable policy.[292] If the inquiry is not referred to a counterintelligence or criminal investigative agency, it must be completed within sixty days of the initial report, unless extraordinary circumstances necessitate an extension.[293] Either way, the results must be reported in a form consistent with paragraph 15-2 of AR 381-10.[294]

The following information is required for any report of investigation into questionable intelligence activity:

> 1. Identification of the personnel (but not by name unless requested by . . . [The Inspector General (TIG), U.S. Army], or . . . [Deputy Chief of Staff], G-2) or unit alleged to have committed the questionable intelligence activity by rank or civilian grade; their security clearance and access(es); unit of assignment, employment, attachment or detail; and their assigned duties at the time of the activity .
>
> 2. When and where the activity occurred;
>
> 3. A description of the activity and how it constitutes a questionable intelligence

> that information necessary to perform their oversight responsibilities, regardless of classification or compartmentation.
>
> *d.* Employees cooperate fully with the President's Intelligence Oversight Board and its representatives.
>
> *e.* All proposals for intelligence activities that may be unlawful, in whole or in part, or may be contrary to policy, will be referred to the AGC.

Id.

[285] AR 381-10, *supra* note 55, para. 14-1.*b*.

[286] DOD 5240.1-R, *supra* note 45, para. C15.1.

[287] *Id*. para. C15.2.1.

[288] By DoD policy, the term "Inspectors General" shall also include the Assistant to the Secretary of Defense for Intelligence Oversight. *Id*. para. C15.2.2.

[289] *Id*. para. C15.3.1.

[290] *Id*. para. C15.3.1.2.

[291] AR 381-10, *supra* note 55, para. 15-4.

[292] *Id*. para. 15-3.

[293] *Id*.

[294] *Id*. Note should also be made that AR 15-6 investigations do not alleviate or satisfy the initial five-day reporting requirement.

activity, citing to the applicable portion(s) of AR 381-10 and/or DoD 5240.1-R, and other applicable law or policy.

4. A discussion of command and/or investigative agency actions planned or ongoing, if applicable, to include whether the report was generated outside the affected command.

5. Status reports should be submitted to TIG every 30 days until the investigation is completed.[295]

The regulation also requires commanders to ensure that their personnel are protected from retaliation if they report questionable intelligence activities.[296] If commanders find that their personnel have been threatened with or subjected to retaliation, they (and the affected employees) must report this to the DoD IG.[297] Army Regulation 381-10 requires Army commanders to ensure that "appropriate sanctions are imposed" upon any employee who violates AR 381-10 or applicable U.S. Signals Intelligence Directives (USSIDs).[298]

General Counsel Offices and IGs involved in intelligence oversight investigations must report questionable activities of a serious nature *immediately* to the DoD General Counsel, and to the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)).[299] They must also make quarterly reports of suspected or reported violations (or the absence thereof), and actions taken with respect to these, through command headquarters, to the ATSD(IO).[300] These quarterly reports are also provided to unit commanding generals. For this reason, supporting SJA offices should not only be intrinsically involved in any investigations or inquiries into questionable intelligence activities, but should also be prepared to respond to Flag-level questions about the impact of the questionable intelligence activity, possible sanctions which may or should be imposed, and recommended courses of action to prevent recurrence.[301]

PRACTICE TIPS: Identifying and Reporting Questionable Intelligence Activities

"Questionable Intelligence Activity" (QIA) is *any* conduct related to an intelligence activity that may violate the law, any Executive Order or Presidential directive, including Executive Orders 12333 and 13470, or any applicable DoD or Army policy, including DoD 5240.1-R and AR 381-10.

A duty to "narc": "Each employee shall report any questionable activity to the General Counsel or Inspector General for the DoD intelligence component concerned, or to the General Counsel, DoD, or ATSD(IO)." (DoD 5240.1-R, Procedure 15, para. C15.3.1.1.).

How to report, and *what* gets reported:

Report any suspected QIA to the servicing IG or legal office; be sure to include:

- A description of the nature of the questionable intelligence activity
- Date, time, and location of occurrence
- Any information on the individual or unit responsible for or committing the questionable activity
- A factual summary of the incident to include names of other witnesses to the event, and, *if possible and feasible,* references to those portions of DoD 5240.1-R that were violated

Include also whether other reports of the incident were made, or if internal inquiries were conducted, and the status of those inquiries if known.

C. Additional Army Intelligence Oversight Program Considerations

Army Regulation 381-10 addresses two additional issues in Chapters 16 and 17. While only tangentially related to intelligence oversight, these are nonetheless quite important to Army members of the Intelligence Community.

Chapter 16 discusses the responsibilities for reporting federal crimes that may be committed by military intelligence personnel, and implements DoD Instruction 5240.04, *Counterintelligence Investigations*.[302] Crimes falling within the purview of Chapter 16 include espionage, sabotage, unauthorized disclosure of classified information, seditious conspiracy to overthrow the U.S. Government (USG), crimes involving foreign interference with the integrity of USG institutions or processes, crimes involving intentional infliction or threat of death or serious physical harm, unauthorized transfer of controlled technology to a foreign entity, and tampering with, or unauthorized access to, information systems.[303]

Chapter 17 covers MI support to force protection, multinational intelligence activities, joint intelligence

[295] *Id*. para. 15-2c.

[296] *Id*. para. 14-3*a*.

[297] *Id.*

[298] *Id*. para. 14-3.*b*.

[299] DoD 5240.1-R, *supra* note 45, para. C15.3.3.1.

[300] *Id*. para. C15.3.3.2.

[301] These suggestions are made based on the author's own experiences; it is a very bad day when a Judge Advocate or legal advisor is caught unaware and ill-prepared for questions such as these.

[302] AR 381-10, *supra* note 55, para. 16-1.

[303] *Id*. para. 16-3.

activities, and other DoD investigative activities. Military intelligence support to force protection is legally complex, especially in the domestic environment. While support of this nature includes identifying, collecting, reporting, analyzing and disseminating intelligence regarding foreign threats to the Army, consistent with obligations imposed upon commanders by AR 525–13, *Antiterrorism*, activities conducted within the United States are limited to collecting foreign intelligence and international terrorism threat data.[304] Only information acquired from federal, state, and local law enforcement agencies may be collected, analyzed, and disseminated. The rationale behind this is simple: these agencies have the primary responsibility for collecting information and criminal intelligence to protect domestically-assigned U.S. military forces.[305] Toward this end, the U.S. Army Criminal Investigative Command serves as the Army liaison to domestic civilian law enforcement agencies. Army counterintelligence personnel are the primary liaisons to these agencies for exchanging foreign threat information.[306]

D. Intelligence Oversight: Conclusions

The procedures described above are designed to protect the constitutional rights and privacy interests of USPs while allowing the DoD to provide state-of-the-art intelligence to our nation's key decision makers. A similar set of DoD and military service policies cover the other side of information collection, which in practice is referred to as "sensitive information." This program does not fall under intelligence oversight policies, and has its own rules.

IV. Sensitive Information—Intelligence Oversight's Fraternal Twin

"Sensitive information" (SI)[307] is a collective term pertaining to information on or about USPs *and others present in the United States* who are not affiliated with the DoD, and is collected or obtained by the DoD. Two types of SI exist, distinguished by who collects the information and why.

Law Enforcement Derived Information (LEDI), also formally known as known as criminal intelligence or "CRIMINT,"[308] is "law enforcement information derived from the analysis of information collected through investigations, forensics, crime scene and evidentiary processes to establish intent, history, capability, vulnerability, and modus operandi of threat and criminal elements."[309] If the information includes information on individuals or organizations within the United States who are not affiliated with the DoD (non-Defense affiliated persons, or "NDAPs"), then it falls within the ambit of DoDD 5200.27 or AR 380-13.[310]

The second form of information, Non–Defense Personnel Information (NDPI), is information about NDAPs that was not acquired for DoD law enforcement purposes, but was nonetheless developed during the performance of official DoD or military operations. Both kinds of information are subject to the restrictions of DoDD 5200.27 and its Army counterpart, AR 380-13.[311]

This kind of information is often collected during consequence management (CM) or disaster assistance events—in short, DSCA operations.[312] Collection of NDAP information during such domestic events must receive intense scrutiny to ensure compliance with DoDD 5200.27. The potential for inadvertently violating this directive and Americans' civil or privacy rights is significant. Judge advocates should be prepared to advise their commanders on appropriate domestic collection procedures and limitations to avoid this danger.

The true challenge arises in that, just as in the case of domestic intelligence collection activities, DoD collection of domestic *information* regarding NDAPs in the United States may seem inconsistent with if not counterintuitive to,

---

[304] *Id*. para. 17-1.

[305] *Id.*

[306] *Id*.

[307] "SI," or Sensitive Information, for purposes of this article, is that information falling within the ambit of DoDD 5200.27, *supra* note 79, whether it is law enforcement-based information or information held by non-DoD law enforcement personnel. "SI" is a term used in common practice throughout U.S. Army North. "LEDI," or Law Enforcement Derived Information, again for purposes of this article, applies to information acquired, stored or distributed by Department of Defense law enforcement and criminal investigation organizations. SI is comparable to intelligence oversight programs although intelligence and information developed by the DoD Intelligence Community is not involved in the SI program. *See id.* paras. 2.3, 6.5.

[308] U.S. DEP'T OF ARMY, REG. 525-13, ANTITERRORISM 56 (11 Sept. 2008) (glossary).

[309] *Id*. sec. II (Terms). *Compare* U.S. DEP'T OF ARMY, REG. 195-2, CRIMINAL INVESTIGATION ACTIVITIES (15 May 2009). Section II, Terms, which defines "criminal intelligence" as "[i]nformation compiled and analyzed in an effort to anticipate, prevent, or monitor possible or potential criminal activity or terrorist threats directed at or affecting the U.S. Army operations, material, activities personnel or installations."

[310] The Army counterpart is AR 380-13, *Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organization*. U.S. DEP'T OF ARMY, REG. 380-13, ACQUISITION AND STORAGE OF INFORMATION CONCERNING NON-AFFILIATED PERSONS AND ORGANIZATION (30 Sept. 1974) [hereinafter AR 380-13].

[311] Figure 1, at the end of this article, illustrates the different types of information and the agencies that provide it.

[312] *See* CHAIRMAN, JOINT CHIEFS OF STAFF, JOINT PUB. 3-28, CIVIL SUPPORT, at I-9 (14 Sept. 2007).

command responsibilities overseas. The difference that must be *constantly* borne in mind in the homeland is that persons residing, or who are present, in the United States enjoy freedoms and protections of privacy rights, conceivably absent elsewhere in the world, but nonetheless guaranteed by the laws of the United States.[313]

***PRACTICE TIP:* Sensitive Information Program Triggers-General Rule**

- When a person, business or organization is identified by name (or using personal identifying information), the SI program is triggered if the information collected or acquired *specifically identifies* persons not affiliated with the DoD
- The SI Program is NOT triggered if information is collected solely on *activities,* and/or non-DoD affiliated persons are neither identified nor identifiable

A. Protecting Civil and Privacy Rights

The Defense Department's policy expressly prohibits collecting, reporting, processing, or storing information on individuals or organizations that are not affiliated with the DoD except when such information is essential to the accomplishment of specific DoD missions.[314] The missions are outlined in DoDD 5200.27 and fall under the headings of protection of DoD functions and property, personnel security, and operations related to civil disturbances.[315]

The sensitive information rules apply any time any information is acquired on identified or identifiable NDAPs and their activities, whether inside the United States or anywhere else in the world. Any information collected or received on NDAPs falls within the ambit of DoDD 5200.27.[316] As a rule of thumb, DoD *may* collect on the activities of non-identified (or unidentifiable) NDAPs as necessary to carry out military missions; but, the moment the person or organization is identified, sensitive information programs are triggered.

PRACTICE TIP: SI is information,

- On ***identifiable or identified*** individuals or organizations who are <u>not</u> affiliated with the DoD;
- That is acquired by DoD elements or organizations that are <u>not part</u> of the Intelligence Community; and,
- Falls within the restrictions of DoDD 5200.27 and AR 380-13.

B. Who Must Comply with the Sensitive Information Rules?

At the outset, judge advocates must be aware that sensitive information rules do not apply to members of the DoD intelligence community; they have their own rules in the form of IO. The Defense Department Sensitive Information rules do apply to non-intelligence personnel in the Office of the Secretary of Defense, the Military Departments, the Defense Agencies, and to all subordinate

---

[313] In this author's experience, this is the *most* difficult challenge confronting commanders, judge advocates, and other military personnel returning from overseas assignments, and especially from Iraq and Afghanistan. It must be remembered that especially during a DSCA event when the military has been tasked to *assist* the affected population, the uncooperative and possibly boisterous or rowdy person who may be the target of a desired collection activity, may be your child's fourth grade teacher, who is tired, hungry, thirsty, and probably frustrated. Despite his or her verbally-combative demeanor, a very specific and protected right to privacy must be afforded to that teacher. He or she is *not* the enemy.

[314] DoDD 5200.27, *supra* note 79, para. 3.1.

[315] *Id.* paras. 4.1-4.3.

[316] *Id*. paras. 2.2.1., 2.2.2; *see also* AR 380-13, *supra* note 310, paras. 2*a* and 2*b.* The Army uses a different analytical process, which lays out who *is* considered affiliated with the DoD, vastly simplifying the process of determining who *is not* affiliated:

> Affiliation with Department of Defense.
> A person, group of persons, or organization is considered to be affiliated with the Department of Defense if the persons involved are—
>
> *a.* Employed by or contracting with the DoD or any activity under the jurisdiction of DoD, whether on a full-time, part-time, or consultative basis;
> *b.* Members of the Armed Forces on active duty, National Guard members, those in a reserve status or in a retired status;
>
> *c.* Residing on, having authorized official access to, or conducting or operating any business or other function at any DoD installation or facility;
>
> *d.* Having authorized access to defense information;
>
> *e.* Participating in other authorized DoD programs, including persons upon whom investigations have been initialed under AR 230-2 (Non-Appropriated Fund, and Related Activities, Personnel Policies and Procedures), AR 604-20 (Security Requirements for Personnel in Both Information and Education Activities), AR 690-1 (Civilian Applicant and Employee Security Program), and AR 930-5 (American National Red Cross Service Program and Army Utilization), DoD Regulation 5220.22-R (Industrial Security Regulation), DA Memorandum 28-1 (Acceptability of Prospective Participants in the Armed Forces Professional Entertainment Program and the Army Sports and Recreation Programs Overseas) and DA Memorandum 340-3 (Program for Unofficial Historical Research in Classified Army Records);
>
> *f.* Applying for or being considered for any status described in a through e above, including individuals such as applicants for military service, pre-inductees and prospective contractors.

See AR 380-13, *supra* note 310, app. A. Following the Army's analytical model, deductively, those persons *not* falling into the above categories are considered persons *not* affiliated with the DoD, and therefore should *not* be the subject of DoD information collection efforts except as provided by DoD policy.

uniformed service members and employees.[317] Also included are all non-intelligence members of the National Guard; the Chief of the National Guard Bureau has issued a policy memorandum mandating that both DoDD 5200.27 and AR 380-13 apply to Army National Guard personnel regardless of whether they are in Title 10 (federal active duty) or Title 32 (state active duty) status.[318]

C. The Three-Step Process for Analysis for Collecting on Persons not Affiliated with the DoD

The DoD policy generally prohibiting the acquisition of information on identified or identifiable NDAPs, while clearly restrictive, does permit limited collection activities. To collect on an NDAP, a three-step analysis must be followed before any collection activity begins. The first question is "Why is information needed on this specifically identified (or identifiable) NDAP?" In other words, will the mission fail if this information is not captured, or is this just "nice to know" information?[319] As we have seen, only information that is essential to accomplish assigned military missions may be collected on NDAPs.

The next question is, "Is there is a reasonable basis to believe (rather than merely a "hunch") that the information acquired shows a direct relationship between the NDAP or information collected on and an impact on DA or DoD?[320] In practice, this has become known as the "DoD nexus requirement". If there is not a valid and articulable nexus, then collection on an identified or identifiable NDAP is prohibited. When the nexus *does* exist, the final step in the analysis must still be conducted prior to collection.

The final question is, "Is the information sought or collected essential to accomplish a designated mission?" DoDD 5500.27 designates three core mission sets that allow the military to collect information on NDAPs: (1) the protection of DoD functions and property, (2) personnel security functions and investigations, and (3) operations related to civil disturbances.[321] These three missions constitute, essentially, the only exceptions to the overarching DoD policy against collecting information on NDAPs. For this reason, the acquisition of information *must* be limited to that which is essential to accomplish one of these core DoD missions.[322] Will one of these missions fail if the DoD does not collecting the information? If not, collecting information on *activities* rather than on *identified persons or organizations* is a far better course of action.

PRACTICE TIPS: Sensitive Information Basic Program Rules

- POLICY: DoD components may *only* acquire information on identifiable persons who are affiliated with the DoD
- THE EXCEPTION: Information *may be acquired* on persons *not affiliated with the DoD* if it is essential to the accomplishment of DoD missions
- ONLY THREE (3) missions fall under the exception:
  - Protecting DoD Functions and Property
  - Conducting Personnel Security investigations and inquiries
  - Supporting Civil Disturbance Operations

1. Protection of DoD Functions and Property

Pursuant to DoDD 5200.27, information may be acquired about activities of identified NDAPs who are threatening, or have threatened, military and civilian DoD personnel and defense activities and installations including vessels, aircraft, communications equipment, and supplies.[323] Only the following enumerated activities can justify the acquisition of such information for that purpose: subversion of DoD personnel through active encouragement of violations of law, disobedience of lawful order or regulation, or disruption of military activities; [324] thefts of arms, ammunition, or equipment; destruction or sabotage of DoD facilities, equipment, or records;[325] acts jeopardizing the security of

[317] DoDD 5200.27, *supra* note 79, para. 2.1.

[318] Memorandum from The Chief of the National Guard Bureau, subject: NGB Policy for Handling of U.S. Person Information (18 June 2008).

[319] During post-natural disaster DSCA operations, when Title 10 forces are deployed and then employed within the affected areas of the AO. Commanders may request (or staff members think this information will be requested) information regarding criminal or "problematic" *elements* present in the employment locations. These "elements" have in practice been defined as gangs, gang members, known felons, or persons known to harbor *general* ill-will or have conveyed criticism of the U.S. Government or DoD in the past. While such knowledge of the identities of such persons may be of tremendous value in combat zones, it has very little relevance domestically, especially in the absence of any of these persons or groups conveying (or carrying out) specific and direct threats against DoD personnel. In a situation in which the DoD is merely a *supporting* resource, without authority to apprehend, , absent Presidential direction to the contrary, or to otherwise impose will or force upon such persons, collection of information on them is absolutely inappropriate. To do otherwise, would not only violate DoDD 5200.27, but could conceivably run afoul of the Posse Comitatus Act and DoDI 3025.21, *supra* note 45, if requested by civilian law enforcement authorities. For this reason, commanders, staffs, or other military personnel have no need for the identities of these "elements", but instead should be more concerned with the *activities* of such persons that may negatively impact military support operations. Further, as consistent with the CJCS Standing DSCA EXORD, collection activity like this is expressly prohibited.

[320] AR 380-13, *supra* note 310, para. 6.

[321] DoDD 5200.27, *supra* note 79, para. 4.

[322] *Id.* para. 5.1.

[323] *Id.* para 4.1.

[324] *Id*. para. 4.1.1.

[325] *Id*. para. 4.1.2.

DoD elements or operations or compromising classified defense information;[326] unauthorized demonstrations on DoD installations;[327] direct threats to DoD personnel in connection with their official duties; direct threats to other persons who have been authorized protection by DoD resources;[328] activities endangering facilities that have classified defense contracts or that have been officially designated as key defense facilities;[329] and crimes the DoD is responsible for investigating or prosecuting.[330]

PRACTICE TIP: Protecting DoD Functions and Property—Summary

Information on identified or identifiable NDAPs *may be acquired* when there is a *reasonable belief* that one or more of the following have occurred, and the person identified was probably involved:

- Theft, destruction or sabotage of DoD material, facilities or records
- Acts jeopardizing security
- Subversion of loyalty, discipline or morale of DoD personnel
- Unauthorized demonstrations on or adjacent to DoD facilities
- Direct threats to DoD military or civilian personnel
- Activities or demonstrations endangering classified defense contract facilities or key defense facilities
- Crimes for which DoD has responsibility for investigating or prosecuting

2. Personnel Investigations

The second core mission for which information may be collected on NDAPs is the conduct of personnel investigations.[331] Just about everyone in the DoD has a background check of some sort. All of us have had to answer extensive questions about our families, places we have lived, job histories, and contacts with foreign nationals. Our answers were verified and supplemented through background investigations. These investigations are conducted on three categories of personnel: members of the Armed Forces, including applicants, reservists, and retirees;[332] DoD civilians and applicants;[333] and persons needing access to information protected under the DoD Industrial Security Program or being considered for participation in other authorized DoD programs.[334] They can be as simple as employment background checks or as complex and lengthy as Single Scope Investigations for clearances and special accesses.

Information on NDAPs may be highly germane when such persons are identified as witnesses or otherwise necessary for an investigation. For example, when your next-door neighbor is questioned during your background check, his or her identifying information and comments are captured as part of the investigation. Although your neighbor may have no affiliation with the DoD, his or her information forms part of the basis of the report submitted to support (or deny) your clearance upgrade or for another job. Collection of identifying information on such an NDAP is acceptable as long as the information acquired is limited to the scope of the investigation.

PRACTICE TIP: Personnel Security Investigations

During the course of Personnel Security Investigations on DoD personnel, information on, or identifying, persons not affiliated with the DoD may be acquired, *but only* as it relates to:

- Members of the Armed Forces, including retired personnel, members of the Reserve components, and applicants for commission or enlistment
- DoD civilian personnel and applicants
- Persons having a need for access to official classified or national defense information

3. Civil Disturbances

The third and final exception permits (careful) collection on the activities of NDAPs when the DoD provides support during civil disturbances. The directive permits collection under very limited circumstances. It states:

> 4.3. Operations Related to Civil Disturbance. The Attorney General is the chief civilian officer in charge of coordinating all Federal Government activities relating to civil disturbances. *Upon specific prior authorization of the Secretary of Defense or his designee,* information may be acquired that is essential to meet operational requirements flowing from the mission assigned to the Department of Defense to assist civil authorities in dealing with civil disturbances. Such authorization will only be granted when there is a distinct threat of a civil disturbance exceeding the law

[326] *Id*. para. 4.1.3.

[327] *Id*. para. 4.1.4.

[328] *Id*. para. 4.1.5.

[329] *Id*. para. 4.1.6.

[330] *Id*. para. 4.1.7.

[331] *Id.* para. 4.2.

[332] *Id*. para. 4.2.1.

[333] *Id*. para. 4.2.2.

[334] *Id*. para. 4.2.3.

> enforcement capabilities of [s]tate and local authorities.[335]

While such a scenario involving Title 10 military personnel is relatively rare,[336] they may be called upon to assist local civilian law enforcement during civil disturbance operations (CDOs). This will only occur when there is a distinct threat that the extent of the civil disturbance will exceed the capabilities of local and state law enforcement resources; the State Governor has requested assistance through the U.S. Attorney General; and, the President has directed the SecDef to provide DoD assets and active duty personnel for the limited purposes he outlines to assist civilian authorities in quelling the disturbance.[337] If, during the course of CDO support, active duty forces acquire information regarding NDAPs involved in the civil disturbance or other illegal activities, it may only be provided to state and local civilian law enforcement officials pursuant to DoDI 3025.21, Enclosures 4 and 7.[338]

The DoD's SI policy also permits the development of "contact lists" of civilian governmental and related personnel who are involved with the control of civil disturbances.[339] Only current names, phone numbers and official positions of NDAPs should be captured and maintained for this purpose.

---

[335] *Id*. para. 4.3 (emphasis added). Army Regulation 380-13, *supra* note 310, provides additional restrictions beyond this Directive:

> **7. Operations related to civil disturbances.**
>
> *a. General*
> … Military forces may be used to restore law and order when the president has determined in accordance with Chapter 15, Title 10, United States Code that the situation is beyond the capability of civilian agencies to control effectively.
>
> *b. Reports on deployment of National Guard under state control and police units in the event of actual civil disturbance.* Active Army commanders may report that National Guard units under state Control and police units are currently employed as a control force to deal with actual civil disturbances occurring within their geographical area of responsibility. Such reports will not contain information identifying individuals and organizations not affiliated with the Department of Defense and will only be based upon information acquired overtly from local, state, Federal officials or from the news media.
>
> *c. Limitations:* Except as authorized in paragraphs d and e below, Army resources may only acquire, report, process or store civil disturbance information concerning nonaffiliated persons and organizations upon receipt of ***specific prior authorization from the Secretary or the Under Secretary of the Army.*** Such authorization will only be granted when there is a distinct threat of a civil disturbance exceeding the law enforcement capability of state and local authorities. The authorization issued by the Secretary or the Under Secretary will set forth the procedures and the limitations on the acquisition, reporting, processing and storing of civil disturbance information.

Id. para. 7 (emphasis added).

[336] In accordance with DoDI 3025.21, *supra* note 45, para. 4, National Guard (NG) forces in state active duty (Title 32) status are the first in line to provide support during civil disturbance operations (CDO):

> a. NG forces in a State active duty status have primary responsibility to support State and local Government agencies for disaster responses and in domestic emergencies, including in response to civil disturbances; such activities would be directed by, and under the command and control of, the Governor, in accordance with State or territorial law and in accordance with Federal law.
>
> b. NG forces may be ordered or called into Federal service to ensure unified command and control of all Federal military forces for CDO when the President determines that action to be necessary in extreme circumstances.
>
> c. Federal military forces shall conduct CDO in support of the AG or designee (unless otherwise directed by the President) to assist State law enforcement authorities. Federal military forces will always remain under the command and control of the President and Secretary of Defense. Federal military forces also could conduct CDO in concert with State NG forces under the command of a dual-status commander, if determined to be appropriate by the Secretary of Defense and the Governor(s) concerned, or in close coordination with State NG forces using direct liaison.

[337] *Id*. encl. 4 para.1; DoDD 5200.27, *supra* note 79, para. 4.3.

[338] DoDI 3025.21, *supra* note 45, encl. 4 para. 4 & encl. 7, para. 1. In most instances where the DoD is called upon to quell civil disturbances, it is probable that the military is operating under Presidential or similar emergency authority as an exception to the Posse Comitatus Act, 18 U.S.C. 1385 (2011). Possible examples would be invocation of the President's authority under Articles II and IV of the Constitution; the issuance of a National Emergency Declaration, 50 U.S.C. §§ 1601–1651 (2011); Presidential activation of the Insurrection Statutes (formerly the Enforcement of the Laws to Restore Public Order Act), 10 U.S.C. §§ 331–34 (2012), 10 U.S.C. § 12406; 50 U.S.C. §§ 205–26; DoDI 3025.21, *supra* note 45; and a Declaration of Martial Law, as described in 32 C.F.R. §§ 501.1 to 501.7 (2013). These sections have been removed from the Code of Federal Regulations as of 30 April 2008. This Part will probably reappear somewhere in 32 C.F.R. §§ 350–399 at some future date. Nevertheless, the President can rely on his martial law authority to restore law and order. Although not specifically mentioned in the Constitution or any Federal law, the "Laws be faithfully executed" clause in Section 3 of Article II of the Constitution is recognized as the basis for the President's martial law authority. The Supreme Court in *Ex parte* Milligan, 71 U.S. 2, 127 (1866) stated that martial law is permissible in territories "where war really prevails," where it is necessary to furnish a substitute for civil government and the only authority left is the military. However, martial law can *never* properly exist where and when the civilian courts *are open and capable* of exercising their law enforcement jurisdiction. *Id.*

[339] DoDD 5200.27, *supra* note 79, para. 6.2.1.

PRACTICE TIP: The 3-step checklist for acquiring information on NDAPs during CDO support activities

During a CDO support activity, you *can* acquire information on persons not affiliated with the DoD if:

- That information is essential to performing a DoD mission to assist civil authorities during a Civil Disturbance; ***and***,
- SecDef (or his designee) has specifically authorized the information acquisition; ***and***,
- There is a distinct threat that the civil disturbance will exceed the law enforcement capabilities of State and local authorities

D. Infrastructure Information

Information on public and private infrastructure may be collected to accomplish any of the three excepted mission sets discussed above. However, this information must be limited to physical data on vital public or private installations, facilities, highways, and utilities, as necessary to perform the assigned mission.[340] For example, Information may be acquired on physical data relating to vital public or private installations, facilities, highways, and utilities necessary to carry out an assigned DoD mission. Therefore if you can demonstrate that the need exists, you may name a store to provide a geographic reference point or map coordinate; name a hospital, indicate medical capabilities or specialties provided by it, or the number of beds available; or, you may identify schools, auditoriums, or other large structures for possible use as public staging areas or pick-up locations for transport.[341] This information should be limited to *only* that information which can provide map coordinates and the capabilities or weaknesses of the infrastructure. In short, a stick pin on a map and an overview of the structure or system. No further information may be acquired or retained.

E. Prohibitions

Due to the sensitivities involved in acquiring information about the activities of NDAPs, DoDD 5200.7 sets forth seven key prohibitions on DoD collection activities that fall within the ambit of Sensitive Information.

First, no information may be acquired on NDAPs except for that specific information which is essential to accomplish the three DoD missions noted above.[342] Second, DoD personnel may not acquire information about an NDAP solely because that person lawfully advocates measures in opposition to Government policy.[343] Third, DoD personnel are also prohibited from conducting any form of physical or electronic surveillance of federal, state, or local officials or of candidates for such offices.[344]

Fourth, DoD personnel may not conduct any form of electronic surveillance of any individual or organization, except as authorized by law.[345] Fifth, they are expressly prohibited from conducting covert or deceptive surveillance or penetration of civilian organizations unless specifically authorized by the SecDef or his designee.[346] Sixth, DoD personnel may not be assigned to attend public or private meetings, demonstrations, or similar activities to acquire information about NDAPs, *even if* collecting such information is otherwise allowed under DoDD 5200.27, without specific prior approval by the SecDef, or the Secretary or the Under Secretary of the Army.[347]

Finally, DoD personnel are prohibited from developing or maintaining computerized databases about individuals or organizations not affiliated with the DoD, unless authorized by the SecDef or the Secretary or the Under Secretary of the Army.[348]

PRACTICE TIP: Historical Problem Areas—Don't Let History Repeat Itself!

- **FIRST AMENDMENT:** Don't acquire information about a person or organization just because they are protesting Government policy, or support racial or civil rights interests [*See Snyder v. Phelps*, No. 09-751 Slip Op., (U.S. S.Ct. 2 Mar 2011)]
- **SURVEILLANCE:** Don't covertly or deceptively surveil civilian organizations *unless you have specific authorization from* the Secretary or the Under Secretary of the Army
- **INFILTRATION:** Don't assign Army military or civilian personnel to attend an organization's public or private meetings, demonstrations, or other similar activities held off-post, *without approval* by the Secretary or the Under Secretary of the Army

[340] *Id*. para. 6.2.2.

[341] *Id.*

[342] *Id.*. para. 5.1.

[343] *Id*. para. 5.2. Note that this prohibition is clearly designed to ensure protection of First Amendment rights of free speech and expression of thought, and avoid the issues that arose during the 1960s and 1970s. *See supra* notes 15–17 and accompanying text.

[344] *Id*. para. 5.3.

[345] *Id*. para. 5.4.

[346] *Id*. para. 5.5. *Compare* DoD 5240.1-R, *supra* note 45, Procedure 10.

[347] *Id*. para. 5.6. A local commander may authorize an exception to this policy if, in his judgment, "the threat is direct and immediate and time precludes obtaining prior approval," in which case the action taken must be reported to the SecDef or his designee. *See also* AR 380-13, *supra* note 310, para. 9.

[348] DoDD 5200.27, *supra* note 79, para. 5.7. *See also* AR 380-13, *supra* note 307, para. 9.

These prohibitions are clear, unequivocal, and buttressed by analogous Army restrictions imposed by AR 380-13.[349] However, as with intelligence oversight provisions, the key to understanding the SI rules lies in whether information will be captured on an *identified* or *identifiable* non-affiliated person. If acquisition and *authorized* retention of the information is necessary to fulfill a DoD mission, retention may be permissible, with some additional hurdles yet to be cleared. As long as the acquisition is consistent with DoD mission parameters, and if the individuals or organizations are not identified or identifiable, or are characterized by codes[350] without further identifying data (such as addresses, locations, or digital images that can be retrievable from a database), then no Constitutional or privacy rights have been violated, and the objectives of the directive and regulation have been fulfilled.

Two examples may help to illustrate these issues. During many DSCA events, efforts are made to provide situational awareness for command elements operating in the disaster areas. Requests are frequently made for full motion video (FMV) capabilities to capture the flow, volume and apparent physical state of the affected populations. This requested information may help decision makers determine the *type* and *extent* of assistance is needed at any given time, by permitting fine-tuning of the DoD effort. A problem arises when the NDAPs whose digital images will be captured, processed and stored in a DoD database have not given the DoD permission to do this. This arguably violates the SI restrictions, not to mention Privacy Act prohibitions. This is because there is neither a solid DoD nexus between the *capture* of an NDAP's digital image, the image *itself* and an impact on DoD missions, personnel or resources. Since this would not fall under one of the three core missions listed above, none of the listed exceptions applies. However, in those circumstances where the image's information is essential to providing DSCA assistance, current technology allows the images to be blurred so as to render each person's image unrecognizable. In this way, the command still gets its situational awareness, but because the NDAPs are not identifiable, the SI rules are not violated.[351]

Another technique may involve researching, compiling and possibly even disseminating generalized reports regarding domestic criminal activities, threats and related issues that could directly affect Army operations throughout the U.S. This practice may at first appear to violate the SI rules, but it does not, since the collection would be focused on *activities* rather than *identifies* of NDAPs. Careful redaction (with the assistance of the supporting SJA office) of *any* NDAP personally identifying information (PII) would ensure such reports emphasize *activities*, since NDAP *identities* would be redacted. In this way, if such a compilation were developed, it could relay activity trends and *modus operandi* that may be of interest throughout the Army force protection community. Any discussions of NDAPs need *not identify* persons or organizations; instead, a code (e.g., SUBJECT 1, SUBJECT 2, or "Identified Person") could be used when referring to the person or organization in question. Reference to an original report number assigned by the originating agency could then be provided in the event further information was needed for investigative purposes. To avoid violating DoDD 5200.27, paragraph 6.3, which states, "Access to information obtained under the provisions of this Directive shall be restricted to Governmental Agencies that require such information in the execution of their duties," any documents of this nature would not be generally releaseable to the public. By carefully following these restrictions, these analytical products could still provide report recipients[352] with critical information about *activities*, and other information needed to enhance awareness, without triggering the SI prohibitions.

To avoid an overbroad reading of these prohibitions, DoDD 5200.27 offers some "Operational Guidance" about permissible collection. The directive does not prohibit reporting crimes and threats to law enforcement.[353] It does not prohibit overtly collecting current listings of federal, state, and local officials whose official responsibilities relate to the control of civil disturbances; or physical data on vital public or private installations, facilities, highways, and utilities, as appropriate, to carry out a DoD mission.[354] And, as we have seen, the directive allows the release of official information to governmental agencies requiring it to execute their duties.[355]

[349] DoDD 5200.27, *supra* note 79, para. 9.

[350] Such as NDP1 (non-DoD affiliated person #1) or NDO 2 (non-DoD affiliated organization #2).

[351] This practice is *arguably* permissible as long as the image or digital likeness cannot be "un-blurred"; however, if the clarity of the image can be restored, then this technique would not be acceptable.

[352] Recipients of these reports should be carefully screened and vetted to ensure compliance with DoDD 5200.27, *supra* note 81, para. 6.3.

[353] DoDD 5200.27, *supra* note 79, para. 6.1 permits "the prompt reporting to law enforcement agencies of any information indicating the existence of a threat to life or property, or the violation of law, nor to prohibit keeping a record of such a report. . . ."

[354] *Id*. para. 6.2. Note should be made regarding the DoD's collection of information pertaining to local officials; this practice is *only* permissible by directive within the context of civil disturbance operations. Whether this collection practice is permissible within military civil support and consequence management parameters not involving civil disturbances remains an open question. A strict reading of paragraph 6.2.1. would indicate that it is not permissible. However, the circumstances of emergencies may dictate the propriety of access to information already collected under this paragraph, regardless of the initial purpose for collection.

[355] *Id*. para. 6.3.

F. Information Retention under DoDD 5200.27

The directive is quite clear about how long information on NDAPs may be retained. The maximum period for any information acquired pursuant to DoDD 5200.27 is ninety days, unless longer retention is required by law or is specifically authorized under criteria established by SecDef or the Secretary of the Army (such as for on-going criminal investigations or military criminal proceedings).[356] Otherwise, the information must be destroyed.[357] When individual service regulations differ in their prescribed retention periods, a legal assessment should be made as to whether a variance has been authorized by the Secretary of Defense by or through his designee, such as a Service Secretary.[358]

PRACTICE TIP: Time Elements

Information acquired on persons not affiliated with the DoD may only be retained for ***90 days***, ***unless***

- Its retention is otherwise required by law…

  OR

- Its retention is specifically authorized by SecDef or SECARMY

V. Pulling It All Together

The above discussion conveyed the history, basics, and doctrine inherent in the DoD's IO and SI programs. These two programs represent the DoD's effort to respect Constitutional and privacy rights while performing its mission of national defense and security. The two programs, although similar, operate independently of each other, and affect different DoD personnel and missions.

Illustration 1, below, captures the relationships between the information components that form the basis of the IO Program and SI rules:

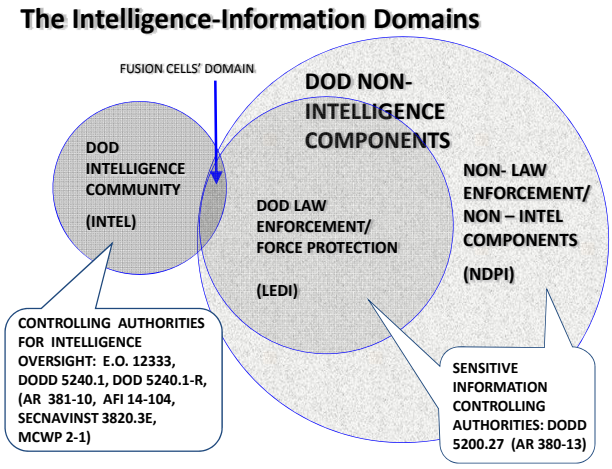

Illustration 1. Information and Function Domains

Each circle represents an Information and Function Domain, consistent with the distinct DoD missions performed. The smaller circle to the left represents information that is destined for use in the Intelligence Cycle by the DoD.[359] The DoD principally seeks information regarding foreign intelligence or counterintelligence. This domain is controlled by the IO authorities indicated.

The second and third overlapping circles on the right of the diagram represent military personnel using "all other information" for non-intelligence purposes. This also includes law enforcement-derived information[360] used for law enforcement purposes. Sensitive information rules apply to this latter domain.

As shown, all these domains overlap to some extent. Fusion Cells operate at the conjunction, pulling in information to create fused or combined threat products. Their core function is to combine available information from responsible agencies and share it so as to avert future terrorist and other force protection situations arising on military installations.[361]

[356] *Id.* para. 6.4. *See also* paragraph 6.5: "This Directive does not abrogate any provision of the Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation, April 5, 1979, nor preclude the collection of information required by Federal statute or Executive Order." *See infra* note 529.

[357] *Id.*

[358] Army Regulation 380-13 establishes a retention and destruction schedule based on the *type* of information acquired, and the *uses* for that information, ranging from 60 days to one year or more. Presumably, the Secretary of the Army was a designee of the SecDef authorized to establish the retention and destruction schedule for the information acquired on non-DoD affiliated personnel. *See* AR 380-13, *supra* note 310, para. 8.*b*.

[359] Also known as the "Intelligence Process," it consists of planning, preparing, collecting, processing, and producing, coupled with the three common tasks of analyzing, disseminating, and assessing. *See*, U.S. DEP'T OF ARMY, FIELD MANUAL 2.0, INTELLIGENCE ch. 4 (May 2004).

[360] *See supra* notes 302–04 and accompanying text.

[361] *See* Homeland Security Information Sharing Act, 6 U.S.C. § 481(c) (2012). As their name implies, Fusion Cells (or Fusion Centers) combine intelligence from all the sources shown in the diagram. In the Homeland, they may consist of inter-agency members coming from federal, state, and local agencies, or may consist solely of DoD personnel, depending on the assigned mission. Fusion Cells may consolidate all-source information *and* intelligence into a single readable product which addresses foreign intelligence and counterintelligence aspects of the data. To ensure compliance with both intelligence oversight and sensitive information programs, fused products use "tear-lines" to separate the portions that apply to force protection and antiterrorism. The information can then be shared with whichever DoD components need it *and* are authorized to receive it. *See also* MICHAEL GERMAN & JAY STANLEY, WHAT'S WRONG WITH FUSION CENTERS?, sec. III, Military Participation (unpaginated) (American

VI. Program Violations

Despite training requirements imposed to support both programs, and the sensitive nature of all policies involved, violations may still occur. Depending on the severity and nature of the violations, command judge advocates should coordinate all such actions with higher headquarters legal offices, local IG offices, Department of the Army-IG and even the Office of The Judge Advocate General (if necessary) prior to advising commanders on possible consequences. Some misconduct that violates the rights of a USP or NDAP may also violate the Uniform Code of Military Justice (as a violation of a lawful regulation or as dereliction of duty) while not implicating a federal statute. Such misconduct may be accidental or otherwise innocently undertaken, and for that reason should remain within the commander's discretion as to whether a counseling, reprimand or Article 15 is appropriate.

More serious violations may result from intentional collection activities, misuse of one's official position or of government resources and equipment, or intentional or wanton disregard of program restrictions.[362] Some of these activities may violate civilian criminal statutes[363] and can result in federal civil and criminal liability for Department of Army employees or Soldiers, *individually*, and for the Army as well.[364] Prompting a test case in this regard is *not* recommended.

PRACTICE TIPS: IO and SI—Side by Side

Intelligence Oversight	**Sensitive Information**
IO rules ***do not apply*** to LE and non-intel personnel There are only two lawfully assigned DoD IC missions: foreign intelligence and counterintelligence DoD IC mission is directed at *foreign* threats to national security; domestic threats are the responsibility of the FBI and CLEAs	SI restrictions ***do not apply*** to the DoD IC; they ***do apply*** to everyone else in the DoD – LE, AT/FP included Follow the two step analysis: Is there a DoD ***nexus***? If so, then is there an applicable ***exception***? protecting DoD functions & property; personnel security investigations; or, support to civil disturbance operations

- REMEMBER: ***neither*** program is triggered if no USPs or Non-DoD Affiliated Personnel are identified or identifiable
- It is *permissible* to collect and report solely on *activities* of persons or organizations as long as they are not identified or identifiable

VI. Summary and Conclusions

This article has but scratched the surface of intelligence oversight and sensitive information processes and authorities. The two programs are separate and independent, although in the current combat-wind down era, the lines between the two are becoming blurred. Which program applies depends on the user, his or her mission, the type of information or intelligence being used, whether USPs or NDAPs are identified, and what will be done with the information.

A few checklists may be of assistance when trying to determine program and process applicability. For intelligence oversight issues, consider the following:

1. Is there an authorized mission to perform intelligence function in question?

2. Is there a United States person involved? Was a United States person identified?

3. Is identification of the United States person absolutely necessary or will a description of the threat or activity suffice?

4. Was the intelligence in question "collected" in the meaning of directive?

5. Was the intelligence retained? For how long, and for what purpose?

Civil Liberties Union Pamphlet, Dec 2007), for a general discussion of concerns regarding Fusion Centers.

[362] Because *none* of these authorities are considered punitive, or have punitive provisions, prosecution under Article 92 of the UCMJ cannot occur. Although rarely punished as such, at least for enlisted personnel this conduct arguably violates Article 134, UCMJ (the general article), depending on the egregiousness of the violation. A recommendation, therefore, to the drafters of the new DoD 5240.1-M would be to include a punitive provision, thereby enabling prosecution for serious violations.

[363] For example, the Federal Wiretap Statute, 18 U.S.C. §2511, prohibits illegal interception, disclosure, or use of phone calls and related electronic communication, the punishment for which is up to five years' confinement in a federal penal institution.

[364] In a worst-case joint and several liability scenario, depending on the extent of the violations perpetrated, strong arguments supporting a Civil Rights violation lawsuit under 42 U.S.C. §1983 (or possibly under a *Bivens* theory, pursuant to Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics, 403 U.S. 388, 395-97 (1971)) could be presented. Qualified immunity arguments on behalf of the Army under a sovereignty immunity defensive theory would be quite interesting, if not challenging depending on the facts of the case.

6. Was the information disseminated, and to whom?

7. Was the dissemination authorized?

8. Have special collection procedures been involved? Have appropriate authorizations been granted?

9. Have any special collection procedures been violated?

10. If "yes" to any of these, has DoD 5240.1-R, Procedure 15 been implicated?

11. Has the servicing military Inspector General been informed? Have the violations been reported and reports initiated to senior officials?

A similar question set may be used for assessing sensitive information issues:

1. What function or mission was being performed requiring the acquisition of the information in question? Under what authority?

2. Was a non-DoD affiliated person or organization involved? Was information acquired, processed, stored or released on this non-DoD affiliated person or organization?

3. Was there an articulable nexus or direct relationship between the person or organization collected on and an impact upon the DoD?

4. Was this acquisition, processing, storing or release of information necessary to the fulfillment of a DoD mission as specified consistent with the excepted missions detailed in DoDD 5200.27?

5. Did the information acquired on this non-DoD affiliated person or organization identify the person or organization? Is this identification necessary to the fulfillment of a DoD mission?

6. Will a description of activity instead suffice to fulfill DoD mission requirements?

7. Was any of this information stored in a DoD computer database?

8. Were any of the prohibitions upon DoD activities under DoDD 5200.27 implicated? If so, how?

9. Did any of the information involve DoD functions and missions, personnel or property? If so, was there an indication of a direct threat to any of these?

10. Or, was there an indication of theft, destruction or sabotage; compromise of classified information; subversion of loyalty, discipline or morale; the potential for demonstrations on or adjacent to a DoD installation; or activities potentially dangerous to classified DoD facilities?

11. Did any of the information involve DoD personnel security investigations? If so, what was the nexus or direct relationship between the person or organization collected on and DoD interests?

12. Did any of the information acquired on the non-DoD affiliated person involve operations related to civil disturbances? If so, was there a nexus or direct relationship between the person or organization collected on and DoD interests or missions?

13. If information on an identifiable or identified non-DoD affiliated person was acquired, how long has the information been stored?

14. Was it destroyed at the 90 day point? If not, was there specific authorization to retain it longer?

15. Was the information disseminated? Was the release specifically authorized?

The practitioner will quickly discover that any checklist he or she uses is merely a *starting point* for analysis, and that although similar issues may arise over time, no two fact patterns are identical. For this reason, judge advocates must very carefully evaluate all issues arising under either intelligence oversight or sensitive information rules.

The current DoD intelligence oversight and sensitive information programs restrict the gathering of information by DoD entities, in order to ensure historical abuses do not arise again. They serve to implement the immortal words of now-retired Major General James L. Dozier: "We must never forget who our bosses really are: the American People. *We* are here to protect *them*."[365]

[365] Major General James L. Dozier, U.S. Army North, Concluding Remarks, Army Force Protection Conference, San Antonio, Tex. (July 22, 2008). Major General Dozier, U.S. Army, Retired, was kidnapped from his apartment in Verona, Italy, on 17 December 1981, by the Red Brigades terrorist group, and was held for forty-two days until being rescued by an elite anti-terrorism unit of the Italian Carabinieri. *See* Colonel (Retired) Thomas D. Phillips, U.S. Air Force., *The Dozier Kidnapping: Confronting the Red Brigades*, AIR & SPACE POWER J. (Feb. 7, 2002), http://www.airpower.au.af.mil/airchronicles/cc/phillips.html.