LOAN DOCUMENT

PHOTOGRAPH THIS SHEET

DTIC ACCESSION NUMBER

LEVEL

TJAGSA

1

INVENTORY

Civilian Demonstrations Near

DOCUMENT IDENTIFICATION

Mar 1992

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

DISTRIBUTION STATEMENT

HANDLE WITH CARE

ACCESSION FOR
NTIS GRA&I
DTIC TRAC
UNANNOUNCED
JUSTIFICATION

BY

DISTRIBUTION/

AVAILABILITY CODES

DISTRIBUTION	AVAILABILITY AND/OR SPECIAL	
A		

DISTRIBUTION STAMP

DATE ACCESSIONED

DATE RETURNED

20061026061

DATE RECEIVED IN DTIC

REGISTERED OR CERTIFIED NUMBER

PHOTOGRAPH THIS SHEET AND RETURN TO DTIC-FDAC

DTIC FORM 70A JUN 90

DOCUMENT PROCESSING SHEET

PREVIOUS EDITIONS MAY BE USED UNTIL STOCK IS EXHAUSTED.

LOAN DOCUMENT

Civilian Demonstrations Near the Military Installation: Restraints on Military Surveillance and Other Intelligence Activities

A Thesis

Presented to

The Judge Advocate General's School, United States Army

The opinions and conclusions expressed herein are those of the author and do not necessarily represent the views of either The Judge Advocate General's School, The United States Army, or any other government agency.

by Major Paul M. Peterson, JA
U.S. Army

40TH JUDGE ADVOCATE OFFICER GRADUATE COURSE

March 1992

Published: 140 Mil. L. Rev. 113 (1993)

Civilian Demonstrations Near the Military Installation: Restraints on Military Surveillance and Other Intelligence Activities

by Major Paul M. Peterson

ABSTRACT: Anti-war and anti-military demonstrations have occurred during every modern conflict. When such demonstrations are anticipated outside an installation, the commander wants to know as much as possible about any potential threat to installation facilities, personnel, or operations. Unfortunately, internal military procedures for obtaining the desired information are inconsistent and confusing. Commanders attempting to follow this guidance may collect and retain information in violation of the Privacy Act and the first amendment. To cure these problems, the thesis proposes significant changes to an existing Department of Defense Directive.

TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

> The ... task is to reject as false, claims in the name of civil liberty which, if granted, would paralyze or impair authority to defend ... our society, and to reject as false, claims in the name of security which would undermine our freedoms and open the way to repression.[1]

I. INTRODUCTION

The commander of a large Army installation convenes a staff meeting. The Provost Marshal[2] tells the commander that a civilian demonstration is scheduled outside one of the gates next week. The commander expresses concern about disruptions of military activities, but the Provost Marshal can't provide him any more detailed information about the demonstration. The commander then instructs his Provost Marshal and his intelligence officer (G-2)[3] to find out everything they can about the organization sponsoring the demonstration and the anticipated course of the demonstration. The commander then turns to his lawyer: "Any problems, Judge?"

This factual situation might easily occur. Labor

strife might precipitate a demonstration at almost anytime, and, during times of international tension, anti-war demonstrations can and do occur. During the recent Operations JUST CAUSE, DESERT SHIELD, and DESERT STORM, for example, anti-war demonstrations occurred near several different military installations even though the actual hostilities were short in duration and relatively popular.

The thesis examines the legal ramifications of domestic intelligence collection under these circumstances. Unfortunately, the military's internal guidance for obtaining such intelligence is ill-defined, confusing, and contradictory. As a consequence, commanders may unwittingly initiate a process of information collection and retention violative of statutory and constitutional rights.[4] The result may be litigation and unwelcome publicity.

II. ORGANIZATION AND SCOPE

The thesis begins with a summary of military involvement in domestic intelligence gathering. Historical knowledge aids in understanding the issues developed in the thesis.

The thesis then sets forth the existing regulatory guidance that impacts on military surveillance of civilians. The guidance varies considerably depending on whether the commander chooses to use law enforcement or military intelligence personnel to collect information.

The thesis then measures the existing regulatory guidance against the Privacy Act[5] and the first amendment.[6] These two authorities are the most likely source of legal challenge.

The thesis concludes with proposed changes to a key Department of Defense Directive. The thesis discusses how the proposed changes render the regulatory guidance more consistent and lessen the likelihood of a successful legal challenge.

The thesis is limited in scope. Since most dissent,

including anti-war dissent, is of domestic origin,[7] the thesis is restricted to collection efforts targeting activities with no foreign sponsorship. The analysis also excludes situations where the President uses his emergency authority to mobilize the military in response to a civil disturbance or where the activity in question is being conducted by soldiers or civilians affiliated with the Department of Defense.

Some important terms require definition prior to beginning the discussion. The Army defines "Physical security" as "[t]hat part of the Army security system, based on threat analysis, concerned with procedures and physical measures designed to safeguard personnel, property, and operations; to prevent unauthorized access to equipment, facilities, materiel, and information; and to protect against espionage, terrorism, sabotage, damage, misuse, and theft."[8] In the context of the thesis, "Physical security intelligence" will mean any information gathering which focuses on the protection of military operations within CONUS when there is no evidence that the persons considered a potential threat are either affiliated[9] with the Department of Defense or sponsored by any

foreign power. "Domestic intelligence," on the other hand, will refer to all intelligence gathering within the United States, by military or civilian agencies, for any purpose, including: physical security, preparation for civil disturbance operations, and detection and monitoring of organized crime or terrorists.

III. HISTORICAL BACKGROUND

A. The Origins of Domestic Intelligence Collection

The United States military, and more specifically the Army, has been involved in collecting information on the political activities of civilians for one reason or another since the nineteenth century. One scholar who has specialized in the study of military intelligence traces military collection of domestic intelligence back to the formation of the Army's Military Intelligence Division in 1888.[10] World War I, however, brought on the first extensive domestic intelligence operations. Tasked at first to provide information about supposed large scale German espionage rings (which never materialized), the military intelligence apparatus began collecting political information on German immigrants and, eventually, persons and organizations whose common goal was opposition to the war. Even though organized domestic intelligence declined during the post-war era, the World War I experience provided a bureaucratic scheme and collection plan that was employed by the military

to again step up domestic surveillance in each ensuing period of crisis (i.e., the Bonus March of 1932, World War II, and the Korean War). There was a tendency for stateside counterintelligence agents to be underemployed and readily available to perform political surveillance, and the civilian hierarchy above the military often was ignorant about the extent or nature of domestic intelligence gathering.

Prior to the early 1970s there was little apparent written authority for military involvement in domestic intelligence gathering. In 1939, President Roosevelt directed that the investigation of all "espionage, counterespionage, and sabotage matters" be controlled and handled exclusively by the Federal Bureau of Investigation (FBI), the "Military Intelligence Division" of the War Department, and "the Office of Naval Intelligence."[11] Subsequent Presidential directives tasked the FBI to "take charge" of these same matters and others (e.g., "subversive activities" and "violations of the neutrality laws"), but the remaining role of the military departments, if any, was not addressed.[12] Only in the area of personnel loyalty and personnel security was significant written

authority[13] provided to the War Department[14] or its successor, the Department of Defense.

B. The Viet Nam War Era

In the late 1950s and early 1960s, the Army became involved in the civil rights conflict. Federalized guardsmen and active duty personnel were mobilized and deployed to stop violence and enforce federal civil rights decrees. Despite a lack of specific authority, the Army began to collect information, often of a personal nature, on activists connected with the civil rights movement. In 1967, the first in a series of large civil disturbances requiring prepositioning and use of federal troops took place. Some of these disturbances, like the March on the Pentagon in 1969, involved potential interference with military personnel, property, or operations; other disturbances simply contained a potential for violence beyond the capability of state or local law enforcement to control. In response to a perceived mission requirement, the Army took steps to expand its collection of information, including personal and

political information, on individuals and groups that might have any connection with future civil disturbances. Operating with little apparent high level supervision, two parallel and redundant intelligence collecting apparatus evolved, with an estimated 1,500 intelligence operatives. These personnel collected data, using overt and covert collection methods, on a wide range of persons and organizations. No standards or procedures existed to ensure that information was relevant, properly verified, properly organized, and properly disseminated.[15]

C. The Public Outcry

In January, 1970, a description of the Army's domestic intelligence system and its purported excesses appeared in a national magazine.[16] The Subcommittee on Constitutional Rights of the Committee on the Judiciary, United States Senate, opened hearings into the issue in February 1970. The subcommittee report[17] detailed multiple problems with the Army domestic intelligence program, including the collection of

personal and political information on nonviolent persons and groups, the covert penetration of targeted organizations, and the retention and possible dissemination of inaccurate information. The subcommittee report stated that the civilians responsible for overseeing the Army had been misinformed and were often unaware of the nature and extent of surveillance activities.[18] The subcommittee report concluded that the military domestic intelligence program was illegal in that there was no statutory authorization for much of the collection activity and the program violated the constitutional rights of the persons subject to collection activities.

D. The Legal Analysis of the Subcommittee

The subcommittee applied a three part legal analysis to the Army's activities.[19] Was any part of the Army intelligence collection program authorized by law? If so, did the execution of any part of the authorized program infringe on individual constitutional rights? And, if so, was the infringement justified by a compelling government interest?

Focusing on the collection of information in preparation for use in potential civil disturbance situations, the subcommittee concluded that the program was not legally authorized. The committee reasoned that there was no express statutory authority for such collection, and that where a citizen's constitutional rights are threatened by military activity, as here, (see paragraph below) the law did not allow for creation of implied authority. Additionally, the statutes enabling the use of military force in civil disturbances did not reasonably contain implied authority for military intelligence collection prior to the actual disturbance itself (e.g., military force was not authorized until the President personally concludes civilian law enforcement is inadequate, and civilian agencies were perfectly capable of collecting any requisite intelligence until this point in time was reached).

The subcommittee also concluded that collection of domestic intelligence by the military infringed on the free speech and association rights of those targeted. The subcommittee felt that the mere knowledge that the Army was collecting information on a given individual

or group would create fear and apprehension among the subjects, cause them to be more circumspect in all of their political activities, and make it less likely that others would want to associate with them. The committee also implied that the collection procedures used by the military were violative of the constitutional right to privacy.

Finally, the subcommittee concluded that there was no compelling governmental interest[20] that could justify the military infringement of constitutional rights.

The military was collecting personal and political information on the theory that the civil disturbances were planned violent events linked by a nationwide foreign-sponsored conspiracy. However, there was never any evidence that the disturbances were other than a series of unorganized and unrelated events.[21] Hence, the political information was of little use. The military was not able to predict the timing, size, or scope of any pending civil disturbance.[22] Resources expended on collection of political data were used at the expense of tactical collection (data on roads, bridges, utilities, etc.) that was not properly

attended to.[23]

Even had there been some governmental interest in the information collected, the subcommittee noted that the collection of intelligence data by civilian agencies (e.g., the FBI) would be less intimidating, leading to the conclusion that the use of civilian investigative agencies would always be constitutionally preferred.[24]

E. Laird v. Tatum

In February, 1970, several individuals and groups who claimed to be subjects of Army surveillance filed suit in federal district court alleging that the Army surveillance violated their first amendment rights. The plaintiffs sought declaratory and injunctive relief, to include an order to destroy all information collected about them and a further declaration that the Army's activities were beyond the scope of any existent legal authority. The trial court dismissed the complaint for failure to state a claim upon which relief could be granted, but the Court of Appeals reversed[25] and ordered an evidentiary hearing. Before

such a hearing could be held, the Supreme Court granted the government's petition for certiorari. On June 26, 1972, the Court held[26] that the plaintiffs had failed to allege a form of personal injury sufficient for standing purposes. Chief Justice Burger, writing for a 5-4 majority,[27] stated that general allegations of negative impact on the rights of free speech, association, and privacy were not the types of specific present or future harm that Article III courts had jurisdiction to adjudicate.

The majority opinion implied that if some more specific injury was alleged as a result of information collected by the Army (e.g., loss of employment or loss of security clearance), the injured party might have standing to challenge the Army's information collection practices. Contemporaneous complaints filed in other courts by plaintiffs similarly situated were dismissed based on the result in Laird v. Tatum.[28] And, while these cases were being processed, DoD was busy trying to purge its data banks and formulate internal guidance for future domestic intelligence collection.

F. The Military Reaction

As early as 1967, senior officials in the Department of the Army (DA) were awakening to the domestic intelligence problem.[29] It was not until 1970, however, that Army-wide guidance was promulgated. On December 15, 1970, DA published a policy letter authorizing the collection of information on civilians for certain reasons, including "unauthorized demonstrations on active ... Army installations or through (sic) demonstrations immediately adjacent to them which are of a size or character that they are likely to interfere with the conduct of military activities."[30]

G. Attempts to Legislate

As a result of the Subcommittee hearings, Senator Sam Ervin, Chairman of the Subcommittee, introduced a bill[31] designed to place specific statutory limits on domestic intelligence collection by the military. The bill, S.2318, was a proposed criminal statute. It forbade any military officer from investigating, recording, or maintaining information on "the beliefs,

associations, or political activities" of persons and organizations not affiliated with the military. S.2318 contained four narrow exceptions[32] to the general prohibition and provided aggrieved persons with a civil cause of action.

Hearings were held on S.2318 in April, 1974. The Department of Defense (DoD) strenuously opposed S.2318.[33] DoD argued that the legislation was unnecessary because the excesses of the past had been eliminated, and new internal regulations and oversight mechanisms were in place to prevent future recurrence of the problem.

S.2318 was not passed by the full Senate and never became law. The failure of this legislation, combined with the refusal of the Supreme Court in Laird to reach the substantive first amendment issues surrounding domestic intelligence, apparently left DoD with significant regulatory flexibility.[34]

The relevant law, however, evolved faster than the regulatory guidance. Senator Ervin continued his work throughout 1974 in the area of privacy and the control of information. He and the Government Operations Committees of the House and Senate drafted the Privacy

Act,[35] which became law on January 1, 1975. Further, decisions rendered subsequent to Laird have cast into doubt its vitality as a barrier to plaintiffs challenging military surveillance. The regulations, the Privacy Act ramifications, and the impact of the post-Laird decisions involving the first amendment are considered in the remainder of the thesis.

IV. EXISTING REGULATORY GUIDANCE

Several regulations and directives impact on the collection of physical security intelligence. Three of these documents, however, are particularly important: Dep't of Defense Directive 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense;[36] Army Reg. 380-13, Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations;[37] and Army Reg. 381-10, U.S. Army Intelligence Activities.[38] In the thesis these three documents will be referred to collectively as "the physical security intelligence regulations."

The Department of Defense issued DoD Dir. 5200.27, its first formal guidance on collection of information concerning nonaffiliated civilians, on March 1, 1971. DoD Dir. 5200.27 used different format and terminology from the then existing Army policy letter on the same subject.[39] AR 380-13, "implementing" DoD Dir. 5200.27, was published on September 30, 1974. Unfortunately, AR 380-13 used somewhat different organization and terminology than DoD Dir. 5200.27 used, creating some

potential for confusion.[40]

In 1978, the Foreign Intelligence and Surveillance Act (FISA)[41] was enacted. FISA set forth specific guidance on the conduct of electronic surveillance when targeting foreign powers and their agents. The President then issued Executive Order 12,036,[42] implementing FISA and establishing additional guidance for the "Intelligence Community" on the conduct of domestic investigative techniques other than electronic surveillance. The Department of Defense, in turn, produced a new regulatory scheme applicable to certain "intelligence components" and "intelligence activities."[43] The Army issued AR 381-10, U.S. Army Intelligence Activities, as a result of this new scheme.[44]

Although AR 381-10 is a product of a series of events beginning with the FISA, the scope of AR 381-10 is much wider than the FISA. AR 381-10 controls all the surveillance activities of Army intelligence components, whether or not such surveillance is "electronic" and whether or not there is a foreign connection. Unfortunately, AR 380-13 has not been revised to reflect the sequence of events which

produced AR 381-10. The existence of AR 381-10 thus creates additional confusion in the physical security intelligence arena.[45]

The applicability of the individual physical security intelligence regulations generally depends on who is tasked to collect the information. The thesis discussion is, therefore, organized around the type of military personnel who might be tasked. Personnel available to perform the mission include the Provost Marshal (with internal Military Police (MP) assets) and the G-2. The local counterintelligence (CI) unit might also respond to the commander's request for assistance.

A. Military Police.

Pursuant to Army Regulations,[46] the installation commander is responsible for the security of the personnel, property, and operations under his command. The missions of assigned military police (MP) personnel include "activities directed at the prevention of crimes ... or as required for the security of persons and property under Army control ...."[47] Additionally, installation MP's establish and maintain a criminal

information program. The purpose of the program is to collect, categorize, and process information which will "identify individuals or groups of individuals in a effort to anticipate, prevent, or monitor possible criminal activity."[48]

1. Collection Threshold.

Specific guidance is available on when information on nonaffiliated civilians may be collected. DoD Dir. 5200.27 discusses, as separate bases for acquisition of information, both concern with the effects of demonstrations and the investigation or prosecution of crimes under DoD jurisdiction. AR 380-13, however, does not apply to criminal investigations, indicating instead that "authorized criminal investigation and law enforcement intelligence activities (i.e., not counterintelligence related)" are covered by other, unspecified, regulations. Since criminal investigative activities and law enforcement intelligence are not defined in AR 380-13, its application to military police activities conducted for physical security purposes is uncertain.[49] Most of the definitive

guidance, therefore, must be drawn directly from DoD Dir. 5200.27.

Information on nonaffiliated personnel may be collected and reported if essential to protect threatened defense personnel and defense activities and installations. The threat must take the form of acts of subversion, theft or destruction of DoD property, acts jeopardizing the security of DoD elements or operations, demonstrations on active DoD installations, or crimes for which DoD has responsibility for investigating or prosecuting.[50] No information may acquired about a person solely because of lawful advocacy of measures in opposition to Government policy.[51]

2. Limitations on Type of Information Collected.

The information collected must be essential to the mission.[52] Information concerning purely political activities, personalities, or activities in which no crime is indicated or suspected, will not be collected, recorded, or reported within the MP criminal information system.[53] No record describing how an

individual exercises rights guaranteed by the first amendment will be kept unless pertinent to and within the scope of an authorized law enforcement activity.[54]

3. Limitations on Collection Methods.

Maximum reliance shall be placed on federal civilian investigative agencies and their state and local counterparts.[55] There shall be no covert or otherwise deceptive surveillance or penetration of civilian organizations[56] unless specifically authorized by the Deputy Under Secretary of Defense after coordination with the FBI.[57] There shall be no electronic surveillance except as authorized by law.[58] No personnel will be assigned to attend public or private meetings, demonstrations, or other similar activities[59] without specific prior approval of the Secretary or Undersecretary of the Army,[60] unless the local commander determines that the threat is immediate and time precludes obtaining prior approval.[61]

4. Limitations on Retention.

According to DoD Dir. 5200.27, information shall be destroyed within 90 days of collection unless its retention is specifically authorized under criteria established by the Deputy Under Secretary of Defense (Policy Review).[62] No formal criteria have been published.[63]

B. The Staff G-2.

Although the applicability of AR 380-13 is uncertain in the context of military police activities, the uncertainty vanishes when considering staff G-2 activities. The provisions of both AR 380-13 and DoD Dir. 5200.27 apply to the activities of the staff G-2 when collecting information about nonaffiliated civilians.[64]

1. Collection Threshold.

Information on persons and organizations not affiliated with the DoD may be gathered in connection with the protection of Army personnel, functions, and property; but only if there is a reasonable basis to

believe that one or more of several express situations exists.[65] One situation is a demonstration on or immediately adjacent to the installation of such a size or character that it is likely to interfere with the conduct of military activities. Another situation is theft or destruction of equipment or facilities belonging to DoD units or installations. A third situation is "[s]ubversion of loyalty, discipline or morale of ... military ... personnel by actively encouraging violation of laws, disobedience of lawful orders and regulations, or disruption of military activities."[66] The acquisition of information on a person "solely because of lawful advocacy of measures in opposition to U.S. government policy or because of activity in support of racial and civil rights interests" is prohibited.[67]

2. Types of Information That May Be Collected.

The information to be gained must "relate" to the described collection situation.[68] No record describing how an individual exercises rights guaranteed by the first amendment will be maintained unless pertinent to

and within the scope of an authorized law enforcement activity.[69]

3. Limitations on Collection Methods.

To determine whether an actual or potential threat situation exists, the commander will conduct routine liaison with local law enforcement agencies and will conduct "counterintelligence surveys and inspections."[70] If the commander has reason to believe that further information about nonaffiliated persons is needed, further inquiries will be made to local law enforcement agencies via the local counterintelligence liaison unit. If the commander has reason to believe that an actual or potential threat situation exists, and the local law enforcement authorities cannot or will not provide requested information, the commander may request authority from Department of the Army (HQDA) to conduct a "special investigation/operation."[71]

There will be no electronic surveillance except as authorized by "law and regulation."[72] The Undersecretary must authorize any covert or otherwise

deceptive penetration of civilian organizations after approval by the Defense Investigative Review Committee (DIRC).[73] The Undersecretary must approve attendance at any public or private meetings, demonstrations, or other similar activities, except where the local commander "in his judgment," perceives the threat as immediate and time precludes obtaining prior approval.[74] The commander may dispatch investigators to observe a demonstration which meets the collection threshold.[75]

4. Limitations on Retention

According to DoD Dir. 5200.27, information shall be destroyed within 90 days of collection unless its retention is specifically authorized under criteria established by the Deputy Under Secretary of Defense (Policy Review).[76] No formal criteria have been published. Nevertheless, AR 380-13 has some criteria which allow for retention beyond 90 days. Information may be retained if, in the previous year, the individual/organization has been connected with an actual example of violence or criminal hostility

directed against the Army; the individual/organization has been connected to a specific threat to Army personnel, functions, or property; the individual/organization's "continuing hostile nature in the vicinity of Army installations continues to provide ... a significant potential source of harm or disruption of the installation or its functions;" or the individual/organization has "... counseled or published information actively encouraging Army personnel to violate the law, disrupt military activities, or disobey lawful orders."[77]

C. Counterintelligence Units.

Unlike the G-2 staff section, the local counterintelligence unit is a "DoD intelligence component."[78] Hence the provisions of Army Reg. 381-10 apply,[79] while DoD Dir. 5200.27 and AR 380-13 are expressly inapplicable.[80]

1. Collection Threshold.

AR 381-10 allows for collection of information that

identifies a U.S. person only if it is collected for a specifically enumerated purpose which is an assigned function of the collecting unit. Intelligence components may collect information about a person if the information is "publicly available" or if the person is "reasonably believed to threaten the physical security of DoD employees, installations, operations, or official visitors,"[81] Collection of information is limited, however, to threats posed by terrorists or foreign governments.[82] Terrorism is defined as the use or threat of violent acts to attain goals political, religious, or ideological in nature. Terrorism in this context does not require a foreign connection; it may be wholly sponsored by a domestic group.[83] The collection of information relating to a U.S. person solely because of lawful advocacy of measures opposed to Government policy is not authorized.[84]

2. Types of Information That May Be Collected.

There are no specific regulatory limits on the content of information that may be collected.

3. Limitations on collection methods.

Information should be collected from publicly available sources with the consent of the subject. If this approach is "not feasible or sufficient," the investigator should use other "lawful investigative techniques."[85]

Certain techniques are specifically controlled. Physical surveillance[86] may only be conducted on personnel affiliated with the military.[87] Undisclosed participation in the activities of domestic organizations is not permitted.[88] However, attendance at public organizational meetings, or meetings or activities which involve organization members but which are not functions or activities of the organization itself, does not constitute participation.[89] It is unclear whether there are any regulatory limitations on the use of nonconsensual electronic surveillance,[90] nonconsensual physical searches,[91] or mail searches.[92]

D. Comparison of Regulatory Guidance.

The difference in the applicable guidance may be

quite significant. If one type of functional personnel suffers from a regulatory restriction, the commander (or HQDA) might use another approach to obtain needed information. CI units appear to be limited to investigations involving violent acts for political, religious, or ideological ends; while neither a violent threat nor a political end is a prerequisite for MP or G-2 involvement. However, MP involvement may be limited to on-post demonstrations while the G-2 is authorized to investigate demonstrations occurring adjacent to the installation.

CI personnel may not conduct physical surveillance, but MP and G-2 personnel are not so limited.

CI personnel may attend public, but not private, organizational meetings. MP and G-2 personnel, however, may attend any meeting, public or private, with the approval of either HQDA, or, in an emergency, the commander.

CI personnel may not actively participate or influence the activities of an organization. MP and G-2 personnel must obtain prior approval before covert or otherwise deceptive penetration of an organization, but there is no limitation on the extent of their

participation following such penetration.

MP personnel may not place information about purely political activities, personalities, or activities in which no crime is indicated or suspected into their criminal information system; and no personnel may file information describing how an individual exercises his first amendment rights unless within the scope, and pertinent to, an authorized law enforcement activity.

V. STATUTORY ANALYSIS

A. The Privacy Act

As noted previously, the tumult of the early 1970s did not produce any legislation that was specifically directed toward the military. However, the perceived invasion of privacy resulting from the actions of the federal government, both civilian and military,[93] did eventually produce some legislation: the Privacy Act of 1974[94] [hereinafter "the Act"].

The focus of the Act is on records maintained by the government that contain information about a specific individual. The Act places restrictions on both the type of information that may be contained in a Privacy Act record and how that information is used and disseminated. Most of the Act's provisions only apply to "systems of records,"[95] or records about individuals that are retrieved by reference to the individual's name or other personal identifier.

Two provisions of the Act are of specific concern to the collector of physical security intelligence.

Subsection (e)(7)[96] provides, with limited exceptions, that no agency will maintain records describing how first amendment rights are exercised. Subsection (e)(1)[97] provides that records maintained by the agency must be relevant and necessary to accomplish a purpose of the agency.

Physical security intelligence collection will likely include information about specific persons. Collection will include evidence of any planning to disrupt military activities, any past history of disruption of federal activities, any past advocacy of such disruption, and any association with groups that have advocated or participated in such disruption.

Information received or collected will probably be recorded in some permanent form (e.g., written, video, or pictures) for future reference. The information may be kept in the personal notes of the investigator, or it may be reproduced and filed in some filing system. If placed in a filing system, the information will likely be placed in a one or more files (e.g., the United States Army Intelligence and Security Command (USAINSCOM) Investigative Files,[98] Counterintelligence Operations Files,[99] or Local Criminal Information

Files[100]) expressly subject to the Act. Even if the information is not placed in a formally established filing system the record will still be subject to the relevant Privacy Act restrictions if it is shared with anyone in the office.[101]

1. Subsection (e)(7).

> Each agency that maintains a system of records shall ... maintain no record describing how any individual exercises rights guaranteed by the first amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.[102]

Any physical security intelligence in the context of a demonstration will undoubtedly contain references to first amendment activity. A record of an individual's involvement in a demonstration describes the exercise of the rights of assembly, free speech, and, perhaps, petition for redress of perceived grievances.

Additionally, a record which links an individual to other individuals or groups involved in or planning a protest describes the exercise of the right of political association. Finally, a record that describes advocacy of political change, even through violent means, describes activity within the scope of the first amendment.

The only exception to section (e)(7) with any potential relevance in a physical security intelligence context is for records that are "... pertinent to and within the scope of an authorized law enforcement activity."[103] The key issue is whether information gathering on nonaffiliated civilians to avoid or alleviate a possible future disruption of military activities fits within this exception.

The regulatory interpretation and the legislative history of the Act are ambiguous. The plain meaning of "law enforcement," however, suggests that the "law enforcement" exception should not cover physical security intelligence operations. These sources of interpretation are discussed in sequence.

a. The OMB Guidelines

Neither "law enforcement" nor "law enforcement activity" are defined within the statute. Pursuant to statutory authorization,[104] the Office of Management and Budget (OMB) has published Guidelines[105] on the interpretation and application of the Privacy Act. The Guidelines, however, do not clarify the scope of the law enforcement exception.[106]

b. The Legislative History

The official legislative history of the Privacy Act is brief, and is not helpful with regard to the law enforcement exception. The Privacy Act in its final form was a hasty compromise between competing House and Senate bills. The language of (e)(7) came from a last minute House amendment. The official legislative history is a Senate Report on a previous attempt at compromise, and the language of (e)(7) did not exist at the time the official legislative history was drafted.

There is, however, some unofficial legislative history. Mr. Ichord, the representative who drafted the final language of (e)(7), submitted a statement

supportive of a broad, but undefined, interpretation of "law enforcement activity." Mr. Ichord specifically mentions investigations for personnel security and access to classified information as within his concept of "law enforcement activity."[107]

On the other hand, the unofficial legislative history in the Senate forms a basis for a contrary interpretation; an interpretation that would exclude military physical security operations. Prior to attempts to integrate the House and Senate versions of the Act, the Senate bill included certain exemptions for "investigative information" and "law enforcement intelligence information."[108] The "investigative information" exception was limited, by definition, to a criminal investigation of a specific criminal act within the statutory jurisdiction of the agency; or an investigation by an agency empowered to enforce any federal statute or regulation, the violation of which subjects the violator to criminal or civil penalties. The "law enforcement intelligence information" exception was limited, by definition to information compiled by law enforcement agencies, which agencies were further defined as "agenc[ies] whose employees

or agents are empowered by State of Federal law to make arrests for violations of State or Federal law."[109] The military has no explicit arrest authority for purposes of physical security operations.[110]

The phrase "law enforcement" also appears in three subsections of the Act other than subsection (e)(7): subsections (b)(7), (j)(2), and (k)(2). In each subsection, the phrase "law enforcement" is used in a similar manner: to describe limited exceptions to the privacy protections afforded by the Act. The meaning of "law enforcement" should, therefore, be interpreted in a consistent manner throughout the Act. Although (b)(7) and (j)(2) turn out to be of little help in the interpretation process,[111] (k)(2) is interesting.

Section (k) allows certain agencies to exempt certain records from many substantive provisions of the Act. Subsection (k)(2) covers "investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) ...." According to the OMB, subsection (k)(2)

> allows agency heads to exempt a system of records compiled in the course of an investigation of an alleged or suspected violation of civil laws,

including provisions of the Uniform Code of Military Justice and associated regulations .... The phrase "investigatory material complied for law enforcement purposes" is the same phrase as opened exemption 7 to the FOIA (Freedom of Information Act) prior to its recent amendment .... The case law which had interpreted ... "law enforcement purposes" for the now amended portions of exemption (b)(7) of the FOIA should be utilized in defining those terms as they appear in subsection (k)(2) of the Privacy Act.[112]

Exemption 7 of the Freedom of Information Act (FOIA)[113] was amended[114] at approximately the same time and by the same committees[115] that wrote the Privacy Act. The FOIA amendments put "lawful national security intelligence investigations" within the scope of "law enforcement purposes."[116] The legislative history of the FOIA amendments indicates that the phrase national security was intended to include "military security."[117]

Even so, "national security intelligence" does not necessarily encompass "physical security intelligence." The phrase "national security" is ambiguous and may be limited to protection against threats emanating from

foreign entities or domestic groups desiring the overthrow of the government.[118]

Additionally, at least one court has specifically rejected the application of FOIA usages to Privacy Act terms on the grounds that the two statutes have radically different purposes.[119]

c. Subsection (e)(7) Case Law

No federal courts have had occasion to interpret subsection (e)(7) in the context of a physical security intelligence operation. The cases that have interpreted subsection (e)(7) can be divided into two categories.

The first category involves complaints against the FBI and the Internal Revenue Service (IRS), federal agencies that are empowered to enforce specific federal statutes or regulations arguably relevant to the investigation in question.[120] The courts in these cases did not ponder whether the investigations were "authorized law enforcement activities," but, rather, whether the information collected was "pertinent to and within the scope" of those law enforcement

activities.[121]

The second category of cases involved the collection and maintenance of information on the conduct of employees. In each employee conduct case, the court held that (e)(7) was not violated, concluding either that the record complained of contained no information describing how the employee exercised his first amendment rights,[122] or concluding that tracking employee conduct and performance fell within the law enforcement activity exception.[123] The sole support for the latter proposition was the language of Representative Ichord and the reference to "personnel security" in his statement.[124] In all these cases the legislative history from the Senate was ignored; although one court did note that the employee/employer relationship was special and closer scrutiny would be given to any collection of information on nonaffiliated persons.[125]

So the legislative history of the law enforcement exception is, at best, ambiguous; and the case law unhelpful. There are some good reasons, however, not to consider physical security intelligence operations as within the scope of the law enforcement exception.

Consider the plain meaning of "law enforcement." The phrase implies an intent to enforce some positive law; while the purpose of security functions is primarily protective. Off-post demonstrations that might disrupt military activities do not necessarily involve violations of law within military jurisdiction,[126] and may not encompass criminal violations of any federal law.[127] Additionally, the use of the root "force" within "law enforcement" implies the right to use force; and various definitions and usages of law enforcement equate law enforcement authority with specific powers (e.g., the right to execute searches, to seize evidence, or to make arrests)[128] in connection with violations of specific laws within the jurisdiction of the one asserting the authority.[129] In conducting physical security operations, however, the military has no arrest, search, or seizure powers, at least with regard to incidents which occur off-post.[130]

In fact, the military's right to conduct physical security operations is essentially the same self-defense right shared by all persons and entities. To equate preparations for self-defense with law

enforcement would enable all persons and organizations to label their security functions as "law enforcement" and their security personnel as "law enforcement officers."

Further, any insistence that physical security intelligence operations are "law enforcement activities" risks labeling such operations as violative of the Posse Comitatus Act. The Posse Comitatus Act provides that

> [w]hoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined not more than $10,000 or imprisoned not more than two years, or both.[131]

The right of the military to conduct physical security or protective functions is not expressly authorized by Congress or the Constitution.[132]

In fact, there is not even an executive order which addresses physical security intelligence operations.[133] There is some question, then, even if security operations are "law enforcement activities," whether

those operations are "authorized" as specifically required by (e)(7).

If military physical security operations are "authorized law enforcement activities," the remaining issue is whether maintenance of information on nonaffiliated civilians is pertinent to and within the scope of that activity. Most courts that have considered this issue have decided that any information that is relevant to the law enforcement activity satisfies the requirement.[134] The 11th Circuit, however, applies a tougher standard: the information must be connected to an investigation of past, present or anticipated violations of statutes which the investigating agency is authorized to enforce.[135]

2. Subsection (e)(1)

"Each agency that maintains a system of records shall ... maintain in its records only such information about an individual that is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[136]

Agencies may choose to exempt some records from this requirement;[137] however, with regard to certain relevant systems of records (e.g., USAINSCOM investigative files and local criminal information files), the Department of the Army has not claimed any exemption for physical security intelligence.

Subsection (e)(1) is more than a relevancy standard. Subsection (e)(1) requires that a conscious decision be made that the information in question is required to meet the needs of an agency.[138] The legislative history indicates that the government must show that maintenance of the information in question is warranted by some "overriding need of society" and that the goal of the government in maintaining the information cannot reasonably be met through alternative means.[139]

OMB, however, has interpreted the underlying purpose requirement of subsection (e)(1) quite broadly: "By the Constitution, a statute, or executive order authorizing or directing the agency to perform a function, the discharging of which requires the maintenance of a system of records."[140] Under this standard, the Secretary's statutory authority to issue

regulations for the "functioning and efficiency of the Army"[141] is probably sufficient implied authority for physical security intelligence operations. Further, the cases do not follow the legislative history in placing the burden on the government to show an overriding government interest and lack of alternative solutions when specific information is challenged under subsection (e)(1). Instead, it appears that the plaintiff is often required to demonstrate that the information collected and maintained is "irrelevant" or "unnecessary" to the function in question.[142] This relaxed relevancy standard weakens subsection (e)(1) as an effective limit on the type of information collected for physical security intelligence purposes.

3. Enforcement.

The Act provides for both criminal penalties[143] and civil remedies.[144] Criminal violations are unlikely under the physical security intelligence scenario.[145] With regard to civil remedies, the Privacy Act can only be used against the United States, and not against individual employees of the United States.[146]

Suit may be brought against the United States for violations of subsections (e)(1) or (e)(7) if the violation had an "adverse effect"[147] on the individual bringing the suit. If the agency "acted in a manner which was intentional or willful," the United States must pay costs, reasonable attorneys fees, and the greater of $1000 or "actual damage" sustained by the individual.[148]

The phrases "adverse effect" and "actual damage" have been broadly construed by the circuit courts. Adverse effect includes psychological effects,[149] and extends to fear of an official investigation.[150] "Actual damages" encompass all the ordinary elements of compensatory damages, including those that are not objectively quantifiable (e.g., pain and suffering due to mental distress).[151]

The meaning of "acted in a manner which was intentional or willful" is less clear. Although plaintiffs do not have to prove that Agency personnel actually knew they were violating the Act at the time of the violation,[152] plaintiffs must demonstrate behavior exceeding gross negligence,[153] or that "the agency committed the act without grounds for believing

it to be lawful."[154]

4. Discussion

Although the "relevant and necessary" requirement of subsection (e)(1) may be satisfied by the current regulations,[155] the application of subsection (e)(7)'s ban on maintenance of first amendment is problematic. Current physical security intelligence regulations generally make no distinction between personal, political, and other information.[156] The only specific requirement is applicable to the military police: "Information concerning purely political activities, personalities, or activities in which no crime is indicated or suspected, will not be collected, recorded, or reported."[157] The physical security intelligence regulations need to be restructured with an eye toward ensuring compliance with subsection (e)(7).

Given the difficulty with interpreting subsection (e)(7), a challenge to the collection and maintenance of first amendment information may fail to show that the agency acted "without grounds for believing it to

be lawful." Although this defense might stop the first plaintiff, it does not justify failing to bring the regulations in line with a proper interpretation of subsection (e)(7). There are several possible changes to be considered.

One way to avoid the application of the Privacy Act entirely is to avoid maintenance of information on identifiable individuals. Information on individuals that is received, either from military investigators, outside agencies, or other sources, might be screened or summarized in such a way as to remove personal identifiers. Identifying collected data with groups, and not individuals, eliminates the applicability of the Act.[158]

The maintenance of some information about individuals may be unavoidable. Individuals who are group leaders or instigators may have to be identified and tracked by name. In this case, the legitimate use of the law enforcement exception to the ban on maintenance of first amendment information may be possible. The Army might, in connection with a physical security investigation, uncover evidence of a specific past, present, or future violation of the law.

The information could be forwarded to the applicable law enforcement agency, which might then open an investigation and request further assistance. The Army could then justify its information practices under the law enforcement exception to subsection (e)(7) by piggybacking off the law enforcement authority of the civilian agency.[159]

Some information, however, has so little relevance to any physical security intelligence operation that it could be excluded categorically. Information on personal financial status, educational history, sexual practices, and religious beliefs could be considered for such exclusion.

These concepts and others are considered in a proposed draft DoD Directive 5200.27,[160] discussed in section VII. below.

B. POSSE COMITATUS ACT

As indicated previously, the Posse Comitatus Act (PCA)[161] may affect the interaction between the military and civilian activities. The Army has taken the position that the PCA does not apply to actions

undertaken primarily for military or foreign affairs purposes, including physical security operations.[162] Since there is no express authority to conduct physical security operations, it is unclear how the Army's position is derived from the Act.

The Supreme Court has not opined on the extent and limits of the PCA, but lower courts have generally defined it as proscribing those actions which are "regulatory, proscriptive, or compulsory" in nature.[163] Congress has authorized specific forms of assistance for counternarcotics efforts and in so doing has specifically disapproved the use of military personnel in search, seizure, arrest, or similar activities.[164] This statutory language could be implied as implicit approval of the "regulatory, proscriptive, or compulsive" definition of the PCA.[165]

To the extent that physical security intelligence operations are passive in nature they are not "regulatory, proscriptive, or compulsive." Unless the Army otherwise labels physical security intelligence operations as "law enforcement activities,"[166] the PCA should not prove a burden to those operations. Additionally, although the PCA provides for criminal

penalties, it is not independent authority for a civil cause of action.[167]

VI. THE FIRST AMENDMENT

Political groups and individuals, particularly those that protest official government policy, will not take kindly to being investigated by a government agency like the Army. To the extent that particular investigative or storage techniques run afoul of particular statutes, like the Privacy Act, the plaintiffs will have a cause of action against the agency. The fourth amendment also offers protection against certain investigative techniques. To stop an entire investigation, however, the plaintiffs may allege that the very existence of the investigation violates the protestor's first amendment rights. Specifically, they could allege that just knowing "big brother"[168] is watching everything they do deters them from aggressively asserting their freedoms of speech, assembly, and association. Regardless of the asserted need for the government surveillance, they will say, the right to conduct their political activities free of this "chill" is paramount.[169]

A. Standing.

As discussed in the historical summary, the only case to reach the Supreme Court as a challenge to Army domestic intelligence was Laird v. Tatum.[170] The plaintiffs' claim was that the Army investigative system 'chilled' their first amendment rights. The Army prevailed in Laird because the plaintiff failed to properly allege and prove the necessary injury-in-fact required by the "case or controversy" language in Article III of the Constitution. Any future plaintiff who wishes to mount a judicial challenge based on an Army Physical Security Intelligence operation in court will first have to get by the Laird barrier. In the twenty years since the Court spoke in Laird, judicial gloss has reduced the size and scope of plaintiff's standing hurdle. Analysis of the "law of standing" provides some insight into how internal military guidance for physical security intelligence might be structured to raise the Laird barrier as high as possible.

(The Laird court) granted certiorari to consider

> whether ... respondents presented a justiciable controversy in complaining of a 'chilling' effect on the exercise of their First Amendment Rights where such effect is allegedly caused, not be any specific action of the Army against them, but only by the existence and operation of the intelligence gathering and distribution system, which is confined to the Army and related agencies.[171]

The Laird court characterized plaintiff's allegations of "chill" as "subjective," which, under Article III, were not an adequate substitute for "a claim of specific present objective harm or a threat of specific future harm."[172]

Unfortunately, the Laird opinion is ambiguous and has been interpreted in many different, and often contradictory, ways.

For example, depending on the court, Laird did (or didn't) involve plaintiffs who were specific targets of investigation.[173] Laird does (or doesn't) apply to investigations which go beyond publicly available sources.[174] Laird does (or doesn't) mandate some 'regulatory, proscriptive, or compulsory' government

action to satisfy the minimum requirements of "chill" standing.[175]

To avoid the difficult standing barrier of Laird, lower courts may simply recharacterize "chill" as "censorship,"[176] or decide that the entire "holding" of Laird is meaningless dicta.[177]

Radically different interpretations of Laird may stem from the lack of principle underlying the Laird holding. Article III of the Constitution limits the jurisdiction of the courts to "cases or controversies." This constitutional limitation has historically required that the plaintiff show, among other things,[178] that "he personally has suffered some actual or threatened injury as a result of the putatively illegal conduct of the defendant."[179] Historically, the Court has connected the "injury-in-fact requirement" to the "case or controversy" provision by reasoning that actual injury motivates the plaintiff to litigate, which ensures adequate presentation of the case.[180]

"Injury in fact" includes physical, monetary, and psychological injuries. Standing is not limited to injuries that are past or present, but may also result from anticipated injuries.[181] Logically, the plaintiff

who is alleging threatened injury, rather than actual injury, is motivated by a present fear of that injury. This motivation is the motivation that drives plaintiffs in chill cases - fear that misuse of information gathered, or even just the knowledge that they are targets, will result in loss of employment, loss of security clearance, loss of reputation, etc.. The only difference between chill cases and other anticipated injury cases is that the plaintiffs cannot say exactly what the government might do to them; the plaintiff can only give a long list of possible future injuries. The point is that the plaintiff's fear may be different in degree (either more or less) than one who can point to a specific threatened injury, but it is not a different type of motivator than has previously been recognized by the court as adequate for Article III standing. Hence, it should not be excluded categorically.[182]

Laird presents another philosophical problem. Once the minimum Article III standing requirements are satisfied, the courts often look to other prudential factors when deciding whether to consider the merits of a particular case. The Laird opinion did not address

one important consideration[183] that supports justiciability and is present in all chill cases. The first amendment is not just another co-equal element of the bill of rights. The first amendment "transcends"[184] the other nine amendments in the sense that is protects both individual and societal interests. To the extent that an individual is limited in his speech, assembly, or association rights by government action, society is also injured. In fact, the free exchange of information is necessary to the basic functioning of a democratic form of government.[185] By arbitrarily excluding "subjective chill" plaintiffs, Laird runs counter to the previous expansive consideration of first amendment interests.[186]

These concepts shed some light on the willingness of certain post-Laird decisions to stretch Laird's facts and findings to derive standing. Two Supreme Court decisions are particularly important.

In Socialist Workers Party v. Attorney General[187] [hereinafter SWP III], decided shortly after the decision in Laird, Justice Marshall considered an appeals court decision enjoining the FBI from monitoring a national convention of the Young Socialist

Alliance. In determining that the plaintiffs had standing under the first amendment to challenge the FBI's surveillance, Marshall distinguished SWP III from Laird because the alleged surveillance in SWP III had the "concrete effects of dissuading some delegates from participating actively in the convention and leading to possible loss of employment .... [W]hether claimed chill is substantial or not is a matter to be reached on the merits."[188] But these injuries are difficult to distinguish from those alleged in Laird. The plaintiffs in Laird did allege that their associational rights had been injured because the Army's surveillance had deterred others from talking to them. Additionally, the plaintiffs in Laird complained that their future employment opportunities might be restricted. The only difference between the two cases (at least as reflected in the facts as stated in the judicial opinions) was that the Army admitted to providing its information only to "related civilian investigative agencies," while the FBI specifically admitted to providing its information to the federal agency which made federal employment decisions. Since the FBI was (and is) one of the Army's "related

civilian investigative agencies" for domestic intelligence purposes,[189] this difference amounted to a superficial distinction. The different outcomes in SPW III and Laird can rationally be distinguished as differences in pleadings or an interpretation of Laird that ignores the Laird facts.

In Meese v. Keene,[190] a 1987 Supreme Court decision, the Court further limited the effective reach of Laird. Plaintiff Keene, a California state representative, wanted to show three films produced in Canada. The Justice Department, in accordance with statutory authority, determined that the films were "political propaganda." This determination created a further requirement for placement of a label at the beginning of each film identifying briefly where it was from and who had produced it. Keene objected to the to the labeling process, claiming that the "political propaganda" determination chilled his first amendment right to display the films. He claimed fear of injury to his reputation and injury to subsequent employment prospects. As proof, he submitted affidavits and the results of a poll showing that his constituents would be less likely to vote for a candidate that displayed

films labeled as "political propaganda" by the government. The Court found, unanimously, that the allegations of reputational injury stemming from showing such films were sufficient for standing purposes.[191]

Not surprisingly, the lower courts have taken notice. The most recent surveillance cases[192] have decided the standing issue in favor of the plaintiff. In Riggs v. City of Albuquerque,[193] the 10th Circuit reversed the District Court based only on this pleading by the plaintiff: "Defendants' (investigative) actions and those of their agents have caused and continue to cause a chilling effect on plaintiffs' first amendment association and free expression rights, the effect of which causes harm to plaintiffs beyond subjective fear, including but not limited to injury to personal, political, and professional reputations" (emphasis in original).[194] The opinion does not indicate how this injury supposedly occurs, or what proof, if any, the plaintiff was required to submit.

Preferably, physical security intelligence operations should be conducted in a manner that makes it difficult for plaintiff to demonstrate standing. A

case that is disposed of on standing grounds is a case that requires no discovery or extensive litigation.

The current physical security intelligence regulations can be modified in two ways to make standing more of a hurdle. First, surveillance operations can be conducted in a more covert manner. Second, more restrictions can be placed on the dissemination of information that is collected and retained.

The current regulations are generally silent on whether an investigative activity should be overt or covert. When a distinction is made, however, the regulations favor overt investigation.[195] Although Congress has expressed a general preference for open government,[196] covert physical security intelligence operations have several advantages.

First, a person who is unaware of the investigation may never realize that he (or she) is a potential plaintiff.

Second, if the investigation is discovered only after the activity being investigated (e.g., the demonstration) is completed, any standing may be limited to a claim for damages and expungement of

files. An injunction against future surveillance activity may be beyond the plaintiff's reach.[197]

Third, the overt presence of investigators may aggravate the chilling injury. As third parties become aware that certain persons are under surveillance, the third parties may refuse to become involved with the targeted persons out of fear of similar government attention. Alternatively, third parties currently involved with targeted persons may terminate the existing relationships (including employment) on the theory that the targeted persons wouldn't be subject to government investigation unless there was something wrong. Overt surveillance may be used as a tool to deter lawful political activity, and courts may view overt military surveillance as evidence of a bad faith purpose instead of a good faith physical security purpose.[198] Evidence of bad faith makes it more likely that a court will find standing.[199]

Surveillance can become "overt" in various ways, with negative results for the investigators. Several cases cite the purposeful transfer to third parties of information gained through surveillance as unreasonable.[200] Another case cites the purposeful

transfer, without lawful purpose, of the fact that plaintiffs were targets of police surveillance as sufficient to create standing.[201] In another case, Paton v. LaPrade,[202] a high school student working on a school project sent for some information from the Socialist Workers Party (SWP). The FBI received the student's name from the postal service pursuant to a standing mail cover[203] on SWP mail. An FBI agent went to her school and spoke with the principal and vice-principal, at which point the FBI discovered plaintiff's educational purposes and apparently decided to close the case. "News of the investigation spread through her school, her community, and the country."[204] Based in part on her newfound notoriety, the student filed a claim against the FBI for violation of first amendment rights through stigmatization, even though there was no evidence that the FBI had done anything beyond talking with the two school officials. On appeal of the District Court's grant of summary judgment for the FBI, the Court of Appeals found that the plaintiff's allegations were sufficient and remanded for additional proceedings. The Paton case indicates both the importance, and the difficulty, of

keeping an operation covert.

The fourth and final reason to use overt surveillance in lieu of covert surveillance is the affect of overt surveillance on the physical security threat. Surveillance that deters lawful political association may not be a like deterrent on significant security threats. Overt surveillance may simply alert the criminals and make them more careful in their planning.

Current physical security intelligence regulations also provide for wide latitude in what information can be stored and how it can be used. There are no real distinctions made between personal and other information.[205] Files are reviewed annually based on a relevance standard, and the local commander has great discretion over what to retain.[206] The information is widely available within the federal government and elsewhere for employment and other considerations unrelated to physical security.[207]

As indicated by SWP, Meese and lower court decisions,[208] the mere possibility that future employment opportunities will be damaged by information disseminated by the surveilling agency may provide

standing. Consideration should be given to restricting the use of physical security intelligence to security purposes, and destruction of collected data once the immediate threat is passed.[209]

These considerations are incorporated into the proposed draft DoD Directive 5200.27 (appendix A), discussed in Section VII below.

B. Substantive First Amendment Claim.

As the previous section indicates, a grant of summary judgment to the defendant for lack of standing is no longer assured. Challenges to government investigations, including physical security intelligence operations, are likely to reach the merits.

Almost all first amendment claims involve some form of chill injury, but it arises in different ways.

The most common claim involves a specific statute that prohibits or requires some form of conduct. The plaintiff wants to do something that is protected by the first amendment but the statute operates to "chill" him from his desired activity.[210]

A different type of chilling injury derives from the government's collection of information on an activity that is unusual or unorthodox. In this latter category, there are many Supreme Court cases that examine the limits of legislative power to investigate alleged subversive activities. All these legislative investigation cases, however, involve some direct

application of government power to force cooperation, usually in an effort to obtain membership lists or other evidence of association[211].

Finally, there are the "pure surveillance" cases, or cases which involve government collection of information but no government projection of regulatory, proscriptive, or compulsive power. Physical security intelligence operations are pure surveillance cases. Unfortunately, court decisions providing detailed analytical guidance for pure surveillance cases are few. For this reason, analysis begins with recent, more general, pronouncements on first amendment methodology.

In Texas v. Johnson,[212] a 1989 case, the Court reversed a criminal conviction under a state statute prohibiting flag desecration.[213] The Johnson Court set forth a general methodology for analyzing first amendment claims.

The first step is to determine whether the challenged regulation or activity impacts on "expressive conduct,"[214] as distinguished from "nonexpressive conduct." If the only impact is on nonexpressive conduct, there is no First Amendment

issue. Plaintiff's allegation of chill from physical security operations will surely include the alleged chill of "expressive conduct."[215]

The next juncture is crucial. "If [plaintiff's] conduct [is] expressive, we next decide whether the State's [activity] is related to the suppression of free expression .... [I]f the State's [activity] is not related ..., then the less stringent standard we announced in United States v. O'Brien for regulations of noncommunicative conduct controls."[216] If an activity or regulation is categorized as "related to suppression," the activity will be subjected to "the most exacting scrutiny."[217] Avoidance of such a strict scrutiny review is important to the survival of a regulatory scheme.[218]

The activity is "related to suppression" if it is expressly directed at the communicative part of the conduct or if it is otherwise undertaken because of the communicative element.[219] The former situation is usually clear from the language of the regulation (or other authority) under which the action is taken, while the latter requires an analysis of the actor's specific motivation.[220] Physical security intelligence

regulations must be carefully crafted to ensure that they neither allow for, nor create the appearance of, improper motivation on behalf of those who implement the regulations. Unfortunately, the existing regulations are not satisfactory in this regard.

The regulations are doubtless intended to be content neutral: regardless of the politics of those protesting, the focus of any investigation should be on acts that directly affect the security of DoD personnel, property, and functions. The regulations are written in such a way, however, that a decisionmaker could authorize an investigation, in whole or part, based on the message of the protestors. Failure to limit the discretion of the decisionmaker can be fatal.[221]

AR 380-13 provides that physical security intelligence operations may only be commenced "if there is a reasonable basis to believe that ... demonstrations immediately adjacent to Army installations ... are of a size or character ... that they are likely to interfere with the conduct of military activities."[222] None of these terms are defined. An official could conclude that "interference

with military activities" is limited to the possibility of physical penetration of the post. He could also reason that the phrase includes the obstruction of military traffic after it leaves post. Unfortunately, he could also reason that "interference with military activities" includes interference with the image or the performance of the military in a less direct way. For example, demonstrations that are near the post will be observed and overhead by some soldiers, and the anti-war message might be overheard by some soldiers and thus damage morale. This last interpretation is one related to speech (i.e., the demonstrator's message) and not to conduct (e.g., blockage of a convoy). Such an interpretation, or even the possibility of such interpretation, could place a physical security collection operation under "strict scrutiny" review.

A related problem afflicts both DoD 5200.27 and AR 380-13. The following is a separate justification for collection of information on nonaffiliated persons: "Subversion of loyalty, discipline, or morale of DoD military or civilian personnel by actively encouraging violation of law, disobedience of lawful order or regulation, or disruption of military activities."[223]

Buried in this sentence is the following justification: "Subversion of ... morale ... by actively encouraging ... disruption of military activities." Again, the meaning of these terms is uncertain, with the potential for misinterpretation and misapplication.[224]

The vagueness of both AR 380-13 and DoD Dir. 5200.27 is exacerbated through the use of the following language: "No information shall be acquired about a person or organization solely because of lawful advocacy of measures in opposition to U.S. Government policy ...."[225] This language implies that lawful advocacy, although not permitted as the sole reason for collecting information, may be a reason for an operation (emphasis added). Hence the approval authority may base a decision to investigate in part on the demonstrators' message and in part on their medium (e.g., a protest outside the gate). Two federal courts have struggled in interpreting similar language and have been unable to agree on its meaning.[226]

The "lawful advocacy" language creates additional confusion within these regulations. "Active encouragement of ... disruption of military activities" is a separate justification for collection operations,

but such a justification, if used, would be equivalent to an authorization based "solely on lawful advocacy." In Brandenberg v. Ohio,[227] the Supreme Court considered an Ohio statute that criminalized "advocating ... the duty, necessity, or propriety of crime ... or other unlawful methods ... as a means of accomplishing ... political reform."[228] The Court held that the government could not criminalize such advocacy, even advocacy of illegal activity, except where such advocacy "is directed to inciting or producing imminent action and is likely to produce such action." But the current regulations fail to spell out this important caveat, rendering further misapplication of the "actively encouragement of ... disruption of military activities" a likely occurrence.

If an activity is conducted for a properly defined, speech neutral purpose, Johnson indicates that analysis continues under the "less stringent" standard of United States v. O'Brien.[229] O'Brien burned his draft card in protest of the draft and was prosecuted under a statute that made knowing destruction or mutilation of a draft card a criminal offense. The Court concluded that the conduct in question (burning the card) was expressive

conduct; and that the statute, at least on its face, was speech neutral. The Court then stated the following:

> To characterize the quality of the government interest which must appear, the Court has employed a variety of descriptive terms: compelling; substantial; subordinating; paramount; cogent; strong. Whatever imprecision inheres in these terms, we think it clear that a government regulation is sufficiently justified if it is within the constitutional power of the government; if it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.[230]

A slightly different, and more succinct, methodology was set forth in a subsequent Supreme Court decision: Clark v. Community for Creative Nonviolence [hereinafter Clark v. CCNV].[231] In Clark v. CCNV, the Court considered the constitutionality of park service

regulations banning overnight camping as they applied to protest groups who wanted to emphasize the plight of the homeless by sleeping overnight in Lafayette Park. Citing O'Brien, the Court stated that "symbolic expression of this kind may be forbidden or regulated if the conduct itself may constitutionally be regulated, if the regulation is narrowly drawn to further a substantial government interest, and if the interest is unrelated to the suppression of free speech."[232] Clark v. CCNV is particularly important as a weather vane of Supreme Court movement on substantive first amendment law, as the case is relatively recent (1984) and represents a consensus of seven justices, including all those justices who dissented in Johnson. Both O'Brien and Clark v. CCNV emphasize the government purpose as a paramount consideration, and, if the regulation is focused on the government purpose, consider any attendant abridgement of first amendment rights as secondary. In fact, the cases, particularly Clark v. CCNV, suggest that the degree of impact on first amendment rights borders on the irrelevant. The O'Brien test does mention incidental effect on the first amendment; the Clark v. CCNV test doesn't refer

to the amendment at all. The majority in Clark v. CCNV refused to consider various proposed alternative regulations that might have had less impact on first amendment protected expression, stating only that "respondents do not suggest that there was, or is, any barrier to delivering to the media, or to the public by other means, the intended message concerning the homeless."[233]

Chilling injuries are different, however, in character than the injuries suffered when a specific form of expression or expressive conduct is denied. A chill injury does not affect the mode of transmission of a message, but affects the speaker or the audience directly. If one party is afraid to listen or associate with another party, there may be no effective means of transmission. The issue becomes whether this difference is sufficient to alter the first amendment analysis. The answer is probably not.

A survey of the few court challenges to "pure" surveillance activities is now appropriate. The first significant surveillance case is Local 309, United Furniture Workers, C.I.O., v. Gates [hereinafter Gates],[234] decided in 1949 by the District Court for the

Northern District of Indiana. A labor union, Local 309, was involved in a contentious strike that, on occasion, resulted in acts of violence. The union held its regular meetings in the county courthouse. Members of the local police, generally considered unfriendly to the union, openly attended the meetings and took notes. The police would not leave when asked. When the union filed suit to enjoin the police surveillance, the police asserted an interest in preventing violence, both at the meetings and at the strike locations. On the basis that there was no evidence supporting a connection between the violent acts and the union or its meetings, the court enjoined the police from further attendance at the meetings. The standard of review chosen by the court, citing the Supreme Court in Thomas v. Collins,[235] was the then prevailing strict scrutiny standard: "Any attempt to restrict those liberties [secured by the first amendment] must be justified by clear public interest, threatened not doubtfully or remotely, but by clear and present danger."[236] It was unclear whether the Gates court accepted the police justification - the prevention of violence - at face value, or whether it decided the

case on the presumption of improper motive.[237] If the Gates court accepted that the police surveillance was good faith, then applying the strict scrutiny standard of Thomas was arguably incorrect as the Thomas case involved a direct restraint on speech.[238] In any event, the Gates court may have managed to associate the strict scrutiny test with some surveillance chill claims. Since Gates, two state courts[239] have used the strict scrutiny analysis in discussing pure chill cases, but in both cases the courts also found that the government investigation was not properly defined in terms of legitimate purpose or scope.[240]

Two Supreme Court cases which found standing in connection with chill injuries provide some insight into how the Court will analyze chill claims on the merits. In Socialist Workers Party v. Attorney General,[241] Circuit Justice Marshall considered the merits of a requested injunction that would keep the Federal Bureau of Investigation from conducting surveillance at the Young Socialist Alliance' annual convention. The YSA had formally renounced the use of violence, but the FBI was still concerned about a minority faction, the "Internationalist Tendency,"

which espoused violence and was seeking to take control of the YSA. The convention was open to the public, and the FBI planned to use confidential informants at the convention to record identities of participants and take notes on the substance of their remarks. No photographic or electronic surveillance, or searches of any kind, were planned, and information collected was only available within the government. The plaintiffs alleged the presence of the FBI informers chilled their associational and speech rights. The District Court[242] granted the injunction, citing Gates and the fact that the FBI was unable to produce any evidence connecting the YSA to violence or illegal activity during the past 34 years. The Court of Appeals stayed the injunction, except for the dissemination of information within the government to the agency responsible for federal employment,[243] citing a concern that plaintiffs probably would be unable to prevail on the merits due to lack of standing and the FBI's legitimate interest in the Internationalist Tendency.[244] The Court of Appeals concluded the evidence supporting the allegations of chill did not outweigh the harm caused to the FBI (the unmasking of its informants).

Justice Marshall affirmed the judgment of the Court of Appeals. He recognized the plaintiff's allegations as sufficient for standing, but accepted the balancing analysis employed by the Court of Appeals.[245] Four factors were weighed in the government's favor: the public nature of the event; the limited nature of the surveillance activity itself; the lack of activity intended to disrupt the convention, and the assurances that there would be no distribution of collected information to nongovernmental entities or to the Civil Service Commission. Marshall's holding implicitly rejected the application of a strict scrutiny standard to claims of chill,[246] at least where the extent or nature of the chill is uncertain.[247]

In Meese v. Keene,[248] the full Court was given an opportunity to classify a chill case under the strict scrutiny standard, but declined to do so. As discussed previously,[249] Keene challenged a federal statute that allowed for the labeling of certain films as "political propaganda," including some films that he wished to show. Keene said that he could not show the films because of damage to his reputation and career. The District Court[250] labeled the effect of the statute as

"censorship," which is arguably a correct description of an act which chills someone from delivering a message. The censorship label, however, categorized the case as a prior restraint. Prior restraints are subject to close scrutiny, and bear "a heavy presumption against (their) constitutional validity."[251] The District Court found the statute unconstitutional, and the Attorney General appealed the case directly to the Supreme Court. The Supreme Court refused, however, to place this chill claim in the prior restraint or censorship category.[252]

The factual basis for beginning an investigation has been a key consideration in pure surveillance cases. If an investigator has insufficient basis upon which to suspect that an investigation is warranted, a full and ongoing investigation will be deemed unreasonable. In Clark v. Library of Congress,[253] a bookshelver at the Library of Congress was subjected to a full FBI investigation based on his occasional attendance at meetings of the Young Socialist Alliance. Friends, family, and co-workers were interviewed. The investigators asked them personal questions about Clark. As a result, Clark's family pressured him to

give up his political activities, and Clark perceived that he failed to receive favorable consideration for several intra-library positions that he applied for subsequent to the investigation. The D.C. Circuit Court of Appeals held, where there was no apparent factual basis for an investigation other than legitimate political beliefs, the investigation was unlawful. In a recent decision, Alliance to End Repression v. City of Chicago,[254] a District Court enjoined the FBI from continuing an investigation into a political organization. The court concluded that the investigation was unreasonable because the original source of information was an informer whose credibility had never been verified.[255]

Unfortunately, the current physical security regulations present ample opportunity for attack based on the reasonableness of authorized investigative techniques. Other than the vague language about "lawful advocacy" previously discussed, DoD Dir. 5200.27 has no guidance concerning the type or quality of factual information necessary to support a physical security intelligence investigation. AR 380-13 is similarly silent, save for the doubly tenuous "Reasonably believe

... likely to [interfere with military activities]."[256]

As noted in the previous discussion of existing regulatory guidance, there is also a wide disparity amongst the regulations affecting physical security concerning the types of investigation techniques that may be used. Some of the techniques available under the more relaxed guidance have been attacked by courts considering pure surveillance cases, and need to be carefully considered. In addition, the guidance should be as uniform as possible, so that a legal attack on the lack of a restriction in one regulation cannot be supported by reference to another regulation that contains the restriction.

Taken as a whole, the cases support certain conclusions. Courts will decide pure surveillance cases based on the purpose and scope of the government's investigation. No court has ever held there was too much chill to overcome a proper government investigation conducted in a reasonable fashion. In particular, where the government satisfies its burden as to proper purpose, the Supreme Court refuses to apply strict scrutiny and will find for the government, at least where the plaintiff does

not make a strong showing of actual chill injury. Hence, if the government can show proper purpose and scope, and affirmative consideration to investigative techniques that reduce or avoid chill, the government will prevail. A draft directive that satisfies these requirements is located at appendix A and discussed in Part VII, below.

VII. ANALYSIS OF PROPOSED REGULATORY CHANGES

Both the current DoD Dir. 5200.27 (Appendix B) and AR 380-13 (Appendix C) need significant changes.[257] The thesis contains a proposed draft (appendix A) of a new DoD Dir. 5200.27. A new AR 380-13 can be created to reflect the changes in policy and detailed guidance contained in the draft DoD Directive 5200.27.[258] The following discussion is keyed to the paragraphs of the proposed draft of DoD Dir. 5200.27.

A. Reissuance and Purpose

This provision deletes reference to the "Defense Investigative Program." This program was established pursuant to DoD Directive 5200.26, Defense Investigative Program, February 17, 1971, which was cancelled, and not reissued, on 12 June 1979.

B. Applicability and Scope

Paragraph B.2.c. is new. The paragraph recognizes

that DoD should not employ unfettered collection operations just because a person or organization has some affiliation with the DoD, unless there is a connection between the information sought and the affiliation. For example, proposed surveillance of a contractor who participates in a political rally should be subject to the restrictions of DoD 5200.27 if the rally bears no reasonable connection to the contractor's work performance.

C. Definitions

There was no definitions paragraph in the old directive, and key terms need definition. The definitions are discussed as the terms are developed below.

D. Policy

No change.

E. Situations Warranting Collection

Subparagraph E.1., previously entitled "Protection of DoD functions and property," is entirely rewritten. The investigation and prosecution of crimes (a classic "law enforcement" function) is conceptually different from security, and is taken out of E.1. and placed at E.4. The Clark v. Community for Creative Nonviolence mandate that the regulation "further a substantial interest ... unrelated to free speech"[259] is employed in redrafting paragraph E.1.

A "substantial government interest" must be defined. The overriding mission of the military is to protect the nation against foreign aggression. The ability to defend against and deter foreign aggression can be defined as protection of "national security." Intelligence operations with a discernible connection to national security will satisfy the "substantial government interest" requirement. The definition of "national security" is included in paragraph B.

Certain threats, such as theft or destruction of property and violence to personnel, are specifically listed in paragraph E.1. because the impact of this type of activity on morale and readiness will always have some arguable connection to national security.

The investigation of threats involving use of force or violence is likely to be useful in the sense that it will spur local authorities, or even the FBI,[260] to preempt the act and void the threat.

The commander's authority on the installation, and authority to protect the installation, also justify physical security intelligence operations where physical invasion of the installation is suspected.[261]

Paragraph E.1. concludes with a "national security" catchall. A demonstration which affects the movement of nuclear and chemical weapons, for example, probably fits within the "national security" catchall; while a demonstration that simply slows everyday commuter traffic would fail to meet this standard. Even a peaceful demonstration that blocks or delays military traffic may fail the national security standard. In the worst case scenario, the result of a peaceful blockade is simply delay until the local authorities are called to clear passage. And, in this worst case scenario, an investigation is unlikely to produce anything of "national security" value. Confirmation of a planned blockade might be passed to the local authorities in the hopes that they will provide enough

manpower to clear the passage faster - with a net positive effect of reducing the delay. The key issue in each case will be whether the delay, in and of itself, has "national security" implications.

The proposed government action must be "... within the constitutional power of the government."[262] The importance of limiting action to "substantial government interests" is highlighted by this part of the Clark v. CCNV mandate. The authority of the military to interfere in civil affairs, discussed previously,[263] dissipates in proportion to the distance from the installation of attempted exercise. The military can always argue that it has the right to defend itself, no matter what the damage to individual first amendment rights. The argument is strongest, however, when limited to situations of a national security character.

The proposed government action must be "... unrelated to the suppression of free speech."[264] Paragraph E.1. is written so that only the actual threat of physical acts (theft, destruction, force, violence, unauthorized entry, physical disruption) justify investigation.[265] Whether the threat results

from a demonstration or other arguably political event is irrelevant, so specific references to demonstrations have been deleted. If information about subversion, or attempted subversion, is desired, it should be treated as a criminal matter or a personnel security matter, not as a physical security problem.[266]

F. Collection Procedures

The Clark v. CCNV mandate that the regulation be "narrowly drawn"[267] is implemented here.

If the local authorities, law enforcement or otherwise, will provide the needed information, there is no need for an independent military investigation.

Approval authority should flow from the civilian leadership,[268] yet the existing regulations provide for emergency action by the commander without significant limits on the commander's discretion.[269] The proposed draft DoD Dir. 5200.27 provides that, even in an emergency situation, someone other than the local commander must consider the situation in detail and ultimately approve of the operation. In addition, the same approval standards should be used for judging a

proposed intelligence operation whether or not it is labeled "emergency."

If investigation is proposed based on an unverified or incredible source, the focus of the initial investigation will be on verifying the credibility of the source.[270]

If an activity can be restructured to avoid the potential reach of any perceived threat, no additional investigation is warranted. In the absence of some threat of entry onto the installation, for example, a peaceful demonstration which will not impact every available gate does not require investigation. The commander can simply use alternative gates.

The factual basis for collection is set forth in paragraph F.1.b. The reasonable suspicion standard is taken from Terry v. Ohio.[271] The reasonable suspicion standard in Terry provides a fairly objective standard that is developed, and will continue to develop, in the case law.

All references to "advocacy" and "lawful advocacy" are eliminated from the directive as unnecessary and confusing. One commentator,[272] citing Brandenberg v. Ohio,[273] argues that evidence of advocacy of illegal

conduct, where such advocacy falls short of the Brandenberg criminalization threshold, cannot provide a constitutional basis of support for initiating an investigation of a political organization. The thesis rejects the proposition that investigation based on advocacy of criminal conduct is unconstitutional.

Brandenberg set standards for the direct criminalization of speech, a legislative act which directly implicates the first amendment. A proper investigation, focused on some future physical act but initiated based on speech, is not a criminalization of speech such as that challenged in Brandenberg.

More importantly, the philosophic underpinning of Brandenberg limits its use as an analytic analogy in considering the constitutionality of investigative activities. By holding that advocacy of illegal conduct cannot be criminalized unless combined with direct incitement to imminent illegal conduct and a reasonable likelihood that such illegal conduct would come about, the Brandenberg Court was attempting to create a breathing space between speech which is clearly protected by the first amendment and speech which can be criminalized. Speech in this breathing

space, which might include advocacy of criminal conduct without an immediate prospect of harm, is not itself constitutionally favored; it just cannot be criminalized for fear that truly protected speech (e.g., a discussion of communist and marxist ideology) will be chilled if the speaker has to agonize over the definition of "advocacy."[274] To the extent a physical security intelligence investigation is initiated in or around speech in the Brandenberg breathing space (e.g., mere advocacy of illegal conduct), the chill does not directly impact constitutionally favored speech. Further, since the chill of an investigation is less than that of a criminal prosecution, any indirect impact on constitutionally favored speech (e.g., a discussion of U.S. military policy) is attenuated.

Definitions of lawful advocacy and proper breathing space are too abstract for meaningful guidance. The proposed directive combines the reasonable suspicion requirement with an imminent harm requirement that focuses the investigation on real time threats. Even if investigation is based solely on "advocacy," lawful or otherwise, the reasonable suspicion and imminent harm requirements should satisfy any constitutional

challenge based on Brandenberg.

Paragraphs E.1.f. and E.1.g. of the draft DoD Directive restrict the range of available investigative techniques. The restrictions are based on the following balance: if a given technique is not absolutely necessary for real time physical security requirements, the amount of chill the technique might cause is weighed against the investigative value of the technique. The restrictions chosen also bring DoD 5200.27 closer in substance to the restrictions in the intelligence component regulations: DoD Reg. 5240.1-R and AR 381-10.

The draft directive favors covert surveillance over overt surveillance. As previously discussed,[275] covert surveillance is preferred from the standpoint of reducing any chill injury.

The draft directive favors the use of publicly available sources of information. The courts have approved of investigations limited to public meetings and public sources.[276]

The draft directive places limits on the use of informers who are officers of the targeted organization.. The cases have not disapproved of the

use of informers or infiltrators per se,[277] but if the informer is an officer of the group investigated, the courts may imply some internal interference beyond the scope of a reasonable investigation.[278]

The draft directive prohibits the use of any device that records video or audio data in permanent form.[279] Consider a hypothetical rally involving a homosexual group protesting military personnel policies outside a military installation. A man in uniform is observing the proceedings. The man may not be particularly threatening; perhaps he is a policeman there simply to keep order should a disturbance break out. The policeman suddenly picks up a camera or a videotape recorder and starts taking pictures of people at the demonstration. The chill factor would increase markedly as attendees wondered who the man was and why he was taking photographs. Interest in the activities of the group would probably cool for those who were afraid of being personally associated with the group or its message.

Contrast the effect of photography with the need for it. While a permanent record may be useful in a future law enforcement proceeding, it is of only marginal

value to an investigation intended to discover and counter a real-time security threat. Audio recording devices are of similarly limited value, although they are a little less invasive because they only record the speaker (and not the listener) and the speaker is not necessarily identifiable from the tape.

The draft directive contains a ban on direct participation in a search, seizure, or arrest to emphasize the minimum requirements of the Posse Comitatus Act.[280]

Overt physical surveillance is particularly intimidating. There is no reason, however, to restrict covert physical surveillance operations.

Collection procedures for personnel security operations, operations related to civil disturbances, and criminal investigations or prosecutions for which DoD has responsibility (paras G.2. through G.4, respectively) may be the same. These topics are beyond the scope of the thesis.

H. Retention of Information.

This paragraph sets out a very restrictive approach

to the retention of information. There are strong arguments that the Privacy Act ban on the collection of information describing the exercise of first amendment rights applies to physical security intelligence operations.[281] There are several cases that focus negatively on the possibility that personal information gathered during the course of political surveillance might become public or otherwise be used for unrelated purposes within the government.[282] In fact, blanket routine uses of the USAINSCOM Intelligence Files and Local Criminal Information Files, where physical security intelligence information is likely to be, include release within the government for purposes of hiring, firing, contracting, obtaining a security clearance, etc..[283]

The draft directive requires that, whenever possible, personal information be summarized to nonpersonal form. Such summarization renders the Privacy Act inapplicable.[284] The draft directive forbids the collection or retention of certain information, including personal financial, educational, sexual, and religious information. This information is largely irrelevant to real-time physical security

requirements, and the lack of such information makes it more difficult for a plaintiff to show "adverse effect"[285] or to claim that the directive is not "narrowly drawn."[286] Finally, all information which is collected must be reviewed every 90 days, and personal information may only be retained if the subject is still an imminent threat to national security.

Another alternative, which is not employed in this draft directive, would be to create a new "physical security intelligence" systems of records, with no use or dissemination except to other law enforcement agencies, and even then only when necessary to avert immediate harm or to facilitate ongoing physical security operations.

Finally, the directive should be published in the federal register. Publishing will put the potential plaintiff on notice of when the military might initiate surveillance. Armed with such notice, the plaintiff can structure his protest or activities without incurring any military investigation or any attendant chill. As the Supreme Court implied in Clark v. Community for Creative Non-Violence,[287] the existence of any alternative way to communicate a message, even if

not the plaintiff's preferred way of communication, will defeat an attack on an otherwise proper exercise of government power.

VIII. CONCLUSION

Anti-war and anti-military demonstrations have occurred during every modern conflict. When such demonstrations are anticipated outside an installation, the commander wants to know as much as possible about the demonstrators and any potential threat to installation facilities, personnel, or operations. Unfortunately, the Army's internal procedures for obtaining such information are confusing and contradictory. As a consequence, commanders may illegally collect and retain information and subject the Army to litigation and poor publicity.

By linking physical security intelligence investigations to specific national security interests, by connecting specific threats to the interest affected, by setting threshold information requirements for triggering investigations, and by using carefully drawn standards of retention and use, the regulations can become "narrowly drawn to further substantial government interests ...that are unrelated to the suppression of speech."

This approach ensures that both the requirements of

the Privacy Act and the First Amendment are satisfied, without sacrificing the flexibility the commander needs to carry out essential missions.

[1] Communications Association v. Doud, 339 U.S. 382, 445 (1950)(Jackson, J., concurring and dissenting).

[2] The staff officer responsible for military police functions on the installation.

[3] The thesis assumes the installation commander is also the commander of a collocated combat unit, and the G-2 is the staff officer responsible for intelligence and security in a combat unit. If there is no collocated combat unit, the installation commander will have a specific staff section responsible for security (e.g., the DEPSEC). The legal analysis remains constant regardless of how the staff section responsible for security is labeled.

[4] See Eric Lardiere, Comment, Justiciability and Constitutionality of Political Intelligence Gathering, 30 UCLA L. Rev. 976, 979 (1983); Howard and Crowley, Pleading, Discovery, and Pretrial Procedure for Litigation Against Government Spying, 55 U. Det. J. Urb. L. 931, 932-939 (1979). See The Privacy Act of 1974, 5 U.S.C. § 552a (1988); The Freedom of Information Act, 5 U.S.C. § 552 (1988); Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2511 (1988) (creates civil cause of action for certain intercepts and uses of oral and wire communications).

[5] The Privacy Act of 1974, 5 U.S.C. § 552a (1988).

[6] "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the rights of the people to assemble, and to petition the Government for a redress of grievances." U.S. Const. amend. I.

[7] "No evidence linking these movements to foreign powers was found ...." Morton H. Halperin et. al., The Lawless State: The Crimes of the U.S. Intelligence Agencies 163 (1976) (referring to the civil unrest of the 1960s). No evidence was ever uncovered that the various protests and demonstrations of the 1960s were interconnected by any sort of conspiracy, either foreign or domestic. Subcommittee on Constitutional Rights, Senate Committee on the Judiciary, 93d Cong., 1st Sess., Report on Military Surveillance of Civilian Politics 5 (Comm. Print 1973)[hereinafter Report on Military Surveillance].

[8] Army Reg. 190-13, The Army Physical Security Program, Glossary (20 June 1985)[hereinafter AR 190-13].

[9] "Affiliation" includes almost any voluntary relationship with the military. See Army Reg. 380-13, Acquisition and Storage of Information Concerning Non-Affiliated Persons and

Organizations, Glossary of Terms (30 Sept. 1974)[hereinafter AR 380-13].

[10] Military Surveillance: Hearings on S.2318 Before the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary, 93d Cong., 2d Sess. 169 (1974)[hereinafter Hearings on Military Surveillance](statement of Joan M. Jensen, Professor, University of San Diego). Ms. Jensen's views were largely adopted by the Subcommittee on Constitutional Rights. See Report on Military Surveillance, supra note 7, at 10-20.

[11] Presidential Directive (June 26, 1939)(untitled), reprinted in 1 Allan Kornblum, Intelligence and the Law, C-3 (Defense Intelligence College Course Textbook SM625/SM629, 1985)[hereinafter Kornblum].

[12] Presidential Directive (September 6, 1939)(untitled); Presidential Directive (January 8, 1943)(Police Cooperation); and Presidential Directive (July 24, 1950)(Information Relating to Domestic Espionage, Sabotage, Subversive Activities, and Related Matters); all reprinted in Kornblum, supra note 11, at C-3 and C-4. Subsequent agreements between the FBI and the Military Intelligence services indicated that the FBI "has jurisdiction over all civilians insofar as espionage, counterespionage, subversion and sabotage are concerned, regardless of employment."

Delimitations Agreement Between the FBI and U.S. Military Intelligence Services, paragraph 3-2 (February 23, 1949)(with supplements), reprinted in Kornblum, supra note 11, at B-49. None of the quoted terms were defined in the documents. A 1979 agreement between the DoD and the FBI in 1979 superceded the delimitations agreement, but discussed only jurisdiction over foreign-based threats and did not otherwise discuss responsibility for "subversive" activities. Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation § 1 (April 5, 1979), reprinted in Kornblum, supra note 11, at B-52.

[13] See, e.g., Exec. Order No. 10,450, 18 Fed. Reg. 2489 (1953)(Security Requirements for Government Employment).

[14] Predecessor to the Department of Defense.

[15] At various times groups such as the Quakers and the Southern Christian Leadership Conference were monitored. Report on Military Surveillance, supra note 7, at 71. Specific persons listed in the intelligence files included Martin Luther King, Jesse Jackson, and Joan Baez, among others. Id. at 79.

[16] C. Pyle, CONUS Intelligence: The Army Watches Civilian Politics, 1 Washington Monthly, Jan. 1970, at 4. Mr. Pyle also

wrote a follow-up article: C. Pyle, CONUS Revisited, The Army Covers Up, 1 Washington Monthly, July 1970, at 49.

[17] Report on Military Surveillance, supra note 7.

[18] Id. at 7.

[19] Id. at 102-16.

[20] Citing U.S. v. O'Brien, 376 U.S. 367, 377 (1968) as the source of constitutional analysis. Report on Military Surveillance, supra note 7, at 115. O'Brien is discussed in further detail infra notes 229-30 and accompanying text.

[21] Report on Military Surveillance, supra note 7, at 5.

[22] Hearings on Military Surveillance, supra note 10, at 178-80 (statement of Professor C. Pyle).

[23] Report on Military Surveillance, supra note 7, at 42.

[24] Id. at 9, 108-09.

[25] Tatum v. Laird, 444 F.2d 947 (D.C. Cir. 1971).

[26] Laird v. Tatum, 408 U.S. 1 (1972).

[27] Justice Rehnquist voted with the majority in the reversal of the Court of Appeals' decision. Previously, Attorney General Rehnquist had defended the Army's intelligence program through personal testimony before the Congress. Justice

Rehnquist, however, refused to recuse himself from the Laird case. Hearings on Military Surveillance, supra note 10, at 90 n.3 (statement of John F. Shattuck, National Staff Counsel, American Civil Liberties Union).

[28] ACLU v. Laird, 463 F.2d 499 (7th Cir. 1972), cert. denied, 409 U.S. 1116 (1973).

[29] Report on Military Surveillance, supra note 7, at 84-88.

[30] The subject of the letter was "Counterintelligence Activities Concerning Civilians not Affiliated with the Department of Defense." The letter is discussed, but not reprinted, in Report on Military Surveillance, supra note 7, at 92.

[31] S.2318, 93d Cong., 1st Sess. (1973).

[32] The exceptions were limited to specific civil disturbance, physical security, and personnel security situations. Id. at § 2(b). The physical security exception covered investigations of "criminal conduct committed on a military installation or involving the destruction, damage, theft, unlawful seizure, or trespass of the property of the United States ...." Id. at § 2(b)(2).

[33] Hearings on Military Surveillance, supra note 10, at 103-24 (statement by David O. Cooke, chairman, Defense Investigative Review Council).

[34] In fact, the two key military regulations (Dep't of Defense Directive 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense (Jan. 7, 1980)[hereinafter DoD Dir. 5200.27] and Army Reg. 380-13, Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations (30 Sep. 1974)[hereinafter AR 380-13]) are largely or entirely unchanged since the early 1970s. See discussion infra notes 36-45 and accompanying text.

[35] 5 U.S.C. § 552a (1988).

[36] (January 7, 1980)[hereinafter DoD Dir. 5200.27].

[37] (30 Sept. 1974)[hereinafter AR 380-13].

[38] (1 July 1984)[hereinafter AR 381-10].

[39] DoD Dir. 5200.27, for example, only discussed demonstrations occurring on-post while the Army policy letter included demonstrations immediately adjacent to post.

[40] AR 380-13, for example, retained the language about demonstrations immediately adjacent to the post. Additionally,

AR 380-13 was not applicable to criminal investigations while DoD Dir. 5200.27 was applicable to criminal investigations. See discussion infra note 49 and accompanying text.

[41] 50 U.S.C. §§ 1801-11 (1988).

[42] Exec. Order No. 12,036, 43 Fed. Reg. 3674 (1978)(United States Intelligence Activities). Exec. Order 12,036 was superceded by Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (1981)(United States Intelligence Activities).

[43] Dep't of Defense Directive 5240.1, Activities of DoD Intelligence Components that Affect U.S. Persons (November 30, 1979)(cancelled and reissued December 3, 1982; cancelled and reissued April 25, 1988)[hereinafter DoD Dir. 5240.1]; Dep't of Defense Reg. 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons (December 1982)[hereinafter DoD Reg. 5240.1-R].

[44] AR 381-10 was initially issued on 15 February 1982 and subsequently reissued 1 July 1984.

[45] For example, AR 381-10 now controls and limits the activities of all counterintelligence units. Language in AR 380-13, however, apparently delineates the functions of

counterintelligence units in a situation involving a demonstration. AR 380-13, para. 6a(4).

[46] AR 190-13, para. 1-5q(1).

[47] Army Reg. 190-30, Military Police Investigations, para. 3-14a(4) (1 June 1978)[hereinafter AR 190-30].

[48] AR 190-30, para. 3-18a; Army Reg. 190-45, Law Enforcement Reporting, para. 2-6a (30 Sept. 1988)[hereinafter AR 190-45](discussion of purpose of criminal information program).

[49] Counterintelligence is defined as "activities, both offensive and defensive, designed to detect, neutralize or destroy the effectiveness of foreign intelligence activities." AR 380-13 at A-2. Since the thesis assumes no foreign connection, the argument can be made that any military police activity for physical security purposes is "not counterintelligence related," and is therefore within the exception to AR 380-13. Physical security operations may also be considered as a form of crime prevention, and crime prevention activities are specifically excluded from AR 380-13. AR 190-30, para. 3-18a.

AR 190-45, however, states that AR 380-13 is applicable to the retention and disposition of information acquired by military

police, and implies that AR 380-13 is also applicable to the acquisition of such information. AR 190-45, paras. 2-4 and 2-6.

[50] DoD Dir. 5200.27, para. D.1.

[51] Id., para. E.2.

[52] Id., para. E.1.

[53] AR 190-30, para. 3-18a.

[54] Army Reg. 340-21, The Army Privacy Program, para. 4-5 (5 July 1985)[hereinafter AR 340-21]. This language is taken verbatim from the Privacy Act of 1974, 5 U.S.C. § 552a(e)(7) (1988), and discussed in detail infra notes 102-35 and accompanying text.

[55] DoD Dir. 5200.27, para. C.3.

[56] Id., para. E.5.

[57] Id., para. B.

[58] Id., para. E.4.

[59] Id., para. E.6.

[60] Id., Enclosure 1, para. D.

[61] Id., para. E.6.

[62] Id., para. F.4.

[63] AR 380-13, para. 8, implies that certain information may be retained beyond 90 days. The application of AR 380-13 to military police, however, is uncertain. See discussion supra note 40 and accompanying text.

[64] Although DoD Dir. 5200.27 excludes "DoD intelligence components," the staff G-2 is not such a component. DoD intelligence components are defined via a specific listing of intelligence units and commands, along with a catch-all for other staffs and organizations when used for "foreign intelligence or counterintelligence purposes." Dep't of Defense Directive 5240.1, DoD Intelligence Activities, para. 4 (April 25, 1988)[hereinafter DoD Dir. 5240.1]. Both foreign intelligence and counterintelligence are specifically limited to operations involving foreign powers or international terrorists. DoD Dir. 5240.1, paras. 3 and 4. The staff G-2 is not one of the specifically listed intelligence units or commands, and the thesis assumes no foreign connection. For similar reasons, Exec. Order No. 12,333, 46 Fed. Reg. 59941 (1981)(U.S. Intelligence Activities), and Army Reg. 381-10, U.S. Army Intelligence Activities (1 July 1984)[hereinafter AR 381-10], are inapplicable.

[65] AR 380-13, para. 6a.

[66] Id., para. 6a(3).

[67] Id., para. 9a.

[68] Id., para. 6c(2).

[69] AR 340-21, para. 4-5.

[70] AR 380-13, para 6b. Reference is made to Army Regulation 381-130, which was superceded by AR 381-20 in September, 1975.

[71] AR 380-13, para. 6b.

[72] AR 380-13, para. 9c.

[73] AR 380-13, para 9d. The DIRC was established by Dep't of Defense Directive 5200.26, Defense Investigative Program (February 17, 1971). This directive was cancelled on June 12, 1979, and the DIRC no longer exists.

[74] AR 380-13, para 9e.

[75] Id., para 6e.

[76] DoD Dir. 5200.27, para. F.4.

[77] AR 380-13, para. 8b.

[78] See discussion supra note 64 and accompanying text.

[79] AR 381-10 does not apply to "law enforcement activities,

including civil disturbances, that may be undertaken by DoD intelligence components." AR 381-10, para. A.3. The definition of "law enforcement activities" ("Activities undertaken for the purpose of detecting violations of law or to locate and apprehend persons who violate the law ...." (AR 381-10, Appendix A, para. 18)), along with the remaining language of para. A.3., indicates that security measures taken prior to the commission of an actual criminal act would not be "law enforcement activities."

[80] DoD Dir. 5200.27, para. B.3.; AR 380-10, para. 2. Although AR 380-13 specifically discusses the role of the local counterintelligence liaison unit, to the extent this role is inconsistent with the provisions of AR 380-10 (a more recent regulation), the provisions of AR 380-13 are inapplicable.

[81] AR 381-10, Procedure 2, para C.7. Army Reg. 381-20, U.S. Army Counterintelligence Activities, para. 2-2(f)(2) (27 Oct. 1986)[hereinafter AR 381-20] provides that "Army CI may take investigative actions necessary to ... protect the security of Army installations, information, functions, activities, and installations."

[82] AR 381-20 goes beyond DoD intelligence directives (i.e., Dep't of Defense Directive 5240.2, DoD Counterintelligence (June 6, 1983)[hereinafter DoD Dir. 5240.2] and DoD Dir. 5240.1)

in authorizing Army counterintelligence units to become involved in countering peacetime domestic terrorism. Compare AR 381-20, Glossary (definition of counterintelligence includes terrorism; terrorism not limited to foreign connection) and para. 3-2b(3) (specific counter-terrorism role) with DoD Dir. 5240.2, para. C.1 (definition of counterintelligence activities that implies a requirement for a foreign connection or, if none, a period of war).

[83] AR 381-20, Glossary, at 22.

[84] AR 381-10, Procedure 2, para. A.

[85] Id., Procedure 2, para. D.

[86] Physical surveillance is defined as "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." Id., Procedure 9, para. B.

[87] Id., Procedure 9, para. C.1. Different criteria apply outside the continental United States.

[88] Id., Procedure 10, para C.1a. This provision limits undisclosed participation to that "essential to achieving a

lawful foreign intelligence or counterintelligence purpose." Without a foreign connection, there can be no such purpose. See DoD Dir. 5240.1. para. C.2 and C.3 (definitions of "foreign intelligence" and "counterintelligence").

[89] AR 381-10, Procedure 10, para. B.4.

[90] DoD Dir. 5240.1 is not applicable to domestic intelligence operations. However, AR 381-10 (implementing DoD Dir. 5240.1) adds the following language: "Information may be gathered by intelligence components using techniques described in procedures 5 through 10 for other than foreign intelligence or counterintelligence purposes ...." AR 381-10, Procedure 1, para. A.1. But AR 381-10, Procedure 5, part 1 discusses electronic surveillance procedures pursuant to the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-11 (1988), which has no relevance to physical security intelligence operations. The rest of AR 381-10, Procedure 5 also appears irrelevant to physical security intelligence operations.

[91] AR 380-10, Procedure 7. This procedure authorizes unconsented physical searches within the United States of active duty personnel for counterintelligence purposes, if and only if a military commander or judge has probable cause to believe that targeted persons are acting as agents of foreign powers.

[92] See Id., Procedure 8.

[93] See Joint Comm. on Gov't Operations, 94th Cong., 2d Sess., Legislative History of the Privacy Act of 1974, S.3418 (Public Law 93-579): Source Book on Privacy, at 5-6 [hereinafter Source Book on Privacy](Introductory Remarks of Senator Sam J. Ervin, Jr., on S.3418).

[94] 5 U.S.C. § 552a (1988).

[95] Section 552a(a)(5).

[96] Section 552a(e)(7).

[97] Section 552a(e)(1).

[98] Privacy Act System Number A0502.10aDAMI, reprinted in Dep't of Army, Pam. 25-51, The Army Privacy Program - System Notices and Exemption Rules, para. 6-7a (1 Oct. 1988)[hereinafter DA Pam. 25-51]. This system of records is located at INSCOM headquarters with "decentralized segments" at "groups, field stations, battalions, detachments, and field officers (sic) worldwide." Categories of individuals covered specifically include "individuals about whom there is a reasonable basis to believe that they are engaged in, or plan to engage in, activities such as (1) theft, destruction, or sabotage of ... equipment (or) facilities ... (2) demonstrations on active ...

installations or immediately adjacent thereto which are of such character that they are likely to interfere with the conduct of military operations." Id, para. 6-7b. The relevant purposes are "to provide authorized protective service; and to conduct counterintelligence and limited reciprocal investigations." Id., para. 6-7e. The information may be collected from various sources, including the interview of individuals who have knowledge of the subject's background and activities or "other individuals deemed necessary." Id., para. 6-7l. The records are maintained on microfiche. Id., para. 6-7g. The only instructions on retention and disposal apply to personnel security investigative files. Id, para. 6-7g(4). The only applicable routine uses are "to provide information for ongoing security and suitability investigations ..." or to "assist federal agencies in the administration of criminal justice and prosecution of offenders." Id., paras. 6-7f(9) and f(10).

[99] Privacy Act System Number ID-A0503.06aDAMI, reprinted in DA Pam. 25-51, para. 6-9. This system of files is located at the same locations as the USAINSCOM investigative files. The same information relevant to individuals involved in demonstrations may be retained. The categories of records in the system appear to be limited, however, to those records with some foreign connection. Id., para 6-9c.

[100] Privacy Act System Number ID-A0509.21DAPE, reprinted in DA Pam. 25-51, para. 6-25. This system of records covers "any citizen or group of citizens suspected or involved in criminal activity directed against or involving the United States Army." Id., para. 6-25b.

[101] Personal notes which are not kept private are considered to be agency records subject to the Privacy Act. See Bowyer v. U.S. Dept. of Air Force, 804 F.2d 428, 431 (7th Cir. 1986); Boyd v. Secretary of the Navy, 709 F. 2d 684 (11th Cir. 1983); Chapman v. National Aeronautic and Space Administration, 682 F.2d 526, 529 (5th Cir. 1982).

[102] Section 552a(e)(7).

[103] The other two exceptions are for information gathered under express authorization of statue or with the consent of the subject individual. § 552a(e)(7). "I know of no existing or enforceable statute which expressly and generally authorizes any particular agency to maintain ... records of political or religious activities ...." 120 Cong. Rec. 36,650 (1974)(statement of Representative Ichord concerning H.R. 16373), reprinted in Source Book on Privacy, supra note 93, at 901.

[104] The Privacy Act of 1974, Pub. L. No. 93-579, § 6, 88 Stat. 1909 (1974)..

[105] Office of Management and Budget, Responsibilities for the Maintenance of Records About Individuals by Federal Agencies, 40 Fed. Reg. 28,948 (1975); Office of Management and Budget, Implementation of the Privacy Act of 1974, Supplementary Guidance, 40 Fed. Reg. 56,741 (1975). Together, these two documents are the "OMB Guidelines."

[106] The OMB Guidelines indicate that the law enforcement activity exception to subsection (e)(7) only applies if the record is required for "an authorized law enforcement function," but the OMB Guidelines provide no further enlightenment on the meaning of "law enforcement." Id. at 28965. One commentator cites the OMB Guidelines for the proposition that the law enforcement exception "applies to civil and criminal law enforcement as well as intelligence activities." John F. Joyce, The Privacy Act: A Sword and a Shield and Sometimes Neither, 99 Mil. L. Rev. 113, 131-32 (1983). There is, however, no mention of "intelligence activities" in the OMB Guidelines' discussion of subsection (e)(7), and no support for the further implication that intelligence activities divorced from civil or criminal law enforcement are encompassed by the law enforcement exception.

[107] "In referring to a 'law enforcement activity' and 'law enforcement purposes,' I am, of course, using the expression 'law

enforcement' in its general meaning and in the broadest reach of the term. I include within that term those purposes and activities which are authorized by the Constitution, or by statute, or by the rules and regulations and the executive orders issued pursuant thereto. Thus, investigatory material maintained shall include, but not be limited to, that which is compiled or acquired by any federal agency (for personnel security or access to classified information purposes)." 120 Cong. Rec. 36,651 (1974)(statement of Representative Ichord). "It is really to make certain that political and religious activities are not used as a cover for illegal or subversive activities ... (but there is) no intention to interfere with the first amendment rights of citizens." 120 Cong Rec. 36,957 (1974)(statement of representative Ichord).

[108] S. 3418, 93d Cong., 2d Sess. §§ 203(a) and 203(b) (1974) (introduced and referred to the Senate Committee on Government Operations, May 1, 1974), reprinted in Source Book on Privacy, supra note 93, at 97.

[109] Source Book on Privacy, supra note 93, at 97.

[110] See discussion infra note 130 and accompanying text.

[111] Section 552a(b) allows for dissemination of a Privacy Act record only under limited circumstances. Subsection (b)(7)

describes one of those circumstances: "for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency has made a written request (for the record) ...." Neither the legislative history, the OMB Guidelines, nor the case law interpreting this section focus on the specific meaning of law enforcement in this context. With regard to the case law, plaintiffs who assert a violation of this section invariably focus on the absence of a written request from the agency in receipt of the record (See, e.g., Doe v. Digenova, 779 F.2d 74 (D.C. Cir. 1985)); while defendants who are asserting proper release usually rely on a different exception to justify release (See, e.g., Covert v. Harrington, 876 F.2d 1989 (9th Cir. 1989) (reliance on routine use exception)).

Section 552a(j) allows certain agencies to exempt certain records from most substantive provisions of the act, including provisions requiring accounting for disclosures, permitting access by the subject of the record, and restricting the types of information that may be collected and maintained. Subsection (j)(2), however, is limited to records related to the enforcement of the criminal laws.

[112] OMB Guidelines, supra note 105, at 28972-73.

[113] 5 U.S.C. § 552 (1988).

[114] Freedom of Information Act Amendments, Pub. L. No. 93-502, 88 Stat. 1561 (1974).

[115] House and Senate Committees on Gov't Operations.

[116] 5 U.S.C. §552(b)(7)(D).

[117] "Likewise, 'national security' is to be strictly construed to refer to military security, national defense, or foreign policy. The term intelligence in section 552(b)(7)(D) is intended to apply to positive intelligence gathering activities, counter-intelligence activities, and background security investigations by governmental units which have authority to conduct such investigations." S. Conf. Rep. No. 1200, 93d Cong., 2d Sess. 7 (1974)(Joint Explanatory Statement of the Committee of Conference), reprinted in 1974 U.S.C.C.A.N. 6285, 6291.

[118] Courts have used the phrase inconsistently. The Supreme Court has used the phrase "national security function" in connection with information gathering on domestic radical organizations (Mitchell v. Forsyth, 472 U.S. 511 (1985)), although the phrase may be limited in the domestic context to attention rendered those groups that espouse the overthrow of the government. See, e.g., U.S. v. U.S. District Court, 407 U.S. 297, 309 n.8 (1972)(holding that the fourth amendment requires prior judicial approval of certain wiretap techniques in certain

national security investigations). " 'National Security' will generally be used interchangeably with 'foreign security,' except where the context makes it clear that it refers both to 'foreign security" and 'internal security.'" Zweibon v. Mitchell, 516 F.2d 594, 613 n.42 (D.C. Cir. 1975), cert. denied 425 U.S. 944 (1976). The executive branch has used "national security" in the foreign threat context. See Exec. Order 12,333, supra note 42.

[119] MacPherson v. Internal Revenue Service, 803 F.2d 479, 482 (9th Cir. 1986). But see Clarkson v. Internal Revenue Service, 678 F.2d 1368, 1374 n.10 (11th Cir. 1982)(analogizing the law enforcement provisions of the FOIA and Privacy Act). Clarkson may be the better approach. Although the Privacy Act and the FOIA have different purposes, narrow interpretations of "law enforcement" facilitate both the purpose of the Privacy Act (by restricting the type of personal information that may be retained by the agency) and the purpose of the FOIA (by increasing the amount of information available to the public).

[120] See 18 U.S.C. § 533 (1988)(authority of the Attorney General to appoint officials (e.g., the FBI) to detect and prosecute crimes against the United States); 26 U.S.C. §§ 7601-

7612 (1988)(authority of internal revenue service to investigate tax matters and perform other enforcement functions).

[121] See, e.g., Patterson v. FBI, 893 F.2d 595 (3d Cir. 1990), cert. denied, 111 S.Ct. 48 (1990)(FBI case); Jabara v. Webster, 691 F.2d 272 (6th Cir. 1982), cert. denied, 464 U.S. 863 (1983)(FBI case); MacPherson v. Internal Revenue Service, 803 F.2d 479 (9th Cir. 1986); Clarkson v. Internal Revenue Service, 678 F.2d 1368 (11th Cir. 1982).

[122] See Pototsky v. Department of the Navy, 717 F.Supp. 20 (D.Mass. 1989); Reuber v. United States, 829 F.2d 133 (D.C. Cir. 1987).

[123] See Nagel v. U.S. Dep't of Health, Education, and Welfare, 725 F.2d 1438 (D.C. Cir. 1984); American Federation of Government Employees v. Schlesinger, 443 F.Supp. 431 (D.C.D.C. 1978).

[124] Nagel, 725 F.2d at 1438; American Federation, 443 F.Supp. at 435.

[125] In Nagel, the D.C. Circuit held that derogatory information in an employee's file, even if arguably covered by the first amendment, was within the 552a(e)(7) law enforcement exception because "An employer's determination whether an

employee is performing his job adequately constitutes an authorized law enforcement activity under Section (e)(7)." Nagel, 752 F.2d at 1441. The court in Nagel reasoned that law enforcement was more than a criminal concept. The court further stated that "if an agency compiles records describing the exercise of first amendment rights by an individual who is not an employee of that agency, it is unlawful unless there is some other basis which renders the information relevant to an authorized criminal investigation or to an authorized intelligence or administrative one." This latter language is traceable to Jabara v. Webster, 691 F.2d 272, 280 (6th Cir. 1982). The 6th Circuit in Jabara determined that the district courts limitation of the law enforcement exception to investigation of "past, present, or future criminal activity" was too narrow, and adopted, without explanation, the FBI's proposed phrasing "relevant to an authorized criminal investigation or to an authorized intelligence or administrative one." Id. at 280. Since Jabara involved the FBI, a criminal investigative agency, the quoted language is dicta to the extent that "intelligence (investigation)" implies something apart from a criminal investigation.

[126] Compare AR 380-13, para. 6a (authorizes information gathering precedent to an off-post demonstration) with AR 380-

13, para. 3b(6) (AR 380-13 not applicable to "authorized criminal investigations and law enforcement intelligence activities"). DoD Dir. 5200.27 also categorizes intelligence operations involving demonstrations (para. D.1.d) as separate from the investigation and prosecution of crimes within the jurisdiction of DoD (para. D.1.g).

[127] Conspiracy to use force in impeding federal government functions is prohibited by 18 U.S.C. § 2384 (1988)(Seditious Conspiracy). If there is no conspiracy or no use of force, there may not be a violation of federal criminal law. To the extent that a federal law might be violated, the FBI, not DoD, has specific responsibility to investigate and take further action. See Memorandum of Understanding Between the Departments of Justice and Defense Relating to the Investigation and Prosecution of Certain Crimes (August 1984), reprinted in Army Reg. 27-10, Military Justice, para. 2-7 (25 January 1990).

[128] See, e.g., the definition of law enforcement officer in the Federal Tort Claims Act: "any officer of the United States who is empowered by law to execute searches, to seize evidence, or to make arrests for violation of federal law" (28 U.S.C. § 2680 (1988)); the definition of law enforcement officer in the Age Discrimination Act: "(one whose duties are) primarily the

investigation, apprehension, or detention of individuals suspected or convicted of offenses against criminal laws of the state" (29 U.S.C. § 630 (1980)); and the authority of internal revenue "enforcement officers" to execute searches, make seizures, and make arrests (26 U.S.C. § 7608(a) (1988)). See also AR 381-10, Appendix A, para. 18 (definition of "law enforcment activities").

[129] See discussion supra note 128. The Army itself has created a blanket "law enforcement" routine use for privacy act records, but "[t]he agency to which the records are referred must be the appropriate agency charged with the responsibility of investigating or prosecuting the violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto." AR 340-21, para. 3-2a. See also Lamont v. Department of Justice, 475 F.Supp. 761, 773 (S.D.N.Y. 1979)(discussing the FOIA exemption for investigatory records compiled for law enforcement purposes). Records of general information-gathering for monitoring purposes are not compiled for law enforcement purposes except where the purpose for which the records are held and used by the agency becomes "substantially violation-oriented." Id. at 773.

[130] See Dep't of Army, Pam. 27-21, Administrative and Civil

Law Handbook, para. 2-19 (15 Mar. 1992)[hereinafter DA Pam. 27-21]. "Short of a declaration of martial law, (the military) remains subordinate to civilian authorities - it does not become an independent law enforcement body. In the absence of a declaration of martial law, the military does not even have a power to arrest which is any more extensive than that of the ordinary citizen." Report on Military Surveillance of Civilian Politics, supra note 11, at 108. 10 U.S.C. §809(e) (1988) and 18 U.S.C. § 1382 (1988) have been cited as implied authority to conduct searches, seizures, and arrests of civilians, but only for civilians on-post. U.S. v. Banks, 539 F.2d 14 (9th Cir.), cert. denied, 429 U.S. 1024 (1976)(holding that the Posse Comitatus Act does not prohibit military personnel from acting on on-base criminal violations committed by civilians).

[131] 18 U.S.C. § 1385 (1988).

[132] Authority to protect military functions, wherever conducted, exists only in implied form. For example, the Secretary is responsible for "the functioning and efficiency of the Department of the Army" (10 U.S.C. § 3013(c)(1) (1988)) and is responsible to issue regulations "for the government of his department, ... and the custody, use, and preservation of its records, papers, and property." (5 U.S.C. § 301 (1988)). The

Supreme Court has cited an inherent authority in the commander, perhaps implied from the Constitution, to maintain order and discipline on a military reservation. Cafeteria Workers v. McElroy, 367 U.S. 886 (1961). Certain statutes have also been cited as implied authority for military security and law enforcement operations on-post. See Banks, 539 F.2d at 16. Despite the lack of a security mission expressly authorized by the Constitution or Act of Congress, Army Reg. 500-51, Support to Civilian Law Enforcement, para. 3-5 (1 July 1983) states that the Posse Comitatus Act is inapplicable to security operations.

[133] Exec. Order No. 12,333, supra note 42, discusses security in the context of protection against foreign threats.

[134] See, e.g., Jabara v. Webster, 691 F.2d 272, 280 (6th Cir. 1982), cert. denied, 464 U.S. 863 (1983); MacPherson v. Internal Revenue Service, 803 F.2d 479 (9th Cir. 1986).

[135] Clarkson v. Internal Revenue Service, 678 F.2d 1368, 1378 (11th Cir. 1982)(citing Jabara v. Kelley, 476 F.Supp. 561, 581 (E.D.Mich. 1979)[hereinafter Jabara I]). Jabara I was the first federal court opinion to consider the application of subsection (e)(7). After Clarkson was decided, Jabara I was reversed on appeal. Jabara v. Webster, 691 F.2d 272 (6th Cir. 1982), cert. denied, 464 U.S. 863 (1983)[hereinafter Jabara II].

Jabara II rejected the specific connection to a past present or future criminal act, and substituted a relevance standard ("relevant to an authorized criminal investigation or an intelligence or administrative one"). Jabara II, 691 F.2d at 280.

[136] 5 U.S.C. § 552a(e)(1) (1988).

[137] See subsection 552a(j)(2) (for certain criminal law enforcement records) and subsection 552a(k)(2) (for other investigatory material compiled for law enforcement purposes). Department of the Army has exempted the Counterintelligence Operations Files, at least to the extent that they satisfy the "compiled for law enforcement purpose" requirement. DA Pam. 25-51, para. 6-9.

[138] 120 Cong. Rec. 40,405 (1974)(Analysis of House and Senate Compromise Amendments to the Federal Privacy Act), reprinted in Source Book on Privacy, supra note 93, at 858, 863. "Information may not be maintained simply because it is relevant; it must be both relevant and necessary." OMB Guidelines, supra note 105, at 28960.

[139] Senate Comm. on Gov't Operations, Report on Protecting Individual Privacy in Federal Gathering, Use, and Disclosure of Information, S. Rep. No. 1183, 93d Cong., 2d Sess. 46

(1974)(discussing § 201(a)(1) of S.3418, which section provided that each Federal Agency shall collect, solicit and maintain only such personal information as is relevant and necessary to accomplish a statutory purpose of the agency), reprinted in Source Book on Privacy, supra note 93, at 151.

[140] OMB Guidelines, supra note 105, at 28960.

[141] 10 U.S.C. § 3013(c)(1) (1988).

[142] See, e.g., Reuber v. United States, 829 F.2d. 133 (D.C.Cir. 1984). Reuber, the plaintiff employee of government contractor Litton, challenged the government's filing and maintenance of a letter of reprimand issued by Litton to Reuber. The Reuber court held for the government, stating the plaintiff failed to demonstrate the information was either "irrelevant or unnecessary." Id. at 139. See also Kassel v. Veterans Administration, 709 F.Supp. 1194 (D.N.H. 1989)(plaintiff unable to show information was "unnecessary or irrelevant").

[143] Section 552a(i).

[144] Section 552a(g).

[145] Subsections (i)(1) and (i)(3) are irrelevant because they deal with wrongful disclosure and the use of deceit in obtaining information already contained within a Privacy Act

record. Subsection (i)(2) provides that an officer or employee who "willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5000." USAINSCOM investigative files and local criminal information files meet the subsection (e)(4) publishing requirement. These systems of records are defined so broadly that it is unlikely that an installation staff member could create, either knowingly or negligently, a record in the physical security intelligence arena that would not be encompassed within the relevant definition. See DA Pam. 25-51, at 37-48.

[146] Section 552a(g)(1).

[147] Section 552a(g)(1)(D).

[148] Section 552a(g)(4).

[149] Parks v. Internal Revenue Service, 618 F.2d 677 (10th Cir. 1980); Johnson v. Department of the Treasury, 700 F.2d 971 (5th Cir. 1983).

[150] Johnson, 700 F.2d at 973.

[151] Johnson, 700 F.2d at 974-86. The Johnson court analyzed the legislative history of the Privacy Act and concluded that the remedies in the Act were intended to be analogous to the those

provided for in common law invasion of privacy. See also Parks, 618 F.2d at 682-83.

[152] Tijerina v. Walters, 821 F.2d 789, 799 (D.C.Cir. 1987).

[153] Tijerina, 821 F.2d at 789; Britt v. Naval Intelligence Service, 886 F.2d 544, 551 (3d Cir. 1989).

[154] Albright v. United States, 732 F.2d 181, 189 (D.C. Cir. 1984).

[155] See supra text accompanying notes 140-42.

[156] Although words like "essential" and "relevant" are used in the regulations, they are not further defined and leave the interpreter with great discretion. The requirement that no information be collected "based solely on advocacy" is a restriction on when information may be collected, not on what information may be collected.

[157] AR 190-30, para. 3-18a.

[158] An argument can also be made that the described procedure can still result in a technical violation of the Act. "Maintenance" is defined, for purposes of the Act, as including "collection." § 552a(a)(3). If information is collected (received) in a form identifiable with an individual, the mere receipt might be considered as "maintenance of a record" even if

individual identifiers are immediately deleted. Maintenance of a record describing how an individual exercises his first amendment rights is violative of § 552a(e)(7) even if the record is never placed in a "system of records." Albright v. United States, 631 F.2d 915 (D.C. Cir. 1980).

Given that the purpose of the Act is to protect the privacy of individuals, however, an argument can also be made that "collection" means "collection with the intent to maintain information in individually identifiable form."

[159] But cf. Clarkson, 1378 F.2d at 1374 (stating that the use of the law enforcement exception is specifically limited to investigation of past, present or anticipated violations of statutes "the agency is authorized to enforce" (emphasis added)).

[160] See infra Appendix A.

[161] 18 U.S.C. § 1385 (1988). See discussion supra notes 131-32 and accompanying text.

[162] Army Reg. 500-51, Support to Civilian Law Enforcement, para. 3-4a (1 July 1983)[hereinafter AR 500-51]. Specific functions which fall in this category include "actions related to the commander's inherent authority to maintain law and order on a military installation or facility;" and "protection of DoD personnel, DoD equipment, and official guests of DoD." There is

no distinction between on-post and off-post functions or activities.

[163] Bissonette v. Hague, 776 F.2d 1384, 1390 (8th Cir. 1985); United States v. Red Feather, 392 F.Supp. 916 (D.S.D.), aff'd sub. nom., 541 F.2d 1275 (8th Cir.), cert. denied, 430 U.S. 970 (1975).

[164] 10 U.S.C. § 375 (1991 Supp.).

[165] Interestingly, where the Army believes the Posse Comitatus Act applies, the Army interprets the prohibitions of the Act broadly. If there is no military function or purpose, for example, the Act would preclude use of military personnel for "surveillance or pursuit of individuals," or as "informants, undercover agents, investigators, or interrogators". AR 500-51, para. 3-5.

[166] See discussion of the law enforcement exception to the Privacy Act's ban on collection of first amendment information, supra notes 131-32 and accompanying text.

[167] Bissonette v. Haig, 800 F.2d 812, 814 (8th Cir. 1986)(dicta).

[168] See Note, Judicial Review of Military Surveillance of

Civilians: Big Brother Wears Modern Army Green, 72 Colum. L. Rev. 1009 (1972)[hereinafter Note, Big Brother].

[169] The use of the term "chill" in the first amendment context has been traced to Wieman v. Updegraff, 344 U.S. 183, 195 (1952) (Frankfurter, J., concurring)(noting the inhibiting effect of loyalty oaths). Schauer, Fear, Risk, and the First Amendment: Unraveling the 'Chilling Effect,' 58 B.U.L. Rev. 685, 685 n.1 (1978).

[170] 408 U.S. 1 (1972).

[171] Id. at 3.

[172] Id. at 13-14.

[173] Compare Presbyterian Church v. U.S.A., 870 F.2d 518, (9th Cir. 1989)(The Laird plaintiffs alleged only that they could "conceivably" become subject to the Army's domestic surveillance program) with Tatum v. Laird, 444 F.2d 947, 954 n.17 (D.C. Cir. 1971)("The record shows that most if not all of the appellants and organizations of which they are members have been the subjects of Army surveillance and their names have appeared in the Army's records.").

[174] Compare Donohoe v. Dowling, 465 F.2d 196, 199 (4th Cir. 1972)(Laird characterized as involving clandestine methods,

infiltration, and sophisticated electronics) with Handschu v. Special Services Division, 349 F. Supp. 766, 769 (S.D.N.Y. 1972)(Laird characterized as involving passive intelligence gathering from open and public sources).

[175] Compare United Presbyterian Church v. Reagan, 738 F.2d 1375, 1379 (D.C. Cir. 1984)(citing Laird for the proposition that lack of regulatory, proscriptive, or compulsive exercise of government power precludes any possibility of standing based on "chill") with Socialist Workers Party v. Attorney General, 419 U.S. 1314, 1318 (1974)(Marshall, Circuit Justice)(the proposition that Laird requires some regulatory, proscriptive, or compulsive exercise of power is incorrect; the Court in Laird was simply distinguishing past cases where such power was exercised).

[176] Keene v. Meese, 619 F.Supp. 1111, 1117 (E.D.Cal. 1985), rev'd on other grounds, 481 U.S. 465 (1987).

[177] The Laird opinion noted the plaintiff's apparent concession that they themselves were not chilled. Laird, 408 U.S. at 13-14. "This concession, if accepted, would leave the Court only with claims that the government action was unlawful, not that anyone before the Court had been 'injured in fact' in any sense." The lack of actual chill to the Laird plaintiffs renders any subsequent discussion of types of chill irrelevant to

the case. Laurence H. Tribe, American Constitutional Law § 3-16, at 122 (2d ed. 1988)(emphasis in original).

[178] Plaintiff must also show that the injury fairly can be traced to the challenged activity of the defendant, and that the injury is likely to be redressed by the requested relief. Valley Forge Christian College v. Americans United for Separation of Church and State, 454 U.S. 464, 472 (1982); Allen v. Wright, 468 U.S. 737, 751 (1984).

[179] Valley Forge Christian College, 454 U.S. at 472.

[180] See Baker v. Carr, 369 U.S. 186, 204 (1962).

[181] See Tribe, supra note 177, § 3-16.

[182] See, e.g., Lamont v. Postmaster General, 381 U.S. 301 (1965). Plaintiff Lamont challenged a statute directing the post office to detain "communist propaganda" mail until the addressee made a request for delivery. The Court accepted the plaintiff's assertions of standing. The Court found the statute an unconstitutional first amendment infringement because those who read such material "might think they would invite disaster if they read what the government says contain the seeds for treason." Id. at 307. Laird distinguished Lamont on the grounds that the plaintiff in Lamont was being required to do something

(e.g., make a request for mail material) by the government. The injury in fact, however, is not making the request; the injury is the fear of what the government will do with a list of those who desire communist propaganda. Lamont is not distinguishable from Laird in this sense.

[183] Given the Laird conclusion that the plaintiffs lacked Article III standing, any discussion of prudential standing factors would have been dicta. Yet the Court did mention its concern that judicial review covering the Army's extensive intelligence activities of the period would have the "federal courts as virtually continuing monitors of the wisdom and soundness of Executive action." Laird, 408 U.S. at 15. One commentator suggests that the Court was leery of becoming involved in such a sensitive and complex political issue, and the "political question" doctrine is the best explanation for the Laird decision. Note, Big Brother, supra note 168, at 1027-28. The political question doctrine would be of less importance, of course, to a legal challenge involving a specific incident at the installation level.

[184] Speiser v. Randall, 357 U.S. 513, 526 (1958).

[185] See Tribe, supra note 177, § 12-1 (discussing historical

and judicial precedents supporting the necessity of free speech to individual fulfillment and stable government).

[186] For example, "an individual whose own speech or expressive conduct may validly be prohibited or sanctioned is permitted to challenge a statute on its face because it also threatens others not before the court - those who desire to engage in legally protected expression but who may refrain from doing so rather than risk prosecution or undertake to have the law declared partially invalid." Brockett v. Spokane Arcades, Inc., 472 U.S. 491, 503 (1985)(discussing the "overbreadth" doctrine). See also Board of Commissioners v. Jews for Jesus, 482 U.S. 569, 574 (1987). Lamont, 381 U.S. at 301, is a de facto case of representation of third party interests in a first amendment context. The only harm to Lamont was the requirement that he identify himself to the post office as interested in 'propaganda' materials. By bringing suit, however, he was telling the world that he was interested in those materials and thus exacerbating, not remedying, the potential personal harm. The only rights that he could have vindicated by his suit were the rights of third parties and society in general. See Police Dossiers and Emerging Principles of First Amendment Adjudication, 22 Stan. L. Rev. 196, 204 (1970).

[187] 419 U.S. 1314 (Marshall, Circuit Justice 1974).

[188] Id. at 1319.

[189] See Report on Military Surveillance, supra note 7, at 52.

[190] 481 U.S. 465 (1987).

[191] Id. at 472, 486. One commentator has remarked on the direct connection between Meese, Laird, and Army surveillance: "An opinion poll asking about those under surveillance by the U.S. Army would surely reveal that such government activity seriously threatens reputations." Jonathan R. Siegal, Note, Chilling Injuries as a Basis for Standing, 98 Yale L.J. 905, 909 (1989). Meese can also be read for the proposition that unsupported allegations of reputational injury can form the basis of standing. After granting Keene his standing, the Court went on to conclude that, since "political propaganda" has a neutral statutory meaning, and the statute actually adds to the amount of information available to the public by requiring that each film be labeled with its source, all that Keene needed to do to avoid injury was to discuss the label and its meaning before each film. In other words, any reputational injury was self-inflicted and avoidable.

[192] Riggs v. City of Albuquerque, 916 F.2d 582 (10th Cir. 1990)(challenge by political activists and politically active organizations to surveillance by city police department); The Presbyterian Church (U.S.A.) v. United States, 870 F.2d 518 (9th Cir. 1989)(challenge by churches to surveillance of church services in connection with investigation of the sanctuary movement by the Immigration and Naturalization Service).

[193] Riggs, 916 F.2d at 582.

[194] Id., 516 F.2d at 585.

[195] See DoD Dir. 5200.27, para. E.5; AR 380-13, para. 9d; and AR 381-10, Procedure 10, para. C.

[196] See, e.g., The Freedom of Information Act, 5 U.S.C. § 552 (1988) and the Government in the Sunshine Act, Pub. L. No. 94-049, 90 Stat. 1241 (1976).

[197] See City of Los Angeles v. Lyons, 461 U.S. 95 (1983). After Lyons was seriously injured by a police chokehold, he sued for damages and an injunction restricting the further use of the chokehold. The Court denied that Lyons had standing to request injunctive relief, as it was unlikely that he would ever again be attacked in the same manner. Similarly, if a protest is local, surveillance is local, and the specific conditions precipitating

that investigation dissipate prior to the plaintiff's request for relief, the protestor may not have standing to enjoin future Army surveillance.

[198] Alliance to End Repression v. Rochford, 407 F.Supp. 115, 118 (N.D.Ill. 1975). See also Local 309, United Furniture Workers, C.I.O., v. Gates, 75 F.Supp. 620 (N.D.Ind. 1948)[hereinafter Gates]. Police may defend overt surveillance as a deterrent to "violence, vandalism, and this kind of thing." Donohoe v. Dowling, 465 F.2d 196, 199 (4th Cir. 1972); Gates, 75 F.Supp. at 623.

[199] See Anderson v. Sills, 265 A.2d 678, 688 (N.J. 1970).

[200] See, e.g., Berlin Democratic Club v. Rumsfeld, 410 F.Supp 144 (D.D.C. 1976); Philadelphia Resistance v. Mitchell, 58 F.R.D. 139 (E.D.Pa. 1972); Alliance to End Repression v. Rochford, 407 F.Supp. 111 (N.D.Ill. 1975); Alliance to End Repression v. Chicago, 627 F.Supp. 1044, 1047 (N.D.Ill. 1985)(police brought along a newspaper reporter who wrote about surveillance activities).

[201] Philadelphia Yearly Meeting of the Religious Society of Friends v. Tate, 519 F.2d 1335 (3d Cir. 1975)(complaint of violation of Civil Rights Act).

[202] Paton v. LaPrade, 524 F.2d 862 (3d Cir. 1975).

[203] A mail cover is a procedure involving examination, prior to delivery, of mail addressed to particular addressees. Information on the exterior of the targeted mail, including the sender's address, is recorded and provided to the requesting investigative agency.

[204] Id., 524 F.2d at 870.

[205] But cf. AR 190-30, para. 3-18a, discussed supra note 53 and accompanying text.

[206] See AR 380-13, para. 8b(2), discussed supra note 77 and accompanying text.

[207] AR 340-21 provides for blanket routine uses which apply to all systems of records except those which specifically state otherwise. Such routine uses include, among other things, information relevant to federal agency decisions on hiring, firing, contracting, and security clearances. Id., para. 3-2.

[208] See, e.g., Paton v. La Prade, 524 F.2d 862 (3d Cir. 1975)(16 year-old plaintiff had standing to attack an FBI investigation because the FBI kept a file on the plaintiff which was available to the Civil Service Commission for federal hiring

decisions, and the plaintiff might study chinese and apply for a government job sometime in the future).

[209] See Fifth Avenue Peace Parade Committee v. Gray, 480 F.2d 326 (2d Cir. 1973), cert. denied, 415 U.S. 948 (1974)(In holding that plaintiffs lacked standing to challenge an FBI investigation, the Court of Appeals stressed that the investigation was attempting to gauge the number of persons attending a planned march and the investigators were not recording individual names and other personal information).

[210] See, e.g., United States v. Robel, 389 U.S. 258 (1967)(statute making it unlawful for a member of any "communist action organization" to work in a defense facility found unconstitutional); Dombrowski v. Pfister, 380 U.S. 479 (1965)(statute criminalizing certain "subversive activities" challenged as chilling legitimate civil rights activities and found unconstitutional).

[211] See, e.g., NAACP v. Alabama, 357 U.S. 449 (1958) and Gibson v. Florida Legislative Investigation Committee, 372 U.S. 539 (1963)(Legislative contempt conviction for failing to disclose NAACP membership lists found an unconstitutional infringement of first amendment rights where the legislature

could show no substantial connection between the NAACP and the communist activities being investigated).

[212] 491 U.S. 397 (1989). Although Johnson was a 5-4 decision, the general analytic scheme employed by the is authoritative. The majority opinion was joined by two of the more liberal members of the Court (Justices Brennan and Marshall) and two of the more conservative members (Justices Scalia and Kennedy). Further, the dissent did not quarrel with the analytical framework used by the majority. Id. at 421.

[213] See also United States v. Eichman, 496 U.S. 310 (1990)(overturning conviction for violating federal statute forbidding flag desecration). The Court's reasoning in Eichman did not vary significantly from its reasoning in Johnson.

[214] Johnson, 491 U.S. at 403.

[215] Plaintiffs challenging physical security intelligence operations will allege chill affecting speech and association, forms of expressive conduct. Even the harm that the government is trying to prevent or avoid (e.g., a peaceful blockade or terrorist act) is expressive conduct.

[216] Johnson, 491 U.S. at 403.

[217] Id. at 412.

[218] The test for a content based restriction is often described as requiring that the government show that the regulation is a precisely drawn means of serving a compelling state interest. See Tribe, supra note 177, § 12-8 at 833-34.

[219] Johnson, 491 U.S. at 407.

[220] If a statute (or regulation) appears to have a neutral purpose on its face, the courts will not examine into the drafter's actual motive. United States v. O'Brien, 391 U.S. 367, 376-77 (1968).

[221] See Shuttlesworth v. City of Birmingham, 394 U.S. 147 (1969); Hague v. Committee for Industrial Operations (C.I.O.), 307 U.S. 496 (1939); Lovell v. City of Griffin, 303 U.S. 444 (1938).

[222] AR 380-13, para. 6a.

[223] DoD Dir. 5200.27, para D.1.a.

[224] DoD Dir. 5200.27, para. D.1.c, includes an additional category for "Acts jeopardizing the security of DoD elements." None of these terms are defined.

[225] Id., para. E.2; AR 380-13, para. 9a.

[226] Compare Alliance to End Repression v. City of Chicago, 561 F.Supp. 575 (N.D.Ill. 1983)[hereinafter Alliance I] with

Alliance to End Repression v. City of Chicago, 742 F.2d. 1007 (7th Cir. 1984)[hereinafter Alliance II], rev'g Alliance I. The plaintiff and the FBI (one of the defendants) had entered into a consent decree. The decree contained the following language: "The FBI shall not conduct an investigation (of the plaintiff) solely on the basis of activities protected by the first amendment." The FBI subsequently issued national guidelines that covered investigative activities. These guidelines stated that "[w]hen, however, statements advocate criminal activity ... an investigation is warranted unless it is apparent ... that there is no prospect of harm." Plaintiff sought an injunction against application of these new guidelines to the plaintiffs, complaining that quoted language in the guidelines was violative of the consent decree. The District Court agreed with the plaintiffs. Alliance I, 561 F.Supp. at 578. The Court of Appeals did not. Alliance II, 742 F.2d at 1020. As summarized by the dissent in the Court of Appeals decision "[w]hile I have found it hard to pinpoint precisely what the majority has held ... I think tentatively that (the language of the decree meant only that) the FBI would decline to conduct an investigation in violation of the constitution, and unconstitutional investigations are those which are motivated solely by an

unambiguous desire to suppress a political movement ...." Alliance II, 742 F.2d at 1020 (Cudahy, J., dissenting).

[227] 395 U.S. 444 (1969).

[228] Id., 395 U.S. at 444.

[229] 391 U.S. 367 (1968).

[230] Id., 391 U.S. at 376-77.

[231] 468 U.S. 268 (1984).

[232] Id., 468 U.S. at 294.

[233] Id., 468 U.S. at 295.

[234] 75 F.Supp. 620 (N.D.Ind. 1948).

[235] 323 U.S. 516 (1945)(state statute mandated state registration and approval before labor organizer could solicit memberships; statute held incompatible with the first and fourteenth amendments).

[236] Id. at 530.

[237] See Gates, 75 F.Supp. at 624-25.

[238] Thomas, 323 U.S. at 532-38.

[239] White v. Davis, 533 P.2d 222, 224 (Cal. 1975); Anderson v. Sills, 256 A.2d 298, 303 (N.J. Super. Ct. Ch. Div. 1969)(court

rejected the balancing approach used in lesser scrutiny cases, resulting in greater scrutiny), rev'd, 265 A.2d 678 (N.J. 1970).

[240] Davis, 533 P.2d at 224 ("Is this intelligence gathering by the police ... constitutionally valid when such (police) reports pertain to no illegal activity or acts?"); Anderson, 256 A.2d at 303 ("Nor should it be the task of the judiciary to balance governmental need against first amendment rights when the regulation, law, or official act goes beyond areas reasonably necessary to reach the permissible government goal").

[241] 419 U.S. 1314 (Marshall, Circuit Justice 1974).

[242] Socialist Workers Party v. Attorney General, 387 F.Supp. 747 (S.D.N.Y.)[hereinafter SWP I], order vacated in part by 510 F.2d 253 (2d Cir.)[hereinafter SWP II], stay of order denied by 419 U.S. 1314 (Marshall, Circuit Justice 1974)[hereinafter SWP III].

[243] The Civil Service Commission.

[244] SWP II, 510 F.2d at 253.

[245] "[T]he Court of Appeals has analyzed the competing interests at some length, and its analysis seems to me to compel denial of relief." SWP III, 419 U.S. at 1319.

[246] "[O]ur abhorrence for abuses of governmental investigative authority cannot be permitted to lead to an indiscriminate willingness to enjoin undercover investigation of any nature, whenever a countervailing first amendment claim is raised." SWP III, 419 U.S. at 1319.

[247] The FBI had been watching the SWP and YSA for years. Justice Marshall questioned, with regard to a short-term injunction effective until trial on the merits, whether granting the injunction would significantly lessen any on-going "chill" injury. SWP III, 419 U.S. at 1319.

[248] 481 U.S. 465 (1987).

[249] Supra notes 190-91 and accompanying text.

[250] Keene v. Meese, 619 F.Supp. 1111, 1117 (E.D.Cal. 1985), rev'd on other grounds, 481 U.S. 465 (1987).

[251] New York Times Co. v. United States (Pentagon Papers Case), 403 U.S. 713, 714 (1971) (per curiam).

[252] The Supreme Court's opinion in Meese did not even address the District Court's use of the "censorship" argument. This failure may be explained by the Court's conclusion that the plaintiff's alleged injuries were, in large part, avoidable. See discussion supra note 191.

[253] 750 F.2d 89 (D.C. Cir. 1984).

[254] Nos. 74C3268, 75C3995, 1991 WL 206056 (N.D.Ill. 1991)[hereinafter Alliance IV]. Alliance IV is the latest decision in a series of related cases (see, e.g., supra note) growing out of police, FBI, and military surveillance activities in the Chicago area. Alliance IV did not actually involve constitutional interpretation, but rather interpretation of a consent decree that the FBI had allegedly violated.

[255] Id. at *9.

[256] AR 380-13, para. 6a (emphasis added).

[257] Other regulations also can use modification, including DoD Dir. 5240.1, DoD Dir. 5240.1-R, AR 381-10, AR 190-30, and AR 190-45. These regulations, however, are more limited in their applicability to physical security intelligence operations than DoD Dir. 5200.27 or AR 380-13.

[258] Since AR 380-13 has not been reissued since 1974, the regulation needs extensive rewriting. At the time this thesis was prepared, the proponents of AR 380-13 were awaiting the reissuance of DoD Dir. 5200.27 before drafting a new AR 380-13. In addition to its dependence on DoD Dir. 5200.27, a new AR 380-13 will have to be consistent with AR 381-10 (e.g., AR 380-13,

para. 5a indicates that AR 380-13 is the "sole and exclusive authority" for collection of information on nonaffiliated persons; however, AR 381-10 and AR 381-20 are new and separate authorities for counterintelligence collection on domestic terrorist threats).

[259] Clark v. Community for Creative Nonviolence, 468 U.S. 268, 294 (1984)[hereinafter Clark v. CCNV].

[260] Sit-ins or other peaceful civil disobedience tactics are not federal crimes. On the other hand, conspiracy to disrupt government activities through force or violence (18 U.S.C. § 2384 (1988)(Seditious Conspiracy)) is a felony within the jurisdiction of the FBI.

[261] See discussion supra note 132.

[262] Clark v. CCNV, 468 U.S. at 294.

[263] See U.S. v. Banks, 539 F.2d 14 (9th Cir.), cert. denied, 429 U.S. 1024 (1976); and discussion, supra notes 130-32 and accompanying text.

[264] Clark v. CCNV, 468 U.S. at 294.

[265] At the 1974 hearings on military surveillance, the DoD representative was asked about the targets of any special operations that had been approved in accordance with the

provisions of the original DoD Dir. 5200.27. "Let me say they were a group who would advocate, for example, putting sand in the fuel tanks of our planes, or another example, advocating throwing a monkey wrench into the reduction gears of a ship or not obeying orders of a commanding officer of a naval vessel." Hearings on Military Surveillance, supra note 10, at 118 (statement of Mr. Cooke).

[266] Personnel security investigations should be pursued from the standpoint of the potential target (i.e., identification of military personnel who are vulnerable to manipulation) rather than tracking nonaffiliated persons who might attempt to subvert military personnel. Separate guidance exists for these loyalty investigations. See Exec. Order No. 10,450, 18 Fed. Reg. 2489 (1953)(Security Requirements for Government Employment).

[267] Clark v. CCNV, 468 U.S. at 294.

[268] "The failure of senior civilian officials to know of the (Army surveillance) program, or if knowing, to halt it, represents one of the most serious breakdowns of civilian control of the military in recent years." Report on Military Surveillance, supra note 7, at 5.

[269] See AR 380-13, para. 9e.

[270] See Alliance to End Repression v. City of Chicago, Nos. 74C3268, 75C3995, 1991 WL 206056 (N.D.Ill. 1991). The FBI conducts a limited investigation called a "preliminary inquiry" when acting on information that is ambiguous, incomplete, or from a source of unknown reliability. When the preliminary inquiry fails to disclose sufficient information to warrant a full investigation, the matter is closed. Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations, para. II.B. (March 7, 1983), reprinted in 32 Crim. L. Rep. (BNA) 3087 (March 23, 1983).

[271] 392 U.S. 1 (1968)(The requirements or the fourth amendment were satisfied when policeman conducted a short stop and a limited search pursuant to a reasonable suspicion based on articuable facts).

[272] Mitchell S. Rubin, Note, The FBI and Dissidents: A First Amendment Analysis of Attorney General Smith's Guidelines on Domestic Security, 27 Ariz. L. Rev 453 (1985).

[273] 395 U.S. 444 (1969).

[274] Schauer, supra note 169, at 722-25. Although Brandenberg was convicted for advocacy of violent activity, the facts as restated by the Brandenberg Court left some question as to whether the plaintiff was just discussing the possibility of

criminal activity or was actually advocating such activity. See Brandenberg, 395 U.S. at 446-47.

[275] See discussion supra notes 195-204 and accompanying text.

[276] See, e.g., Donohoe v. Dowling, 465 F.2d 196 (4th Cir. 1972); Socialist Workers Party v. Attorney General, 419 U.S. 1314, 1319 (Marshall, Circuit Justice 1974)[hereinafter SWP III].

[277] See, e.g., SWP III, 419 U.S. at 1318; Handschu v. Special Services Division, 349 F.Supp. 766, 769 (S.D.N.Y. 1972).

[278] Alliance to End Repression v. Chicago, 627 F. Supp. 1044, 1047 (N.D.Ill. 1985).

[279] Cf. Fifth Avenue Peace Parade Committee v. Gray, 480 F.2d 326 (2d Cir. 1973), cert. denied, 415 U.S. 948 (1974). In Gray, the FBI studied bank and transportation records and watched bus routes in an effort to predict the numbers of demonstrators attending a mass rally in Washington D.C. In refusing to recognize any cognizable injury to plaintiff, the Court of Appeals relied on FBI representations that it had recorded no personal information and taken no photographs.

[280] 18 U.S.C. § 1385 (1988). See supra notes 163-66 and accompanying text.

[281] See supra notes 108-110, 131-135 and accompanying text.

[282] See supra notes 208-09.

[283] See AR 340-21, para. 3-2c; DA Pam. 25-51, paras. 6-7 and 6-25.

[284] See supra notes 94-95 and accompanying text.

[285] See discussion of Privacy Act enforcement, supra notes 147-149 and accompanying text.

[286] See substantive first amendment analysis, supra note 232 and accompanying text.

[287] 468 U.S. 268, 294 (1984).

Appendix A

DRAFT

NUMBER 5200.27

Department of Defense Directive

SUBJECT: Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense

References: (a) DoD Directive 5200.27, subject as above, January 7, 1980 (hereby canceled)

(b) DoD Directive 5240.1, "Activities of DoD Intelligence Components that Affect U.S. Persons," April 25, 1988

(c) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December, 1982

(d) Memorandum of Understanding Between the Departments of Justice and Defense Relating To the Investigation and Prosecution of Certain Crimes, August, 1984

A. REISSUANCE AND PURPOSE

This Directive reissues reference (a) to establish general policy, limitations, procedures, and operational guidance pertaining to the collecting, processing, storing, and dissemination of information concerning persons and organizations not affiliated with the Department of Defense.

B. APPLICABILITY AND SCOPE

1. This Directive is applicable to all DoD Components, except for DoD Intelligence Components.

2. This Directive is applicable only to the acquisition of information concerning the activities of:

a. any U.S. citizen who is not affiliated with the Department of Defense; or

b. any person or organization, not affiliated with the Department of Defense, located in the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, or U.S. territories or possessions.

c. any person or organization affiliated with DoD, if there is no connection between the purpose for which the information is being collected and the affiliation.

C. DEFINITIONS

1. DoD Component. The Office of the Secretary of Defense, Military Departments, Office of the Joint Chiefs of Staff, Unified and Specified Commands, and the Defense Agencies.

2. DoD Intelligence Component. Those DoD components which satisfy the criteria of DoD Directive 5240.1 (reference (b)), paragraph C.4.

3. Persons and Organizations Affiliated with the Department of Defense. Persons or organizations that are employed by or under contract with the DoD; active, reserve, or retired members of the Armed Forces; residing on or having requested access to any DoD installation; having authorized access to defense information; participating in any other authorized program; or who are seeking a status listed in this subparagraph.

4. Reasonable Suspicion. A suspicion based on

specific, articuable facts; more than a mere hunch.

5. Imminent. Within a definitive period of time, not to exceed thirty days.

6. Essential to National Security. Connected directly, in some articuable way, to the nation's ability to deter and defeat foreign aggression.

7. Personal Information. Any information which identifies a person by name or other personal identifier.

8. Physical Surveillance. See procedure 9, reference (c).

D. POLICY

1. Department of Defense policy prohibits collecting, reporting, processing, or storing information on individuals or organizations not affiliated with the Department of Defense, except int those limited circumstances, as defined in this Directive, where such information is essential to the accomplishment of the Department of Defense mission.

2. Information-gathering activities shall be

subject to overall civilian control, including frequent inspections at the field level and a high level of general supervision.

3. Where collection activities are authorized, maximum reliance shall be placed upon domestic civilian investigative agencies, Federal, State, and local.

4. (Not Reproduced - only concerns overseas operations)

E. SITUATIONS WARRANTING COLLECTION.

DoD Components are authorized to gather information for the following purposes.

1. Physical Security of Personnel, Functions, and Property. Information may be acquired about nonaffiliated personnel that threaten military personnel, property, and functions, but only to protect against the circumstances listed in this paragraph and only in accordance with the collection techniques of paragraph F.

a. Theft, destruction, or damage of military property.

b. The use of force or violence against military personnel.

c. Unauthorized personnel entering a military installation.

c. Physical acts disrupting military activities essential to the national security.

2. Personnel Security (Not Reproduced)

3. Operations Related to Civil Disturbance. (Not Reproduced)

4. Crimes for which DoD has Responsibility for Investigating or Prosecuting. Responsibility is set forth in reference (d).

F. COLLECTION PROCEDURES

1. Physical Security.

a. Commanders are encouraged to solicit general information, on a continuing basis, from local civilian investigative agencies concerning the situations

described in paragraph E.1. above.

b. When the commander has a reasonable suspicion that one or more of the situations described in paragraph E.1 is imminent, he will attempt to obtain any additional needed information from local authorities. If this information is insufficient, and the commander believes that off-post investigation is needed, he will develop an investigative scheme and supporting plan.

c. The plan will set forth the proposed investigation, indicating in particular:

1. The activity that is threatened.

2. The subsection of paragraph E that is implicated.

3. Why there is no way to restructure the planned activity to avoid the threat without conducting an off-post investigation.

4. The scope of proposed investigation, including an assertion that the requirements of paragraph e, f, and g below will be complied with.

d. The plan must be approved by the Secretary of the Military Department. Approval authority may be delegated to an Undersecretary or Assistant Secretary. In an emergency, if the appropriate civilian authority cannot be contacted in timely manner, anyone in the local commander's chain of command may approve the operation. The commander will still comply with paragraph F.1.c, including telephonic notification to the approval authority of the elements of information required by F.1.c.

e. If the credibility of the information source supporting the investigation has not been verified, the investigation will verify the reliability of the source before proceeding further.

f. Where possible, investigators will proceed without identifying themselves or their affiliation with the military, and will gather information from public sources. Information collected will relate only to the imminent threat designated in paragraph E above.

g. The following is prohibited:

1. The placement or use of informers or infiltrators who are officers in a targeted organization,

unless there is a reasonable suspicion that the organization plans the imminent use of force or violence against military personnel or property.

2. The collection of any personal information unless there is reason to believe the individual is actively and personally involved in planning or executing an activity posing a threat as defined in paragraph E.1. Mere membership or other association with an organization suspected of planning or executing such an activity is insufficient, by itself, to support collection of personal information.

3. The use of any technique intended to intimidate, harass, or otherwise influence the activities of any person or organization.

4. The use of electronic surveillance.

5. The use of cameras, videotape recorders, audiorecorders, or any other device that will make a permanent audio or video record.

6. The direct participation in a search, seizure, or arrest.

7. Overt physical surveillance.

2. Personnel Security. (TBD)

3. Operations Related to Civil Disturbances. (TBD)

4. Crimes for Which DoD Has Responsibility for Investigating or Prosecuting. (TBD)

H. RETENTION OF INFORMATION

1. Personal Information collected in accordance with paragraph E.1.

a. Unless a clear need for retention can be identified, personal information will be edited or summarized immediately after collection to remove the names of individuals and other personal identifiers.

b. No information about personal financial status, educational history, sexual practices, or religious beliefs will be collected or retained under any circumstances.

c. All personal information will be deleted within 90 days of collection, unless a continuing reasonable suspicion exists that the individual poses an

imminent threat under circumstances defined in paragraph E.1..

2. Information collected in accordance with paragraphs E.2. through E.4 shall be destroyed within 90 days of collection unless its retention is required by law or unless its retention is specifically authorized under separate criteria of the Secretary of Defense.

I. GENERAL GUIDANCE

1. Nothing in this directive shall be construed to prohibit 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 report.

2. Nothing in this Directive ... (continue as in paragraph F2, original DoD 5200.27)

J. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately.

January 7, 1980
NUMBER 5200.27

USDP

Department of Defense Directive

SUBJECT: Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense

References: (a) DoD Directive 5200.27, subject as above, December 8, 1975 (hereby canceled)
(b) DoD Directive 5240.1, "Activities of DoD Intelligence Components that Affect U.S. Persons," November 30, 1979

A. REISSUANCE AND PURPOSE

This Directive reissues reference (a) to establish for the Defense Investigative Program general policy, limitations, procedures, and operational guidance pertaining to the collecting, processing, storing, and disseminating of information concerning persons and organizations not affiliated with the Department of Defense.

B. APPLICABILITY AND SCOPE

1. Except as provided by subsection B.3., below, this Directive is applicable to the Office of the Secretary of Defense, Military Departments, Office of the Joint Chiefs of Staff, Unified and Specified Commands, and the Defense Agencies (hereafter referred to as "DoD Components").

2. The provisions of this Directive encompass the acquisition of information concerning the activities of:

a. Persons and organizations, not affiliated with the Department of Defense, within the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories and possessions; and

b. Non-DoD-affiliated U.S. citizens anywhere in the world.

3. This Directive is not applicable to DoD intelligence components as defined by DoD Directive 5240.1 (reference (b)).

4. Authority to act for the Secretary of Defense in matters in this Directive which require specific approval are delineated in enclosure 1.

C. POLICY

1. Department of Defense policy prohibits collecting, reporting, processing, or storing information on individuals or organizations not affiliated with the Department of Defense, except in those limited circumstances where such information is essential to the accomplishment of the Department of Defense missions outlined below.

2. Information-gathering activities shall be subject to overall civilian control, a high level of general supervision and frequent inspections at the field level.

3. Where collection activities are authorized to meet an essential requirement for information, maximum reliance shall be placed upon domestic civilian investigative agencies, Federal, State and local.

4. In applying the criteria for the acquisition and retention of information established pursuant to this Directive, due consideration shall be given to the need to protect DoD functions and property in the different circumstances existing in geographic areas outside the United States. Relevant factors include:

a. The level of disruptive activity against U.S. forces;

b. The competence of host country investigative agencies;

c. The degree to which U.S. military and host country agencies exchange investigative information;

d. The absence of other U.S. investigative capabilities; and

e. The unique and vulnerable position of U.S. forces abroad.

D. AUTHORIZED ACTIVITIES

DoD Components are authorized to gather information essential to the accomplishment of the following defense missions:

1. Protection of DoD Functions and Property. Information may be acquired about activities threatening defense military and civilian personnel and defense activities and installations, including vessels, aircraft, communications equipment, and supplies. Only the following types of activities justify acquisition of information under the authority of this subsection:

a. Subversion of loyalty, discipline, or morale of DoD military or civilian personnel by actively encouraging violation of law, disobedience of lawful order or regulation, or disruption of military activities.

b. Theft of arms, ammunition, or equipment, or destruction or sabotage of facilities, equipment, or records belonging to DoD units or installations.

c. Acts jeopardizing the security of DoD elements or operations or compromising classified defense information by unauthorized disclosure or by espionage.

d. Unauthorized demonstrations on active or reserve DoD installations.

e. Direct threats to DoD military or civilian personnel in connection with their official duties or to other persons who have been authorized protection by DoD resources.

f. Activities endangering facilities which have classified defense contracts or which have been officially designated as key defense facilities.

g. Crimes for which DoD has responsibility for investigating or prosecuting.

2. Personnel Security. Investigations may be conducted in relation to the following categories of persons:

a. Members of the Armed Forces, including retired personnel, members of the Reserve Components, and applicants for commission or enlistment.

b. DoD civilian personnel and applicants for such status.

c. Persons having need for access to official information requiring protection in the interest of national defense under the Department of Defense Industrial Security Program or being considered for participation in other authorized Department of Defense programs.

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 which 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 enforcement capabilities of State and local authorities.

E. PROHIBITED ACTIVITIES

1. The acquisition of information on individuals or organizations not affiliated with the Department of Defense will be restricted to that which is essential to the accomplishment of assigned Department of Defense missions under this Directive.

2. No information shall be acquired about a person or organization solely because of lawful advocacy of measures in opposition to Government policy.

3. There shall be no physical or electronic surveillance of Federal, State, or local officials or of candidates for such offices.

4. There shall be no electronic surveillance of any individual or organization except as authorized by law.

5. There shall be no covert or otherwise deceptive surveillance or penetration of civilian organizations unless specifically authorized by the Secretary of Defense, or his designee.

6. No DoD personnel will be assigned to attend public or private meetings, demonstrations, or other similar activities for the purpose of acquiring information, the collection of which is authorized by this Directive without specific prior approval by the Secretary of Defense, or his designee. An exception to this policy may be made by the local commander concerned, or higher authority, when, in his judgment, the threat is direct and immediate and time precludes obtaining prior approval. In each such case a report will be made immediately to the Secretary of Defense, or his designee.

7. No computerized data banks shall be maintained relating to individuals or organizations not affiliated with the Department of Defense, unless authorized by the Secretary of Defense, or his designee.

F. OPERATIONAL GUIDANCE

1. Nothing in this Directive shall be construed to prohibit 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.

2. Nothing in this Directive shall be construed to restrict the direct acquisition by overt means of the following information:

a. Listings of Federal, State, and local officials who have official responsibilities related to the control of civil disturbances. Such listings may be maintained currently.

b. Physical data on vital public or private installations, facilities, highways, and utilities, as appropriate, to carry out a mission assigned by this Directive.

3. Access to information obtained under the provisions of this Directive shall be restricted to governmental agencies which require such information in the execution of their duties.

4. Information within the purview of this Directive, regardless of when acquired, shall be destroyed within 90 days unless its retention is required by law or unless its retention is specifically authorized under criteria established by the Secretary of Defense, or his designee.

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.

G. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward two copies of implementing regulations to the Deputy Under Secretary of Defense (Policy Review) within 120 days.

W. Graham Claytor, Jr.
Deputy Secretary of Defense

Enclosure - 1
Delegation of Authority

B-5

DELEGATION OF AUTHORITY

A. The Secretary of the Army is designated to authorize those activities delineated in subsection D.3., basic Directive. This authority may not be further delegated to other than the Under Secretary of the Army.

B. The Deputy Under Secretary of Defense (Policy Review) (DUSD(PR)) is designated to authorize those activities delineated in subsection E.5., basic Directive, within the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories and possessions. This authority may not be delegated. The investigating DoD Component, prior to requesting approval for authorizations under this provision, shall coordinate prospective activities with the Federal Bureau of Investigation.

C. The DUSD(PR) and the Secretaries of the Military Departments are designated to authorize those activities (delineated in subsection E.5., basic Directive) abroad[1] when membership of the civilian organization is reasonably expected to include a significant number of non-DoD-affiliated U.S. citizens. This authority may not be further delegated to other than the Under Secretaries of the Military Departments. When the Military Department Secretary or Under Secretary exercises this delegation of authority, the DUSD(PR) shall be advised promptly.

D. The Secretaries of the Military Departments are designated to authorize in their Departments those activities delineated in subsection E.6., basic Directive, within the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, and U.S. territories and possessions. This authority may not be further delegated to other than the Under Secretaries of the Military Departments.

E. The Secretaries of the Military Departments are designated to authorize in their Departments those activities (delineated in subsection E.6., basic Directive) abroad[1] when a significant number of non-DoD-affiliated U.S. citizens are expected to be present. This authority may be further delegated, in writing, as circumstances warrant, to an authorized designee. The DUSD(PR) will be notified immediately of such further delegations of authority. When the Secretary or Under Secretary of a Military Department or his designee exercises this delegated authority, the DUSD(PR) shall be advised promptly.

F. The DUSD(PR) is designated to authorize those activities delineated in subsections E.7. and F.4., basic Directive. These authorities may not be further delegated.

[1]"Abroad" means "outside the United States, its territories and possessions."

ARMY REGULATION
No. 380-13

HEADQUARTERS
DEPARTMENT OF THE ARMY
WASHINGTON, DC, *30 September 1974*

SECURITY

ACQUISITION AND STORAGE OF INFORMATION CONCERNING NON-AFFILIATED PERSONS AND ORGANIZATIONS

Effective immediately upon receipt

This is a new Army regulation which supersedes letter AGDA-A-M, 1 June 1971, subject: Aquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense. It provides direction concerning the acquisition, reporting, processing, and storage of information on persons or organizations not affiliated with the Department of Defense. Local supplementation of this regulation is prohibited except upon approval of the Assistant Chief of Staff for Intelligence.

1. Purpose. This regulation implements DOD Directive 5200.27 and establishes policy and procedures governing the acquisition, reporting, processing and storage of information on persons or organizations not affiliated with the Department of Defense.

2. Policy. *a.* Department of the Army policy prohibits acquiring, reporting, processing or storing of information on persons or organizations not affiliated with the Department of Defense, except under those circumstances authorized in paragraphs 6 and 7 below when such information is essential to accomplish Department of Army missions.

b. All information-gathering activities are subject to overall civilian control and general supervision by the Secretary or Under Secretary of the Army.

c. Where acquisition activities are authorized by this regulation to meet an essential requirement for information, maximum reliance will be placed on liaison with domestic civilian investigative agencies, Federal, state, and local.

3. Applicability and scope. *a.* This regulation is applicable to the following:

(1) All Department of the Army civilian and military personnel, major Army commands, installations, activities, agencies, and organizations within the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, the Panama Canal Zone, Guam, American Samoa and the Guano Islands.

(2) In addition to its applicability in the geographic areas cited directly above, the provisions of this regulation shall apply to the acquisition, reporting, processing and storage of infor-

*This regulation supersedes: DA Ltr AGDA-A-M, 1 June 1971, CS, 1 June 1971, Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense, and DA Ltr DAAG-PAP-A (M) 25 October 1972, DAMI-DOI P, 6 November 1972, Screening of the Army's Intelligence Files.

mation concerning non-DOD-affiliated US citizens anywhere in the world.

(3) All resources of the Department of the Army including but not limited to counterintelligence units, staffs and personnel, as well as any other unit, staff or personnel who request, acquire, process, store, evaluate or report information covered by the policies and procedures of this regulation.

(4) Investigative/counterintelligence activities undertaken to:

(*a*) Safeguard defense information.

(*b*) Protect Army personnel against subversion.

(*c*) Protect Army functions and property, including facilities having classified defense contracts or those officially designated key defense facilities.

(*d*) Conduct counterintelligence surveys, services and inspection.

(*e*) Conduct investigative activities authorized in connection with civil disturbance responsibilities as outlined in paragraph 7 below.

(*f*) Conduct personnel security investigative leads as requested by the Defense Investigative Service.

b. This regulation does not apply to—

(1) Pre-trial investigations required by the Uniform Code of Military Justice.

(2) Activities involving cryptography.

(3) Utilization by public information officers of relevant information from published sources solely for the purpose of preparing responses to public inquiries. However, such information is not to be retained for the purpose of providing an Army element with background information about the activities, associations and beliefs of individuals unless its retention is authorized elsewhere in this regulation.

(4) Foreign intelligence information including the acquisition reporting, processing and storing of such information.

(5) Activities conducted on the Pentagon Reservation in accordance with the provisions of DOD Directive 5100.49, "Pentagon Counterintelligence Program."

(6) Authorized criminal investigation and law enforcement information gathering activities (i.e., those activities not "counterintelligence related") which are the responsibility of military police and the US Army Criminal Investigation Command. Such activities will continue to be conducted in accordance with applicable regulations.

c. This regulation does not abrogate any provisions of the Delimitations Agreement of 1949, as amended, between the Federal Bureau of Investigation and the Departments of the Army, Navy, and Air Force (AR 381-115).

4. Explanation of terms. The terminology as used in the glossary, appendix A, is applicable for the purpose of this regulation.

5. General. *a*. This regulation is the sole and exclusive Department of the Army authority for acquiring, reporting, processing and storing of investigative information on persons and organizations not affiliated with the Department of Defense. No other Department of the Army or subordinate command regulation, policy letter, circular or other form of authority, classified or unclassified, will be used to justify activities prohibited by this regulation.

b. Apparent violations of policies set forth in this regulation will be reported by Army personnel to their superior and to the Inspector General. Commanders will expeditiously report such apparent violations through channels to HQDA (DAMI-DOI) WASH DC 20310.

c. Army components of unified commands receiving instructions which they believe violate the provisions of this regulation will immediately report such instructions to HQDA (DAMI-DOI).

d. Unsolicited sources.

(1) Walk-in sources volunteering information not authorized for acquisition by this regulation will be referred to the appropriate Federal, state or local law enforcement agency. If the source refuses such referral, the information will be obtained and immediately furnished to the proper civilian law enforcement office; if source so requests, his identity will be protected.

(2) Information received from anonymous telephone callers, written messages or from any other means will be referred or processed as indicated in paragraph 5*d*(1) above.

e. Although this regulation imposes certain restrictions on the conduct of counterintelligence and investigative activities, it is not intended to, nor does it, prohibit the Army from protecting its personnel, functions, and property from the threats described in paragraph 6. Action authorized by this regulation will be undertaken to identify and counter such threats.

C-2

6. Operations related to protection of Army personnel, functions and property. *a.* Information on persons and organizations not affiliated with the Department of Defense may be acquired, reported, processed, and stored under the authority of this paragraph only if there is a reasonable basis to believe that one or more of the following situations exists:

(1) Theft, destruction or sabotage of weapons, ammunition, equipment, facilities, or records belonging to DOD units or installations.

(2) Possible compromise of classified defense information by unauthorized disclosure or by espionage.

(3) Subversion of loyalty, discipline or morale of Department of the Army military or civilian personnel by actively encouraging violation of laws, disobedience of lawful orders and regulations, or disruption of military activities.

(4) Demonstrations on active or reserve Army installations or demonstrations immediately adjacent to them which are of such a size or character that they are likely to interfere with the conduct of military activities. Armed Forces Induction Centers, US Army Recruiting Stations located off-post and facilities of federalized National Guard Units are considered to be active DOD installations. For the purpose of this subparagraph, ROTC installations on campuses are not considered to be active or reserve Army installations and coverage of demonstrations at or adjacent to such installations is not authorized.

(5) Direct threats to DOD military or civilian personnel regarding their official duties or to other persons authorized protection by DOD resources.

(6) Activities or demonstrations endangering classified defense contract facilities or key defense facilities, including the Panama Canal and those related operational facilities of the Panama Canal approved by HQDA as key to the defense and operation of the Panama Canal.

b. Effective liaison with local law enforcement agencies will be conducted on a regular basis to determine if actual or potential situations described in paragraphs 6*a*(1), (2), (3) and (6) exist. Counterintelligence surveys and inspections (AR 381–130) will be conducted for the same purpose. If, based on information received, the commander of a major Army command or an Army installation commander has reason to believe that inquiries involving persons and organizations not affiliated with DOD must be made to determine whether or not an actual threat situation exists, the counterintelligence unit having liaison responsibility will request the appropriate civil law enforcement authorities to provide the information required by the commander. However, under no circumstances will the law enforcement authorities be requested to furnish information the acquisition of which is prohibited by this regulation. If the civil law enforcement authorities cannot or will not provide the needed information, the facts of the situation and a request for authorization to utilize Army investigators in a specific manner to conduct a special investigation/operation will be forwarded by the counterintelligence unit having liaison responsibility to HQDA (DAMI–DOI). This request will be submitted in the format in appendix B.

c. The criteria to be used in submitting a request to conduct a special investigation/operation involving persons or organizations not affiliated with DOD are as follows:

(1) The target group must represent a significant and demonstrable threat to the security/effectiveness of Army functions and property.

(2) The information to be gained must relate to the situations outlined in paragraph 6*a* of this regulation.

(3) The information cannot or will not be provided by Federal, state and local law enforcement agencies and coordination with the Federal Bureau of Investigation (AR 381–115) has been completed.

d. Upon termination of an authorized investigation/operation, a summary report, including an analysis of the results and value of the investigation/operation, will be forwarded to HQDA (DAMI–DOI). If an authorized investigation/operation is subsequently expected to extend beyond 12 months, a request for revalidation with justification must be submitted to HQDA as outlined above.

e. Observation by Army investigators of demonstrations as described in paragraph 6*a*(4) above is authorized.

f. Upon receipt of information concerning threats described in paragraph 6*a*(5) above, appropriate personnel will be informed and all pertinent information furnished expeditiously to the local office of the Federal Bureau of Investi-

C-3

gation, to the local and state police and to HQDA (DAMI-DO).

g. Characterizations.

(1) For the purpose of this regulation, "characterizations" will only contain threat information as described in paragraph 6*a* above.

(2) When the commander of a major Army command or an Army installation commander identifies a need for a characterization concerning a specific person, group or organization, he will request one from HQDA (DAMI-DOA) WASH DC 20314, citing justification. Such characterizations will not be prepared locally.

(3) HQDA (DAMI-DOA) will disseminate such characterizations to Army commands, when required, for their use in protecting Army personnel, functions and property.

7. Operations related to civil disturbances. *a. General.* The Attorney General of the United States is the chief civilian officer in charge of coordinating all Federal Government activities relating to civil disturbances. The Secretary of the Army, as Executive Agent for the Department of Defense, relies upon the Department of Justice at the national level to furnish civil disturbance threat information required to support planning throughout the Department of Defense for military civil disturbance needs, and early warning of civil disturbance situations which may exceed the capabilities for control by local and state authorities. 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.

d. Planning. As an exception to the above limitation, overt acquisition and current maintenance of the following information by field commanders is authorized:

(1) Listing of local, State and Federal officials whose duties include direct responsibilities related to the control of civil disturbances.

(2) Data on vital public and commercial installations, facilities and private facilities believed to be appropriate targets for individuals or organizations engaged in civil disorders.

e. Acquiring, evaluating, and analyzing civil disturbance information within HQDA. The US Army Military Support Agency (USAMSA), Office of the Deputy Chief of Staff for Operations and Plans, DA, and the Office of the Assistant Chief of Staff for Intelligence (OACSI), DA, will be provided threat and early warning information by the Department of Justice. OACSI is the only agency authorized and responsible for processing this information. Any subsequent field collection and reporting of civil disturbance information must have the prior approval of the Secretary or Under Secretary of the Army.

f. Dissemination.

(1) Analyzed reports prepared by OACSI in accordance with subparagraph *e* above will be furnished appropriate field commanders only when specifically directed by the Secretary or Under Secretary of the Army. The dissemination of analyzed reports to the field does not authorize field commanders to acquire or process civil disturbance information. Analyzed reports provided by OACSI will be used for planning purposes. They will be retained by OACSI and by field commanders no longer than 60 days after the termination of the situation to which they pertain.

(2) Analyzed reports will be promptly disseminated within the Army Staff and Army

C-4

secretariat to those officials responsible for civil disturbance operations.

8. Storage. *a. Prohibition.* No Army element will retain in its files any information the acquisition of which is prohibited by this regulation.

b. Period of retention.

(1) *General.* Information acquired in accordance with this regulation will not be retained longer than the period set forth below unless its retention for a greater period is specifically required by law.

(2) *Information related to the protection of Army personnel, functions, and property.* Threat information falling within the categories listed in paragraph 6*a* above may be retained in the files subject to annual review and verification. At the time of the annual review, continued retention of information on individuals or organizations not affiliated with the Department of Defense is authorized only if—

(*a*) It is determined that the information was acquired properly under the provisions of paragraph 6*a* above and that the individual or organization falls into one of the following categories:

1. The individual or organization has been connected with an actual example(s) of violence or criminal hostility directed against an Army activity/installation/facility within the previous year.

2. The individual or organization has been connected with an explicit threat to Army personnel, functions or property within the previous year.

3. The individual's or organization's continuing hostile nature in the vicinity of Army installations continues to provide at the time of the annual review a significant potential source of harm to or disruption of the installation or its functions.

4. The individual or organization has, within the previous year, counseled or published information actively encouraging Army personnel to violate the law, disrupt military activities or disobey lawful regulations or orders.

(*b*) When, on the date of the annual review described above, an authorized investigation under paragraph 6*a* is in progress, information may be retained for a period of 1 year or until the investigation is completed, whichever occurs sooner. Any further retention must be authorized in accordance with this paragraph.

(3) *Civil disturbance information.*

(*a*) Civil disturbance information developed or acquired during an authorized period of field acquisition, reporting or processing activities must be destroyed within 60 days after the termination of the civil disturbance.

(*b*) After action reports and historical summaries of civil disturbance activities conducted by the US Army may be retained permanently but will avoid references to non-affiliated persons or organizations to the greatest extent possible.

(*c*) Planning information, as described in paragraph 7*d*, may be retained while the information is correct and current.

(4) *Published documents.* Library and reference material generally available to the general public may be retained without limitation. This material will not be maintained or inserted in subject or name files unless the information is retainable under other criteria authorized by this regulation.

(5) *Characterizations.* Only characterizations provided by HQDA will be maintained on file. A characterization so provided may be retained until the threat is locally determined to be non-existent or until notification is received from HQDA (DAMI-DOA) that it is rescinded or superseded, whichever is sooner. DAMI-DOA is responsible for conducting an annual review pursuant to paragraph 8*b*(2) above, of all characterizations on hand to verify their currency and validity, and for notifying all recipients when a characterization is rescinded or superseded.

(6) *Special investigations/operations.* Information acquired in the course of an approved special investigation/operation (paragraph 6*e* above) may be retained permanently by the US Army Investigative Records Repository. This includes information properly acquired prior to the conduct of the special investigation/operation and that acquired from any source during the course of the investigation/operation. However, once the special investigation/operation terminates, any new information properly acquired relating to non-affiliated subjects of the prior special investigation/operation is subject to normal retention criteria, including annual verification procedures.

(7) *Formerly affiliated person.* Investigative files of persons who were formerly affiliated with the Department of Defense may be retained for 15 years except that files which resulted in

C-5

adverse action against the individual will be retained permanently. However, once the affiliation is terminated, acquiring and adding material to the file is prohibited unless and until the affiliation is renewed or the material is otherwise retainable under this paragraph. In the latter instance, any new material is subject to annual verification procedures.

(8) *Universities conducting Department of Defense research.* Possession of a facility clearance by a university does not make the university affiliated for purposes of this regulation. Individual clearance holders at universities are affiliated with the Department of Defense and their investigative files are subject to the same standards for acquisition and retention as are those of other affiliated persons. Any Department of the Army facilities or property at universities may be included under the provision of paragraph 6*a*(1).

(9) *Filing of retainable information.* Inclusion of retainable information in a file relating to a particular Department of Defense installation or facility (rather than in dossiers on a non-affiliated group or person) does not exempt the file from the requirement for annual review and validation. Historical files, after action reports and other similar noninvestigative documents to the maximum extent will avoid inclusion of specific names of non-affiliated persons and organizations that have engaged in activities information about which may be required, reported, processed, and retained under this regulation.

(10) *Other categories.* As specified below, retention of information concerning certain non-affiliated persons or organizations whose activities involve them with the Department of Defense is authorized.

(*a*) Activities involving a one-time request for admission to installations (e.g., speakers, bands, drill teams). Retention is authorized for 1 year after the event.

(*b*) Activities involving a request that Army personnel attend or officiate at civilian sponsored meetings or ceremonies as representatives of the Army or DOD. Retention is authorized for 1 year after the event.

(*c*) Information resulting from activities involving requests from members of the public for photos or signatures of commanders, copies of unit insignia, or similar unit data. Retention is authorized subject to annual review for pertinency.

(*d*) Information resulting from activities involving an unsubstantiated report from members of the public alleging imminent invasions, terrorist plots and similar events of a delusional nature and assorted "crank" files may be retained in excess of 1 year subject to annual review for pertinency.

9. Prohibited activities related to persons and organizations not affiliated with the Department of Defense. *a.* No information will be acquired about a person or organization solely because of lawful advocacy of measures in opposition to US Government policy, or because of activity in support of racial and civil rights interests.

b. There will be no electronic surveillance of Federal, State or local officials or of candidates for such offices. There will be no physical surveillance of such persons except as indicated in paragraph 9*f* below.

c. There will be no electronic surveillance of any individual or organization except as authorized by law and regulation.

d. There will be no covert or otherwise deceptive surveillance or penetration of civilian organizations unless specifically authorized by the Secretary or the Under Secretary of the Army and, in the case of such activities conducted in the geographic areas set forth in paragraph 3*a*(1), after approval by the Chairman of the Defense Investigative Review Council.

e. No Army personnel, military or civilian, will be assigned to attend public or private meetings, demonstrations, or other similar activities held off-post to acquire information authorized by this regulation without specific approval by the Secretary or the Under Secretary of the Army. This prohibition includes any attempt to encourage or request the unofficial attendance of any persons at such events, whether or not such personnel have official counterintelligence or investigative responsibilities. An exception to the policy set forth in this paragraph is authorized a local commander when, in his judgment, the threat is direct and immediate and time precludes obtaining prior approval. In such cases a report will be made immediately to HQDA (DAMI-DOI).

f. The physical presence of a non-DOD affiliated person on an Army post or installation, in the absence of a threat as outlined in paragraph 9*a* above, does not warrant acquisition, reporting, processing, or storing of information on the in-

C-6

dividual. However, an installation commander may have any person or group of persons escorted while on post by uniformed personnel or their activities monitored by non-technical and non-deceptive methods, if considered necessary for post security. Military investigators may be directed to attend any meetings or demonstrations held on post.

g. No computerized data banks will be maintained containing information on civil disturbances or on persons and organizations not affiliated with the Department of Defense unless authorized by the Secretary or Under Secretary of the Army and after approval by the Chairman of the Defense Investigative Review Council.

h. Investigative checks may be made on relatives or associates of the affiliated subject of an authorized investigation if required by the scope of the authorized investigation. However, it is prohibited to make these associates or relatives the subject of an investigation or to cross reference their names in files to be retained. Information on any non-DOD affiliated subject, or in the case of investigations of other subjects conducted under the provisions of paragraph 6*a* of this regulation, may be retained in the subject's file. This information may be cross-referenced only if it falls within the criteria established in paragraph 6*a* of this regulation.

10. Relations with other agencies. *a.* Nothing in this regulation prohibits either the prompt reporting to law enforcement agencies of any information indicating either the existence of a threat to life or property, or violation of law, or prohibits keeping a record of such a report. Any threat to a person authorized protection by the US Secret Service should be treated expeditiously and reported to the nearest office of the Secret Service.

b. This regulation does not prohibit the receipt of information from all agencies in the course of liaison authorized by this regulation provided—

(1) such information is promptly screened; and

(2) information not authorized for the retention by this regulation is immediately destroyed.

c. The conduct of bilateral operations against foreign intelligence agencies in cases where a non-DOD agency has control is authorized. However, if the operation requires the penetration or the covert or otherwise deceptive surveillance of a domestic civilian organization by Army personnel, specific advance approval by the Secretary or Under Secretary of the Army and, in the case of such activities conducted in the geographic areas set forth in paragraph 5*a*(1), by the Chairman of the Defense Investigative Review Council is required.

d. A request from another agency for information does not provide authority for actions which would violate the provisions of this regulation.

e. The provisions of this regulation apply to Department of the Army personnel under the operational control of DOD. DA personnel under the operational control of another agency, or detailed, loaned or otherwise not under the operational control of DOD are exempt from the provisions of this regulation.

f. Access to information obtained under the provisions of this regulation will be restricted to any executive agency of the Federal Government, State or local agency having a legitimate need to know in connection with a matter of official business and processing appropriate clearance. In doubtful cases, the question of whether access should be provided to a particular agency should be referred to HQDA(DAMI-DO) for resolution.

11. Dissemination of policy. *a.* Copies of this regulation will be maintained in all offices where duties include the acquisition, reporting, processing, or storing of information covered by this regulation. All personnel in these offices are required to familiarize themselves thoroughly with the provisions of this regulation. Appropriate units/agencies/offices will maintain a copy of this regulation in a policy book reflecting that all assigned personnel have thoroughly read, familiarized themselves, understood, and will comply with the provisions thereof.

b. All commands and agencies will take immediate action to revise existing policy letters, regulations, or other guidance to insure consistency with this regulation. In case of conflict, this regulation will apply. Copies of major Army command regulations implementing this regulation will be furnished HQDA(DAMI-DOI-C).

c. Requests for exception or additions to the policies contained herein should be addressed through command channels to HQDA (DAMI-DO).

C-7

12. Verification, inspections, and reports. *a. Verification.* The person in charge of any headquarters or office in which files are maintained which contain information the retention of which is subject to this regulation will —

(1) Comply with the verification control procedures set forth in appendix C, this regulation.

(2) Verify and report to his immediate superior on an annual basis that all such information on file is authorized for retention. In doubtful cases, the person in charge will seek the guidance of his immediate superior if he is unable to determine whether or not retention is authorized.

b. Inspections. As a minimum, annual inspections at both operating and staff levels will be conducted to insure compliance with the provisions of this regulation.

c. Reports. Each major Army command, agency or activity subject to the requirements of this regulation, paragraph 3*a* above, will submit a letter report covering the preceding fiscal year to HQDA (DAMI-DO) WASH DC 20310, not later than 7 August annually. This report will reflect that an annual inspection of headquarters and subordinate elements was conducted to insure compliance with the provisions of this regulation and, if appropriate, corrective actions taken. The report will also contain a specific verification that the file holdings of the reporting command, agency or activity, and those of subordinate elements contain no information the retention of which is prohibited by this regulation. The Report Control Symbol for this report is DD–A(A) 1118.

APPENDIX A
GLOSSARY OF TERMS

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 initiated under AR 230–2 (Non-Appropriated Funds 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.

Characterization. A biographical sketch of a person or a statement of the nature and intent of an organization or group.

Civil Disturbance. Group acts of violence and disorders prejudicial to public law and order within the geographic areas listed in paragraph 3*a*(1) of this regulation. The term civil disturbance includes all domestic conditions requiring or likely to require the use of Federal armed forces pursuant to the provisions of Chapter 15 of Title 10 United States Code.

Civil Disturbance Information. All information on persons and organizations not affiliated with the Department of Defense and their activities, gathered to discharge the Army's civil disturbance responsibilities as outlined in paragraph 7 of this regulation. Information on actual and potential civil disturbances is included in this definition.

Collection. The acquisition of information in any manner, including direct observation, liaison or solicitation from official, unofficial or public sources.

Covert or otherwise deceptive surveillance. An activity designed to gather information which is planned and executed to conceal the identity of or permit plausible denial by the sponsor of the activity or when it is planned and executed so that it is reasonable to believe that the personnel involved are not associated with any military investigative agency.

Espionage. Overt, covert, or clandestine activity designed to obtain information relating to the national defense with intent or reason to believe that it will be used to the injury of the United States or to the advantage of a foreign government. For espionage crimes see Chapter 37 of Title 18, United States Code.

Investigation. A duly authorized, systematized, detailed examination or inquiry to uncover facts and determine the truth of a matter.

Investigative counterintelligence activities.

a. Investigative—Activities, other than counterintelligence activities as defined below, which are undertaken for one of the purposes described in paragraph 3*a*(4) of this regulation. Investigative activities include the collecting, processing, reporting, storing, recording, analyzing, evaluating, producing, and

C-9

disseminating of information within the scope of this regulation.

b. Counterintelligence—Activities, both offensive and defensive, designed to detect, neutralize or destroy the effectiveness of foreign intelligence activities.

Investigative/counterintelligence information. Includes all data developed as a result of investigative/counterintelligence activities, such as investigations, operations, and services, and through liaison with local, State, and Federal agencies. It may also be acquired from unsolicited sources, and from public sources, such as newspapers, magazines, books, periodicals, hand bills, and radio and television broadcasts. Authorities for investigations, operations, and services include AR 381-12, AR 381-14, AR 381-47, AR 381-115, AR 381-130, AR 604-5 and AR 604-10.

Key facility list (Key Defense Facilities). A list composed of selected critical industrial facilities, utilities, and Government-owned installations, located within the continental United States, which have been designated by the Secretary of Defense. The Panama Canal and those related operational facilities approved by HQDA for the purpose of this regulation, are to be treated as a key defense facility.

Local commander. Commissioned officer with a security responsibility for Army personnel, functions or property.

Overt. Conducted openly and in such a way that the sponsor is or may be known or acknowledged.

Penetration. The infiltration under Army auspices of an organization or group for the purpose of acquiring information.

Processing. The collation, evaluation and analysis of raw information to produce finished intelligence.

Reporting. Communicating information to another person or organization, whether orally, mechanically, electrically, in writing or otherwise.

Sabotage. An act, with intent to injure, interfere with, or obstruct the national defense of the United States by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war material, premises, or utilities, including human and natural resources. See Chapter 105, Title 18, United States Code.

Storage. The retention of data in any form, including card files, dossiers, folders, computers, microfilm, or punch cards, usually for a specified period, for the purposes of orderly retrieval and documentation.

Surveillance. The observation or monitoring of persons, places, or things by visual, aural, photographic, electronic (including COMSEC measures) or other physical means directed for the purpose of obtaining information.

Subversion of Army Personnel. Actions designed to undermine the loyalty, morale, or discipline of Army military or civilian personnel.

C-10

APPENDIX B

SPECIAL INVESTIGATION/OPERATION REQUEST FORMAT

Format. The following format will be used in submitting a request to conduct an off-post investigation/operation involving persons or organizations not affiliated with the Department of Defense.

1. *Threat Assessment.* A brief description of the target group and identification of the threat to the Department of Defense functions and property.

2. *Information Objectives.* A description of the essential information to be gathered and its relevance to present or future threats to the security of the Department of Defense.

3. *Concept of the Operations.* A brief description of the operation including timing, cover story, number of personnel involved, location of the target.

4. *Risk Analysis.* A discussion of the safety of the operatives, the vulnerability of the operation to compromise, the results and impact of any compromise, and contingency plans in the event of compromise.

VERIFICATION CONTROL

C–1. This appendix establishes uniform procedures for processing, purging and revalidating information acquired under the provisions of this directive.

C–2. *Newly acquired material.* All newly acquired material subject to this regulation shall be reviewed at the time of acquisition. If retention of the material is authorized, (Retention Control Sheet) DA Form 4312–R (Fig. C–1) will be prepared and affixed to the material. If retention is not authorized, the material will be forwarded to the appropriate civilian law enforcement agency or destroyed. When retained material is reproduced the DA Form 4312–R will be reproduced simultaneously and retained with the reproduced copies of the material. Supplies of DA Form 4312–R will be reproduced locally on 10½ by 8 in. paper.

C–3. *Existing file holdings. a.* US Army Investigative Records Repository (USAIRR).

(1) All dossiers on file at the USAIRR are being systematically purged. Pending completion of this purge and thereafter, whenever a USAIRR dossier is retrieved from file for any reason, it will be reviewed for retention under the criteria set forth in this regulation. Non-retainable material will be purged. If retention is authorized, a DA Form 4312–R will be completed and affixed to the dossier. A duplicate copy of the DA Form 4312–R will be maintained in a suspense file to assist in the management of the required annual review and verification procedure. If this suspense control is accomplished through data processing equipment, the duplicate suspense copy of DA Form 4312–R is not required.

(2) Information on file at the USAIRR in the form of reels of microfilm originated in Europe will be reviewed for retention whenever a reel is withdrawn from file for any reason. Non-retainable material will be purged. The use of DA Form 4312–R and annual verification are not required.

b. All other file holdings. All other Army elements holding files containing information authorized by this regulation will upon receipt of the regulation screen all such files for compliance with the retention criteria herein. Upon decision that retention of a file is authorized, a DA Form 4312–R will be completed and affixed. A duplicate copy of each DA Form 4312–R will be placed in a suspense file to assist in the management of the required annual review and verification procedure.

RETENTION CONTROL SHEET For use of this form, see AR 380-13; the proponent agency is OACSI.		DATE
SUBJECT		
INITIAL REVIEW		
DATE ACQUIRED/REVIEWED	RETENTION DECISION ☐ 60 DAYS ☐ 1 YEAR ☐ INDEFINITE	DATE TO BE DESTROYED/REVIEWED
REVIEWER'S SIGNATURE		OFFICE SYMBOL
ANNUAL REVIEW		
DATE REVIEWED	REVIEWER'S SIGNATURE	OFFICE SYMBOL
DATE REVIEWED	REVIEWER'S SIGNATURE	OFFICE SYMBOL

RETENTION CRITERIA
(Check One)

☐ 1. The individual or organization has been connected with an actual example(s) of violence or criminal hostility directed against an Army activity/installation/facility within the previous year. *(Para 8b(2)(a)1).*

☐ 2. An explicit threat to Army personnel, functions, or property within the previous year. *(Para 8b(2)(a)2).*

☐ 3. A continuing activity of a hostile nature in the vicinity of Army installations continues to provide at the time of the annual review a significant potential source of harm to or disruption of the installation or its functions. *(Para 8b(2)(a)3).*

☐ 4. Within the previous year, counseled or published information actively encouraging Army personnel to violate the law, disrupt military activities or disobey lawful regulations or orders. *(Para 8b(2)(a)4).*

☐ 5. Information acquired in connection with an authorized investigation in progress on the date of the annual review. Such information may be retained for one year or until the investigation is completed, whichever is sooner. Any further retention must be in accordance with other criteria listed on this form. *(Para 8b(2)(b)).*

☐ 6. Civil disturbance information developed or acquired during an authorized period of field acquisition, reporting and processing activities must be destroyed within 60 days after the termination of the civil disturbance. *(Para 8b(3)(a)).*

☐ 7. After action reports and historical summaries of civil disturbance activities conducted by the US Army may be retained permanently, but will avoid references to non-affiliated persons or organizations to the greatest extent possible. *(Para 8b(3)(b)).*

☐ 8. Planning information described in paragraph 7 may be retained while the information is correct and current. *(Para 8b(3)(c))*

☐ 9. Published documents such as library and reference material generally available to the general public may be retained without limitation. This material will not be maintained or inserted in subject or name files unless the information is retainable under other criteria listed on this form. *(Para 8b(4)).*

☐ 10. Only threat characterizations provided by HQDA will be maintained on file. A characterization so provided may be retained until the threat is locally determined to be nonexistent or until notification is received from HQDA that it is rescinded or superseded, whichever is sooner. *(Para 8b(5)).*

☐ 11. Special investigations/operations. Information acquired in the recourse of an approved special investigation/operation *(paragraph 6b)* may only be retained permanently by the US Army Investigation Records Repository. *(Para 8b(6)).*

☐ 12. Formerly affiliated persons. Subsequent to termination of affiliation, only threat information may be added to an individual's file subject to annual verification. *(Para 8b(7)).*

DA FORM 4312-R, 1 OCT 74

Figure C-1. DA Form 4312-R.

TAGO 177A

UNCLASSIFIED

DEPARTMENT OF THE ARMY
PENTAGON TELECOMMUNICATIONS CENTER

CDSN = SCP503 MCN = 78270/01763 TOR = 782702707
RTTUZYUW RUEADWD0684 2700205-UUUU--RUEAPPR RUEADWD.
ZNR UUUUU
R 261720Z SEP 78
FM DA WASHDC //DAMI-CIC//
TO AIG 7405
AIG 7406
AIG 7446
AIG 7447
ZEN/AIG 9053
ZEN/AIG 9054
RUDORRA/CDR 650TH MI GP SHAPE BELGIUM
ARSTAF
BT

UNCLAS
SUBJECT: CHANGE 1 TO AR 380-13
A. AR 380-13, ACQUISITION AND STORAGE OF INFORMATION CONCERNING NON-AFFILIATED PERSONS AND ORGANIZATIONS, DATED 30 SEP 74.
1. REFERENCE IS CHANGED AS FOLLOWS:
ON PAGE A-1, ADD TO SUBPARAGRAPH C UNDER AFFILIATION WITH DEPARTMENT OF DEFENSE: "INCLUDED IN THIS CATEGORY ARE COMMAND SPONSORED DEPENDENTS OF DA MILITARY AND CIVILIAN PERSONNEL LOCATED IN OVERSEAS AREAS NOTLISTEDIN PARAGRAPH 3A(1), THIS REGULATION. WITHIN AREAS CITED IN PARAGRAPH 3A(1), ONLY THOSE DEPENDENTS WHO RESIDE ON A DOD CONTROLLED INSTALLATION ARE AFFILIATED FOR THE PURPOSES OF THIS REGULATION UNLESS THEY FALL WITHIN ONE OR MORE OF THE OTHER AFFILIATED CATEGORIES."
2. DA GUIDANCE PREVIOUSLY PROVIDED WHICH CONFLICTS WITH THE ABOVE POLICY IS HEREBY RESCINDED.
BT
ACTION ADDRESSEES
207 ARSTAF-E (DA MEMO 105-1 APPLIES)
00207 TOTAL NUMBER OF COPIES REQUIRED
#0684

UNCLASSIFIED

C01724

PRIORITY

[illegible]
[illegible] 4-0000-[illegible]
[illegible] 00000
[illegible] 1542Z SEP
FM DA WASHDC // DAMI-DO//
TO AIG 7425
AIG 7406
AIG 7446
AIG 7447
ZEN/AIG 9253
ZEN/AIG 9054
RUDORRA/CDR 650TH MIG SHAPE BELGIUM
INFO ARSTAF
BT
UNCLAS
[illegible] INFORMATION CONCERNING TERRORIST ACTIVITIES
A. DIA CONTINUING INTELLIGENCE REQUIREMENT (CIR) 1-56A-49327.
SUBJECT: TERRORISM.
B. AR 380-13, ACQUISITION AND STORAGE OF INFORMATION CONCERNING NON-AFFILIATED PERSONS.
C. DAMI-DO MSG DTG 292030Z JUN 76, SUBJECT: IMPLEMENTATION OF EXECUTIVE ORDER 11905: UNITED STATES FOREIGN INTELLIGENCE ACTIVITIES.
1. IN ACCORDANCE WITH REFERENCE A, ARMY UNITS SHALL ACQUIRE INFOR-

MATION CONCERNING TERRORIST ACTIVITY ACTUALLY OR POTENTIALLY TARGETED AGAINST DOD. THE FOLLOWING PARAGRAPHS EXPLAIN THE PROVISIONS OF REFERENCES B&C CONCERNING THE COLLECTION OF INFORMATION AS THEY APPLY TO THE ACQUISITION OF SUCH TERRORIST INFORMATION.
2. AS USED IN THIS MSG, A "US PERSON" MEANS ANY U.S. CITIZEN, ANY ALIEN ADMITTED TO THE US FOR PERMANENT RESIDENCE, ANY ORGANIZATION OR GROUP COMPOSED IN SUBSTANTIAL PART OF SUCH INDIVIDUALS, OR ANY CORPORATION OR OTHER ORGANIZATION INCORPORATED OR ORGANIZED IN THE US. A NON-DOD AFFILIATED ORGANIZATION/GROUP LOCATED OVERSEAS IS A "US PERSON" ONLY IF IT IS COMPOSED "IN SUBSTANTIAL PART" OF NON-DOD AFFILIATED US CITIZENS/ALIENS ADMITTED TO THE US FOR PERMANENT RESIDENCE. HOWEVER, EVEN IF SUCH AN ORGANIZATION/GROUP IS NOT COMPOSED OF SUBSTANTIAL NUMBERS OF NON-DOD AFFILIATED US CITIZENS/ALIENS ADMITTED TO THE US FOR PERMANENT RESIDENCE, IT WILL BE CONSIDERED A US PERSON IF MEMBERS WHO ARE NON-DOD AFFILIATED US CITIZENS/ALIENS ADMITTED TO THE US FOR PERMANENT RESIDENCE OCCUPY PROMINENT POSITIONS AND/OR HAVE SIGNIFICANT INFLUENCE IN THE ORGANIZATION/GROUP.
3. THE FOLLOWING POLICY GOVERNS THE COLLECTION OF INFORMATION ON INDIVIDUALS AND ORGANIZATIONS WHO THREATEN TO OR ENGAGE IN TERRORIST

ACTS AGAINST DOD:

A. ALL SUCH INFORMATION ACQUIRED WILL BE BROADLY DISSEMINATED TO INCLUDE DIA IN ALL CASES AND THE FBI OR CIA AS APPROPRIATE.

B. WITHIN THE US (PARA 3A(1), REF B), INFORMATION SHALL BE ACQUIRED ONLY IF IT SATISFIES THE CRITERIA OF PARA [illegible], REF B. IF THE INFORMATION CONCERNS A NON-DOD AFFILIATED PERSON, REF B APPLIES AND A RETENTION CONTROL SHEET IS REQUIRED. IF THE INFORMATION CONCERNS A DOD AFFILIATED PERSON, REFERENCE C APPLIES AND PARA 2-7C, REF [illegible], REQUIRES THAT THE INFORMATION SATISFY THE THREAT CRITERIA IN PARA [illegible] OF REF B. NO RETENTION CONTROL SHEET IS REQUIRED.

C. OVERSEAS.

(1) SUCH INFORMATION ON DOD EMPLOYEES (AS DEFINED IN PARA 1-5F, REF C) AND NON-US PERSONS (FOREIGNERS) WILL BE COLLECTED AND STORED. RETENTION CONTROL SHEETS ARE NOT REQUIRED.

(2) SUCH INFORMATION ON NON-DOD AFFILIATED US PERSONS WILL BE COLLECTED ONLY IN ACCORDANCE WITH THE PROVISIONS OF PARA A, REF B. RETENTION CONTROL SHEETS ARE REQUIRED.
4. AR 380-13 PARA 10A DOES NOT PROHIBIT THE PROMPT REPORTING TO APPROPRIATE LAW ENFORCEMENT AGENCIES OF INFORMATION INDICATING THE EXISTENCE OF ANY THREAT TO LIFE AND/OR PROPERTY [illegible] VIOLATION OF LAW.

[illegible] SCHCOA

C-15

[illegible] EAGLE [illegible] OF US [illegible]

IF THE INFORMATION IS NOT RETAINABLE UNDER AR 380-13, NO RECORD OF IT WILL BE RETAINED ONCE IT IS REPORTED TO LAW ENFORCEMENT AUTHORITIES.

3. THIS MESSAGE DOES NOT APPLY TO AUTHORIZED CRIMINAL INVESTIGATION AND LAW ENFORCEMENT INFORMATION GATHERING ACTIVITIES (I.E., THOSE ACTIVITIES NOT "COUNTERINTELLIGENCE RELATED" WHICH ARE THE RESPONSIBILITY OF MILITARY POLICE AND THE US ARMY CRIMINAL INVESTIGATION COMMAND. SUCH ACTIVITIES WILL CONTINUE TO BE CONDUCTED IN ACCORDANCE WITH APPLICABLE REGULATIONS.

4. THIS MESSAGE WAS COORDINATED WITH THE OFFICE OF TJAG AND DISTEL, [illegible], AND THE ARMY GENERAL COUNSEL.

ET

#3800

Called Mr. Nicholson 1535 26 Sep

NNNN

ZYUW RUEOBNA0510 2221937-UUUU--RUEOBNA.
UUUUU
Z 191937Z AUG 77
FM 7TH SIG COMD FT RITCHIE MD//CCN-IS//
TO [illegible] SIG 831
[illegible] 192137Z AUG 77
FM [illegible]DA WASHDC//DAPE-HRE-PO//
TO AIG 7300
AIG 7405
AIG 7406
AIG 7407
AIG 7446
AIG 7447
RULGSAA/TAG ST. CROIX, VI
ZEN/AIG 9053
ZEN/AIG 9054
INFO ARSTAF
RUCLBWA/CMDT USAMPS, FT MCCLELLAN AL//
BT
UNCLAS
SUBJ: CHANGE TO AR 190-40, SERIOUS INCIDENT REPORT, (SIR) AND CLARIFICATION REFERENCE REPORTING OF NON-DOD-AFFILIATED INFORMATION

C01447

RECEIVED AUG 18

PAGE 02 RUEOBNA0510 UNCLAS
REFERENCES:
A. AR 190-40, 21 MAR 77
B. AR 380-13, 30 SEP 74
1. INFORMATION PERTAINING TO IDENTIFIED NON-DOD-AFFILIATED PERSONS / ORGANIZATIONS SUBMITTED IN THE TEXT OF AN SIR IAW REF A IS SUBJECT TO PROVISIONS OF REF B, EXCEPT WHEN ADDRESSEES/USERS ARE EXEMPTED BY PARA 3B, REF B.
2. ADDRESSEES/USERS NOT EXEMPT FROM PROVISIONS OF REF B, BUT RECEIVING SUCH REPORTS, ARE REMINDED THAT, AT THE TIME OF RECIEPT, ALL INFORMATION PERTAINING TO NON-DOD-AFFILIATED PERSONS AND ORGANIZATIONS MUST BE REVIEWED TO DETERMINE IF RETENTION IN AUTHORIZED IAW REF B AND, IF RETAINED, A DA FORM 4312-R (APP C, REF B) WILL BE PREPARED AND AFFIXED TO THE MATERIAL.
3. TO FACILITATE CONTROL OF REPORTS CONTAINING IDENTIFIABLE NON-DOD-AFFILIATE INFORMATION BY ADDRESSEES/USERS OF SIR REPORTS, HOLDERS OF REF A WILL MAKE THE FOLLOWING CHANGE.
ADD PARA 3-11: REPORTS CONTAINING INFORMATIONS IDENTIFYING NON-DOD-AFFILEATED PERSONS AND ORGANIZATIONS WILL CONTAIN THE FOLLOWING AT THE END OF THE SUBJECT LINE: (NAFFO); E.G., SUBJECT: SIR NUMBER 770001 (NAFFO). THE LAST SENTENCE OF THE LAST PARAGRAPH OF THE SIR WILL CONTAIN THE

PAGE 03 RUEOBNA0510 UNCLAS
FOLLOWING STATEMENT: "THIS REPORT CONTAINS INFORMATION PERTAINING TO NON-DOD-AFFILIATED PERSON(S)/ORGANIZATION(S) AND IS SUBJECT TO PROVISIONS OF AR 380-13, EXCEPT WHERE ADDRESSEE/USER IS EXEMPTED BY PARAGRAPH 3B, THEREOF."
INFORMATION CONTAINED HEREIN WILL BE INCORPORATED IN FUTURE REVISION OF REF A.
BT
#0510

U.S. ARMY
ADJUTANT GENERAL'S SCHOOL

PJA
Cpt Beeson

DEPARTMENT OF THE ARMY
PENTAGON TELECOMMUNICATIONS CENTER

CDSN = SC0545 MCN = 76279/10785 TOR = 762791824
PTTUZYUW RUEADWD1005 2791824-UUUU--RUEAPPP RUEADWD.
ZNR UUUUU
P 051827Z OCT 76
FM DA WASHDC //DAMI-DOS//
TO AIG 7405
AIG 7406
AIG 7446
AIG 7447
RUDORRA/CDR 650TH MI GP SHAPE BELGIUM
ARSTAF
BT

Bill Dawson
7071's

UNCLAS
SUBJECT: ACQUISITION AND STORAGE OF INFORMATION CONCERNING NON-AFFILIATED PERSONS AND ORGANIZATIONS (RCS DDA(A) 1118)
A. ~~AR 380-13~~ SUBJECT AS ABOVE.
B. DA MSG 081651Z APR 76, SUBJECT: CHANGE IN DUE DATE, AR 380-13 ANNUAL VERIFICATION/INSPECTION REPORT.
C. DA MEMORANDUM 380-13, DATED 29 MARCH 1976, SUBJECT AS ABOVE.
1. THE PURPOSE OF THIS MSG IS TO REMIND ADDRESSEES OF THE ANNUAL REPORTING REQUIREMENT CONTAINED IN PARA 12C OF AR 380-13 AND IN PARA 3A(3), DA MEMO 380-13.
2. REFERENCE B ADVISED THAT THE ANNUAL AR 380-13 VERIFICATION/INSPECTION REPORT IS DUE TO REACH HQDA (DAMI-DOS) NLT 7 NOV 76.
3. MACOMS AND HQDA STAFF AGENCIES WILL CONSOLIDATE REPORTS SUBMITTED BY SUBORDINATE ELEMENTS.
BT
ACTION ADDRESSEES
102 ARSTAF-A (DA MEMO 105-1 APPLIES)
00102 TOTAL NUMBER OF COPIES REQUIRED
#1005

P