Headquarters
Department of the Army
Washington, DC
27 January 2023

***Army Regulation 381–10**

Effective 27 February 2023

Military Intelligence

The Conduct and Oversight of U.S. Army Intelligence Activities

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:

MARK F. AVERILL
Administrative Assistant
to the Secretary of the Army

History. This publication is a major revision. The portions affected by this major revision are listed in the summary of change.

Authorities. The authorities for this regulation are Executive Order 12333, 10 USC 7013, DoDD 5240.01, DoDD 5148.13, DoDM 5240.01, and DoD 5240.1–R.

Applicability. This regulation applies to the Regular Army, the Army National Guard/Army National Guard of the United States and the U.S. Army Reserve. It also applies to anyone employed by, assigned to, or acting for Army intelligence elements when conducting intelligence activities under SECARMY authorities.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff, G–2. The Army General Counsel, in coordination with The Judge Advocate General, has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific requirements.

Army internal control process. This regulation contains internal control provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see appendix B).

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Deputy Chief of Staff, G–2, 1000 Army Pentagon, Washington, DC 20310–1000.

Distribution. This publication is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

*This regulation supersedes AR 381-10, dated 3 May 2007.

Contents (Listed by chapter and page number)

Chapter 1
Introduction

Section I

General

1–1. Purpose
This regulation implements DoDD 5148.13, DoDM 5240.01 and establishes policy and procedures for the conduct and oversight of Army intelligence and intelligence-related activities. Army intelligence activities include intelligence activities conducted under Secretary of the Army (SECARMY) authorities and the training to conduct intelligence activities by Army personnel. These policies are intended to ensure Army intelligence activities are conducted in a manner that uses all reasonable and lawful means to gain timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, and protects the constitutional and legal rights and the privacy and civil liberties of U.S. persons. This regulation also imposes reporting requirements for Army personnel conducting intelligence activities under the authority of a combatant commander.

1–2. References, forms, and explanation of abbreviations
See appendix A. The abbreviations, brevity codes, and acronyms (ABCA) used in this electronic publication are defined when you hover over them. The abbreviations used in this publication are listed in the abbreviations, brevity codes, and acronyms database located at https://armypubs.army.mil/abca/searchabca.aspx.

1–3. Associated publications
Policies associated with this regulation are found in DoDD 5240.01, DoDD 5148.13, DoDM 5240.01, and DoD 5240.1–R.

1–4. Responsibilities
Responsibilities are listed in section II of chapter 1.

1–5. Records management (recordkeeping) requirements
The records management requirements for all record numbers, associated forms, and reports required by this regulation are addressed in the Records Retention Schedule-Army (RRS–A). Detailed information for all related record numbers, forms, and reports are located in Army Records Information Management System (ARIMS)/RRS–A at https://www.arims.army.mil. If any record numbers, forms, and reports are not current, addressed, and/or published correctly in ARIMS/RRS–A, see DA Pam 25–403 for guidance.

1–6. Legal advice, conflicts with other policies, and understanding terminology
a. Legal advice. Commanders will seek legal advice from their supporting U.S. legal advisor. Commanders must obtain a written legal review—

(1) Prior to the conduct of electronic surveillance, concealed monitoring, physical searches, searches of mail and the use of mail covers, physical surveillance, or undisclosed participation in an organization in support of an intelligence mission (hereafter collectively referred to as special collection techniques) which are conducted in accordance with DoDM 5240.01.

(2) Prior to contracting for goods and services, providing assistance to civilian law enforcement authorities and other civil authorities, or conducting research involving human subjects for intelligence purposes which are executed in accordance with DoDD 5240.01, DoD 5240.1–R, or any successor documents.

(3) When requesting intelligence operational authorities (that is, operational proposals, counterintelligence special operations concepts, and so forth).

(4) Legal advisors will assist commanders in executing their responsibilities to ensure personnel and organizations understand and comply with laws, directives, regulations, and established intelligence oversight policies and principles regarding the conduct of intelligence activities; and to ensure compliance with policies pertaining to investigations, reporting, tracking, and documenting of questionable intelligence

activities (QIAs), significant or highly sensitive matters (S/HSM), and the reporting of Federal crimes as required.

b. Conflicts with other policy. If provisions in this regulation conflict with Department of Defense (DoD) policy, DoD policy takes precedence.

c. Understanding terminology. DoDM 5240.01 and DoDD 5148.13 use carefully defined terms that intelligence elements, commanders, and legal advisors must read and understand when executing intelligence and intelligence-related activities.

Section II

Responsibilities

1–7. The General Counsel

The GC is the legal counsel to the SECARMY and the chief Department of the Army (DA) legal officer. The General Counsel's responsibility extends to any subject of law and other matters as directed by the SECARMY. The General Counsel will—

a. Exercise the SECARMY's oversight of intelligence activities and monitor sensitive Army intelligence activities for legality and propriety.

b. In conjunction with The Judge Advocate General (TJAG) of the Army and the Deputy Chief of Staff (DCS), G–2, develop and oversee policies and programs for Army intelligence and counterintelligence.

c. Ensure the SECARMY reviews and approves any proposed intelligence operational activity that has the potential to be viewed as controversial or could create the appearance of impropriety or otherwise be embarrassing to the Army.

d. Designate the Office of the General Counsel (OGC) senior intelligence and security legal advisor to serve as the Army's senior intelligence oversight official (SIOO) who will—

(1) Review intelligence issues before any Secretariat official decision.

(2) Conduct all formal Army coordination with Department of Justice (DOJ) senior officials regarding intelligence matters.

(3) Review for concurrence certain intelligence oversight activities as listed in this regulation.

(4) Forward reports of Federal crimes that meet the Attorney General's guidelines for reporting through the DoD General Counsel to the DOJ.

(5) Review all matters that raise questions of interpretation concerning the procedures and activities covered by this regulation that cannot be resolved at lower echelons.

(6) Review, in coordination with TJAG, all requests for exception, waiver, modification, or amendment of policies covered by this regulation.

(7) Maintain direct liaison with the DoD SIOO.

(8) Coordinate with the Army Inspector General to ensure proper reporting, investigation, and resolution of reported QIAs and S/HSMs.

(9) Review and process requests for identities of U.S. persons in disseminated intelligence and counterintelligence reports as specified in chapter 6.

1–8. The Chief Information Officer

The CIO will—

a. Provide Civil Liberties, Privacy, and Transparency advice with respect to the conduct and oversight of U.S. Army intelligence activities when requested.

b. Coordinate with the DCS, G 2 for reports sent to the Director of National Intelligence (DNI) under chapter 6 of this regulation.

1–9. The Inspector General

TIG will—

a. Conduct oversight inspections of intelligence activities as prescribed by AR 20–1 and this regulation.

b. Maintain liaison with the DoD SIOO.

c. Receive and process all QIA or S/HSM reports and ensure the reported incidents are investigated or forwarded to appropriate authorities for investigation.

d. Ensure reports of QIA and S/HSM are forwarded to appropriate officials as required.

e. Prepare a quarterly report to the DoD SIOO of QIAs and S/HSMs reported during that quarter and any resultant actions. Include significant intelligence oversight activities and inspections, identified trends, and suggestions for improvements in the oversight process.

f. Review for potential policy changes, conflicts, or significant trends, the Department of the Army Inspector General (DAIG) for intelligence oversight quarterly summary of QIA and S/HSM incidents with the DCS, G-2's Army intelligence oversight program manager (AIOPM).

g. Ensure that subordinate command inspectors general are knowledgeable of intelligence oversight programmatic requirements to conduct AR 20–1-directed intelligence oversight inspections.

1–10. The Chief of Legislative Liaison

The CLL will process requests for identities of U.S. persons in disseminated intelligence and counterintelligence reports as specified in chapter 6.

1–11. The Deputy Chief of Staff, G–2

The DCS, G–2 will—

a. Exercise Army staff responsibility for intelligence oversight and be responsible for the propriety of U.S. Army intelligence activities as the Army's senior intelligence officer (SIO) and Defense Intelligence Component head as defined in DoDM 5240.01.

b. Develop, in conjunction with the General Counsel and TJAG, policies and programs for Army intelligence and intelligence oversight. Plan and supervise the execution of those policies and programs.

c. Review and approve procedures related to intelligence collection, retention, or dissemination as described in this regulation.

d. Maintain appropriate web pages for current policy interpretation, references, and training materials.

e. Provide intelligence oversight support to 650th Military Intelligence (MI) Group intelligence activities upon request.

f. Review and process requests for identities of U.S. persons in disseminated intelligence and counterintelligence reports as specified in chapter 6.

g. Designate and appoint in writing an intelligence professional to serve as the Army AIOPM and DCS, G–2 intelligence oversight officer (IOO). The AIOPM must have access to all Army intelligence activities, to include intelligence activities protected by special access programs, alternative or compensatory control measures, and other security compartments. The AIOPM must have reasonable access to the DCS, G–2 or their delegee to monitor oversight compliance and will be rated by the Army SIOO. The AIOPM will—

(1) Serve as the DCS, G–2 IOO and primary staff officer responsible for coordinating the DCS, G-2's responsibilities for intelligence oversight and related matters.

(2) Support the Army SIOO in the execution the SECARMY's oversight of intelligence activities.

(3) Coordinate with TIG for the monitoring of all investigations of QIA and S/HSM.

(4) Coordinate required DA or higher-level requests for special collection procedural approvals.

(5) Participate in DAIG intelligence oversight and externally mandated inspections, as required.

(6) Conduct staff assistance visits to Army elements conducting intelligence activities, as needed.

(7) In conjunction with the Army SIOO and TIG, develop and implement an intelligence oversight checklist for use by Army intelligence elements to ensure compliance with this policy.

(8) Coordinate with the Commanding General (CG), U.S. Army Training and Doctrine Command (TRADOC), through the CG, U.S. Army Intelligence Center of Excellence (ICoE), to develop an IOO course and intelligence oversight training within all ICoE programs of instruction.

(9) Serve as the DCS, G-2's Civil Liberties, Privacy, and Transparency official.

h. The Commander, U.S. Army Intelligence and Security Command (INSCOM) will—

(1) Exercise responsibility for the legality and propriety of INSCOM intelligence activities, as a Defense Intelligence Component head as specified in DoDM 5240.01.

(2) As the Service Cryptologic Component Commander, be responsible for the compliance by all Army signals intelligence (SIGINT) activities with the policies, tasking, and technical guidance provided by the DoD and the Director, National Security Agency (DIRNSA)/Chief, Central Security Service (CHCSS), and coordinate with the DIRNSA and CHCSS for the oversight of Army units performing DIRNSA-authorized SIGINT missions.

(3) Approve or delegate approval authority for those procedures specified in this regulation.

(4) Ensure INSCOM employees report QIA, S/HSM, and Federal crimes defined in this regulation.

(5) Include the authorities and limitations on intelligence activities that will collect, retain, or disseminate U.S. person information (USPI) in force protection plans and procedures.

(6) Designate in writing intelligence professionals to serve as the INSCOM intelligence oversight and compliance advisor (IOCA) and Deputy IOCA. The IOCA and Deputy IOCA must have direct access to the CG, INSCOM and serve as the primary and alternate IOOs.

(7) Assist subordinate organizations in the development of intelligence oversight programs.

(8) Validate or certify the Army SIGINT workforce is trained to DIRNSA/CHCSS-established standards and appropriately cleared to perform duties across the United States Cryptologic System.

(9) Assist DIRNSA/CHCSS in the development of SIGINT oversight training relevant and readily available to Army elements. Coordinate and advise with the CG, TRADOC to ensure DIRNSA/CHCSS required SIGINT oversight training is included in Army training.

(10) Publish intelligence oversight program guidance for all major subordinate commands and ensure compliance with this regulation.

i. The Commander, 650th MI Group will—

(1) Exercise responsibility for the legality and propriety of 650th MI Group intelligence activities.

(2) Ensure compliance with this regulation.

(3) Include the authorities and limitations on intelligence activities that collect, retain, or disseminate USPI in force protection plans and procedures.

(4) Ensure requests for approval of 650th MI Group intelligence activities are reviewed by a U.S. legal advisor familiar with DoD and Army intelligence policy. The 650th MI Group may request this support from Office of The Judge Advocate General (OTJAG) when the 650th MI Group legal advisor is not available.

(5) Designate intelligence professionals in the intelligence operational chain to function as the command's primary and alternate IOOs. Ensure the individuals appointed to perform IOO duties are knowledgeable of all the issuances associated with North Atlantic Treaty Organization-related intelligence activities.

(6) Establish internal organizational reporting responsibilities pursuant to the unit's internal policies and regulations.

(7) Ensure all 650th MI Group employees report QIA, S/HSM, and reportable Federal crime reports in accordance with the reporting requirements of this regulation.

1–12. The Chief, National Guard Bureau

The CNGB will—

a. Ensure that all Army National Guard (ARNG) personnel understand that conducting intelligence activities, as defined in DoDM 5240.01, is exclusively a Federal mission and may only be conducted in Title 10 status. ARNG personnel may perform training for intelligence functions in Title 10 or Title 32 status.

b. Ensure that ARNG personnel refer questions on the authority for conducting intelligence activities in Title 10 or Title 32 status to their servicing legal office or the Army SIOO.

c. Ensure that all ARNG intelligence personnel and personnel assigned to an ARNG intelligence element—

(1) Are trained to comply with law, Executive orders (EO), intelligence community directives, DoD policy, and Army policy.

(2) Receive intelligence oversight training that complies with the requirements in DoDD 5148.13 and this regulation.

(3) Are trained to execute any Title 10, United States Code (10 USC) mission for which the ARNG is mobilized.

d. Include the authorities and limitations on intelligence activities that collect, retain, or disseminate USPI in force protection plans and procedures.

e. Ensure intelligence professionals in the intelligence operational chain are designated to function as the command's primary and alternate IOOs.

1–13. The Judge Advocate General

TJAG will—

a. Provide legal advice directly to the SECARMY, Chief of Staff of the Army, the Secretariat, and members of the Army Staff.

b. Develop and oversee, in conjunction with the General Counsel and DCS, G–2, policies and programs for Army intelligence and counterintelligence. Oversee, in coordination with the General Counsel, sensitive activities and counterintelligence investigations.

c. Review for legal sufficiency requests of special collection techniques submitted to the DCS, G–2 for approval under the provisions of this regulation.

d. Provide appropriate intelligence law and policy instruction.

e. Review, in coordination with the Army General Counsel, all requests for exception, waiver, modification, or amendment of policies and procedures covered by this regulation.

f. Upon request, provide legal advice to the 650th MI Group on intelligence oversight issues.

1–14. The Provost Marshal General

The PMG will—

a. Ensure AR 190–45 includes a means to report Federal crimes directly to the OGC and DCS, G–2 as described in chapter 5.

b. In coordination with the Army SIOO, assist the Assistant Secretary of the Army (Manpower and Reserve Affairs) in developing law enforcement policy to include information describing the difference between criminal intelligence and foreign intelligence and counterintelligence; associated authorities and limitations; and the collection, retention, and dissemination of USPI.

1–15. The Commanding General, U.S. Army Forces Command

In addition to paragraph 1–17, the CG, FORSCOM will ensure that the Commander, U.S. Army Reserve Command will—

a. Ensure compliance with DoDM 5240.01, DoD 5240.1–R, and this regulation.

b. Ensure, through their SIO or the DCS, G–2, the propriety of command intelligence activities.

c. Ensure QIA, S/HSM, and Federal crimes reporting procedures exist within U.S. Army Reserve elements.

d. Designate intelligence professionals in the intelligence operational chain to function as the command's primary and alternate IOOs.

1–16. The Commanding General, U.S. Army Training and Doctrine Command

In addition to paragraph 1–17, the CG, TRADOC will—

a. Through the ICoE, and in close coordination with the Army SIOO, DCS, G–2 and AIOPM, develop an IOO course and intelligence oversight training within all ICoE programs of instruction.

b. Give credit for completing IOO courses conducted by other agencies and certified by the Army SIOO as providing training that is equivalent to the Army IOO course.

c. Develop SIGINT oversight training programs, in close coordination with the Commander, INSCOM; IOCA; Army Cryptologic Operations; and National Security Agency/Central Security Service.

d. In consultation with the Army SIOO, incorporate intelligence oversight training into pre-command courses and senior leadership courses for those commanders with subordinate intelligence elements.

e. Ensure doctrine addresses the limitations on intelligence activities regarding the collection, retention, and dissemination of USPI.

1–17. The Commanders, Army commands

The Commanders, ACOMS will—

a. Ensure, through their SIO or the Assistant Chief of Staff G–2, the propriety of command intelligence activities.

b. Ensure compliance with DoDM 5240.01, DoD 5240.1–R, and this regulation when conducting intelligence activities under SECARMY authorities.

c. Publish intelligence oversight program guidance.

d. Include the authorities and limitations on intelligence activities that collect, retain, or disseminate USPI in force protection plans and procedures.

e. Designate intelligence professionals in the intelligence operational chain to function as the command's primary and alternate IOOs.

1–18. The Commanders, Army service component commands

The Commanders, ASCCs will—

a. Ensure, through the SIO or the Assistant Chief of Staff, G–2, the propriety of command intelligence activities.

b. Ensure compliance with DoDM 5240.01; DoD 5240.1–R; and the training, oversight, and reporting requirements of this regulation.

c. Publish intelligence oversight program guidance.

d. Include the authorities and limitations on intelligence activities that collect, retain, or disseminate USPI in force protection plans and procedures.

e. Notify the Commander, INSCOM when INSCOM personnel will execute special collection techniques under the command's operational control and approval.

f. Designate intelligence professionals in the intelligence operational chain to function as the command's primary and alternate IOOs.

1–19. The Agency Head/Commanders, direct reporting units with an Army intelligence element

The Commanders of DRUs with an Army intelligence element will—

a. Ensure, through the SIO or the Assistant Chief of Staff, G–2, the propriety of command intelligence activities.

b. Ensure compliance with DoDM 5240.01, DoD 5240.1–R, and this regulation.

c. Publish intelligence oversight program guidance.

d. Include the authorities and limitations on intelligence activities that collect, retain, or disseminate USPI in force protection plans and procedures.

e. Notify the Commander, INSCOM when INSCOM personnel will execute collection techniques under the command's operational control and approval.

f. Designate intelligence professionals in the intelligence operational chain to function as the command's primary and alternate IOOs.

1–20. The Army Inspectors Generals

The Army IGs will—

a. As part of their inspection program, determine if Army intelligence elements are conducting intelligence activities in compliance with law, EOs, intelligence community directives, DoD policy, and Army policy.

b. Determine whether inspected elements are involved in any QIA or S/HSM. If an inspection discovers a QIA or S/HSM, inspector generals will report the matter in accordance with chapter 4 of this regulation.

c. Ascertain whether any organization, staff, or office not specifically identified as an Army intelligence element is being used for foreign intelligence or counterintelligence purposes and, if so, ensure its activities comply with this regulation.

d. Ascertain whether any organization, staff, or office not specifically identified as an Army intelligence element is conducting intelligence or counterintelligence activities without an assigned mission to do so. If the inspections identify an element within an Army unit that is conducting intelligence or counterintelligence activities without an assigned mission to do so, TIG will report the matter in accordance with chapter 4 of this regulation.

e. Evaluate leadership awareness and understanding of intelligence authorities governing the collection, retention, and dissemination of USPI.

f. Determine whether inspected elements' approved SIGINT missions comply with National Security Agency/Central Security Service policies and directives.

g. Determine whether procedures exist within each element for reporting QIA, S/HSM, and Federal crimes, and that personnel are aware of their reporting responsibility.

h. Provide advice to commanders and IOOs as needed.

1–21. The Commanders of U.S. Army organizations that conduct intelligence activities or intelligence training under Secretary of the Army authority

The Commanders of U.S. Army organizations that conduct intelligence activities or intelligence training under SECARMY authority will—

a. Ensure all assigned or attached MI personnel conducting intelligence activities do so in accordance with law, EOs, intelligence community directives, DoD policy, and Army policy.

b. Ensure MI personnel conducting intelligence activities are fully aware of and comply with their individual responsibilities as prescribed in this regulation.

c. Include intelligence oversight as part of the command's organizational inspection program.

d. Ensure the auditability of USPI collected, retained, and disseminated in accordance with DoDM 5240.1 and this regulation.

e. Establish documented procedures for retaining data containing USPI and recording the reason for retaining the data and the authority approving the retention, and establish procedures to document the basis for conducting queries of unevaluated information that is intended to reveal USPI, if needed.

f. Establish internal organizational intelligence oversight reporting responsibilities pursuant to the unit's internal policies and regulations.

g. Administer an intelligence oversight training program that is mission specific and tailored to unique unit requirements and provides initial and annual refresher intelligence oversight training to all MI employees. At a minimum, intelligence oversight training will include—

(1) Familiarity with the authorities, restrictions, and procedures established in this regulation, DoDD 5148.13, DoDD 5240.01, DoDM 5240.01, DoD 5240.1–R, and all other applicable intelligence community directives, DoD issuances, and Army policies governing applicable intelligence activities, including training for MI employees who access or use USPI on the civil liberties and privacy protections that apply to such information, and training on DoDM 5240.01, Procedure 4 for MI employees who might disseminate USPI.

(2) Responsibilities of DoD personnel and DoD contractor personnel for reporting QIAs or S/HSMs in accordance with DoDD 5148.13 and chapter 4 of this regulation.

h. Ensure all employees complete intelligence discipline specific training required for the conduct of intelligence activities.

i. Ensure that no one under their command retaliates against employees who report waste, fraud, or abuse per AR 20–1.

j. Ensure that no one under their command takes adverse action against any DoD personnel or DoD contractor personnel because they intend to report, report, or reported what they reasonably believe are—

(1) QIAs.

(2) S/HSMs.

(3) Facts or circumstances that reasonably indicate to the employee that an employee of an intelligence agency has committed, is committing, or will commit a violation of Federal criminal law.

(4) Facts or circumstances that reasonably indicate to the employee that a non-employee has committed, is committing, or will commit one or more of the specified crimes in Section VII of the 1995 DOJ Memorandum of Understanding for the Reporting of Information Concerning Federal Crimes.

k. Ensure appropriate sanctions, disciplinary, or administrative actions are imposed upon any employee who violates an EO, presidential directive, or any regulatory policy or procedures implementing the provisions of EO 12333.

l. Provide the command's legal counsel; DCS, G–2; TIG; TJAG; Army General Counsel; DoD General Counsel; DoD SIOO; and any inspector general of competent jurisdiction (or the representatives of those officials) with access to any employee and with all information necessary to perform their intelligence oversight responsibilities, including information protected by special access programs, alternative compensatory control measures, or other security compartmentalization.

m. Ensure employees cooperate fully with the President's Intelligence Oversight Board and its representatives.

n. Ensure all proposals for intelligence activities that may be unlawful, in whole or in part, or may be contrary to policy, will be referred to TIG, TJAG, or the Army General Counsel.

o. Designate intelligence professionals in accordance with para 1–24 in the intelligence operational chain to function as the command's primary and alternate IOOs.

p. Ensure contractors involved in the conduct of intelligence activities comply with law, applicable federal regulations, and the terms and conditions of the applicable contract or agreement. Commanders will ensure that contracts for the conduct of intelligence activities explicitly incorporate the relevant provisions of AR 381–10.

q. Maintain records documenting compliance with intelligence oversight training.

r. Implement reporting procedures for QIA, S/HSM, Federal crimes, and violations of Army-specific intelligence policies in accordance with DoDM 5240.01 and this regulation.

1–22. Intelligence oversight officers

All IOOs will—

a. Represent commanders in matters of intelligence oversight, ensuring all MI personnel within the command are familiar with law, EOs, intelligence community directives, DoD policy, and Army policy regarding the conduct of intelligence activities.

b. Provide advice and assistance with respect to intelligence oversight; keep leadership informed on new policy and guidance; monitor intelligence oversight training; and oversee all unit intelligence activities, operations, and reporting.

c. Assist the commander in ensuring the unit's intelligence activities are conducted and consistent with applicable law, EOs, intelligence community directives, DoD policy, Army policy, and established oversight principles.

d. Assist in the implementation of the commander's intelligence oversight program.

e. Develop mission specific intelligence oversight training and education programs and participate when available.

f. Ensure compliance with requirements regarding the investigation, reporting, tracking, and documenting of QIA, S/HSM, and reportable Federal crimes in accordance with DoDD 5148.13 and this regulation.

g. Review all unit requests for intelligence operational authorities and the use of procedures governing the conduct of DoD intelligence activities prior to approval.

h. Assist the commander in ensuring all personnel periodically review intelligence databases to ensure the retention of USPI is consistent with DoDM 5240.01 (specifically, that USPI is retained only for authorized functions and is not held beyond any evaluation period prior to a permanent retention decision or beyond the established disposition criteria).

i. Prepare subordinate units for intelligence oversight inspections and conduct inspections or assessments of subordinate unit programs.

j. Successfully complete all intelligence discipline specific oversight training within 30 days of appointment as the IOO, and any subsequent Army IOO course or equivalent certified under para 1–16 within 180 days of appointment.

k. Assist the commander in ensuring all personnel in their unit complete intelligence oversight training in accordance with this regulation.

l. Monitor and maintain unit training statistics to ensure compliance.

m. Assist Inspectors General in the review and inspection of the unit's intelligence activities and intelligence oversight program.

Section III

Army-Specific Intelligence Policies

1–23. Unique terminology

This regulation uses terms that differ considerably from standard Army usage. The reader must be thoroughly familiar with the glossary to understand this regulation. Many of the terms and corresponding definitions listed in the glossary are defined in DoDM 5240.01, EOs, intelligence community directives, or law. If any provision in this regulation conflicts with a term defined in DoD policy, DoD policy takes precedence.

1–24. Intelligence oversight officer selection and use requirements

Intelligence oversight is an inherently governmental function, which precludes contractors from serving as an IOO. Commanders will document the appointment of all IOOs using appointment orders or other appropriate policy or operational instruments. An IOO must be an intelligence professional knowledgeable of all the issuances associated with the conduct of intelligence activities. An IOO must be commensurate in rank to the level of responsibility within the organization conducting intelligence activities. An IOO must hold the appropriate security clearance and accesses and have complete access to all information on their respective command's intelligence activities and support mechanisms. While a command need not have an IOO assigned at lower subordinate levels, all command personnel must have unfettered access to the IOO. A command IOO is a distinct duty, separate from any intelligence discipline specific requirements, such as the DIRNSA/CHCSS requirement for a commander of an approved SIGINT mission

designating in writing an IOO for SIGINT operations, although commanders may appoint one person to fill both roles.

Chapter 2
U.S. Army Implementation of Procedures Governing the Conduct of Department of Defense Intelligence Activities

2–1. Introduction
DoDM 5240.01 and DoD 5240.1–R establish Attorney General-approved procedures to enable DoD conduct of authorized intelligence activities in a manner that protects the privacy and civil liberties of U.S. persons. These procedures authorize Defense intelligence components to collect, retain, and disseminate information concerning U.S. persons in compliance with applicable laws, EOs, DoD policies, and regulations. Army intelligence elements and each MI employee must abide by these procedures at all times during the conduct of intelligence activities.

2–2. Requirement for intelligence mission and authorities
a. Army intelligence elements or anyone subject to this regulation engaging in an intelligence activity must have documented mission and authorities to conduct such activities. Any intelligence activity conducted without properly documented mission and authorities must be reported and investigated as a possible QIA.

b. For Army intelligence activities under SECARMY authority and for purposes of DoDM 5240.01, Procedure 2, the mission of Army MI is to serve the defense and defense-related intelligence needs of the DA to conduct prompt and sustained combat incident to operations on land. The mission of Army MI also includes intelligence activities to support national requirements, as appropriate; questions of appropriateness will be referred to the servicing legal office.

2–3. Army implementation of specific procedures governing the conduct of Department of Defense intelligence activities
a. Army intelligence elements or anyone operating under SECARMY authority will conduct intelligence activities consistent with the procedures as stated in DoDM 5240.01 and DoD 5240.1–R.

b. In accordance with DoDM 5240.01, the DCS, G–2 and Commander, INSCOM are the only Defense Intelligence Component heads within the DA.

c. DoDM 5240.01 and DoD 5240.1–R require Defense Intelligence Component head (or delegee) approval prior to conducting specific activities. Table 2–1 lists these specific intelligence activities and identifies Army approving officials and delegation authority for each activity. Army intelligence elements must receive the approval of an Army Defense Intelligence Component head (or delegee) prior to conducting any of these specific activities as addressed in DoDM 5240.01 or DoD 5240.1–R.

2–4. Procedures for special circumstances collection
This paragraph provides guidance to Army personnel for evaluating whether a collection opportunity conducted under SECARMY authorities should be considered a special circumstance collection under DoDM 5240.01 and to prescribe procedures for gaining authorization to conduct a special circumstance collection.

a. Special circumstances collection procedures.

(1) *Special circumstances collection criteria.* Special circumstances collection is not defined in DoDM 5240.01. However, the criteria for what satisfies special circumstances collection is defined, and it requires judgments about the volume, proportion, and sensitivity of the USPI likely to be acquired, and the intrusiveness of the methods used to collect the information. Decision makers must evaluate volume, proportion, sensitivity, and intrusiveness in the totality of the circumstances and not as individual factors. A very small volume of extremely sensitive information or a very high volume of low-sensitivity information can create a special circumstance.

(2) *Special circumstances collection criteria.* The Army intelligence element that proposes to collect USPI in a manner that may be considered a special circumstances collection will assess whether the collection of the USPI is a special circumstances collection based on the volume, proportion, and sensitivity of the USPI likely to be acquired and the intrusiveness of the methods used to collect the information.

(3) *Authorization process.* The collecting Army intelligence element will forward a request to conduct a special circumstances collection to the DCS, G–2 or the Commander, INSCOM for review and approval. The DCS, G–2 or the Commander, INSCOM will consult with their supporting legal office and privacy and civil liberties officials and consider the request in light of the following criteria: Does the collection fall within one of the categories of intentional collection of USPI as defined in DoDM 5240.01? Is the collection reasonably based on all the circumstances as set forth in DoDM 5240.01?

(4) *Enhanced safeguards.* If it is determined that due to the volume, proportion, sensitivity, and method of collection that a special circumstance collection exists, the DCS, G–2 or the Commander, INSCOM, in consultation with their supporting legal office and privacy and civil liberties officials, will also consider whether enhanced safeguards to protect access to the information are required using the criteria in DoDM 5240.01.

(5) *Safeguard implementation.* If enhanced safeguards are determined to be necessary based on the factors set forth in *paragraph 2–4b* of this regulation, the DCS, G–2 or the Commander, INSCOM in consultation with their supporting legal office and privacy and civil liberties officials will consider and identify for implementation any of the measures from DoDM 5240.01. that they deem appropriate.

b. Request routing process.

(1) The collecting Army intelligence element will route a written summary of the results of its assessment required in paragraph 2–4b(1) of this regulation in a staff package to the DCS, G–2 or the Commander, INSCOM. A copy of the staffing package, to include a memorandum for the authorization of the special circumstances collection, also will be provided to the Army SIOO.

(2) If special circumstances collection commenced prior to completing the decisional procedures identified in paragraph 2–4c(1), as soon as possible after the collection, the collecting Army intelligence element will prepare a staff package to the DCS, G–2 or the Commander, INSCOM , to include a memorandum for the authorization of the continued retention of the collected information, and, if desired, for the authorization for permanent retention in accordance with the retention standards listed in DoDM 5240.01. The staffing package will include a written summary of the results of its assessment required in paragraphs 2–4b(1) and 2–4b(2) of the reasons or its collection prior to authorization and the determinations on the need for enhanced protections. The staffing package, to include a memorandum for the authorization of the special circumstances collection, also will be forwarded to the Army SIOO.

c. Post-decisional procedures.

(1) The DCS, G–2 or the Commander, INSCOM will immediately provide the Army SIOO, through the AIOPM, a copy of the signed memorandum for the authorization of the special circumstances collection.

(2) If the signed memorandum represents an approval for special circumstances collection (or, in the cases of para 2–4c(2), the retention of special circumstances collection), the Army SIOO, in accordance with DoDM 5240.01, will notify the DoD SIOO.

Table 2–1
Army intelligence oversight approval authorities—Cont

Procedure number	Item number	Approving officials	Authority to delegate	Reference
1. General provisions	Approve emergency exception to policy	DCS, G–2	Not authorized	DoDM 5240.01, para 3.1d(2)
		CG, INSCOM		
2. Collection of USPI	Approve USPI collection: threats to safety	DCS, G–2	Yes (note 1)	DoDM 5240.01, para 3.2c(5)(b)
		CG, INSCOM		
	Approve USPI special circumstances collection	DCS, G–2	Yes, single delegee only (notes 1 and 2)	DoDM 5240.01, para 3.2e
		CG, INSCOM		
	Approve collecting foreign intelligence concerning U.S. persons within the United States	DCS, G–2	Yes, single delegee only (notes 1 and 2)	DoDM 5240.01, para 3.2.g(3)(c)
		CG, INSCOM		

Table 2–1
Army intelligence oversight approval authorities—Continued

Procedure number	Item number	Approving officials	Authority to delegate	Reference
3. Retention of USPI	Approve extended retention of collected USPI (intentional/incidental/voluntarily-provided)	DCS, G–2	Yes, single delegee only (note 1)	DoDM 5240.01, para 3.3c(5)(a)
		CG, INSCOM		
	Determine the need for enhanced retention safeguards to protect USPI	DCS, G–2	Yes (note 1)	DoDM 5240.01, para 3.3.g(1)
		CG, INSCOM		
	Implementation of enhanced retention safeguards to protect USPI	DCS, G–2	Yes (note 1)	DoDM 5240.01, para 3.3.g(2)
		CG, INSCOM		
4. Dissemination of USPI	Determine dissemination of USPI to foreign governments or international organizations	DCS, G–2	Yes (note 1)	DoDM 5240.01, para 3.4c(6)(c)
		CG, INSCOM		
	Determine dissemination of USPI to an entity for the limited purpose of assisting the defense component	DCS, G–2	Yes (note 1)	DoDM 5240.01, para 3.4c(7)
		CG, INSCOM		
	Assess risk of USPI dissemination for protective purposes	DCS, G–2	Yes (note 1)	DoDM 5240.01, para 3.4c(8)
		CG, INSCOM		
	Approve dissemination of large amounts of unevaluated USPI	DCS, G–2	Yes, single delegee only (note 1)	DoDM 5240.01, para 3.4d
		CG, INSCOM		
	Approve dissemination of USPI not for foreign intelligence, counterintelligence, security, law enforcement, cybersecurity, humanitarian assistance, disaster relief, threats to safety, or protective purpose	DCS, G–2	Yes (note 1)	DoDM 5240.01, para 3.4f
		CG, INSCOM		
5. Electronic surveillance	Notify officials intent to conduct electronic surveillance in emergency situations (requires U.S. Attorney General approval through DoD General Counsel)	DCS, G–2	Yes, single delegee only (note 1)	DoDM 5240.01, para 3.5.g(1)
		CG, INSCOM		
	Authorize continued electronic surveillance (up to 72 hours) of a foreign person outside U.S. who then enters the U.S. (emergency situations)	DCS, G–2	Not authorized	DoDM 5240.01, para 3.5.g(2)
		CG, INSCOM		

Table 2–1
Army intelligence oversight approval authorities—Continued

Procedure number	Item number	Approving officials	Authority to delegate	Reference
6. Concealed monitoring	Approve concealed monitoring inside the U.S. or directed at U.S. persons outside the U.S.	DCS, G–2	Yes (note 1)	DoDM 5240.01, para 3.6c(3)
		CG, INSCOM		
7. Physical searches	Request emergency physical searches directed against active duty military personnel under Foreign Intelligence Surveillance Act	DCS, G–2 (request through OGC for Attorney General approval)	Yes (note 1)	DoDM 5240.01, para 3.7c(3)
		CG, INSCOM (request through OGC for Attorney General approval)		
	Request emergency physical searches of persons other than active duty military personnel or their property inside the United States under Foreign Intelligence Surveillance Act	DCS, G–2 (request through OGC for Attorney General approval and Federal Bureau of Investigation (FBI) execution)	Not authorized	DoDM 5240.01, para 3.7d(3)
		CG, INSCOM (request through OGC for Attorney General approval and FBI execution)		
	Request emergency physical searches of persons other than active duty military personnel or their property outside the United States under Foreign Intelligence Surveillance Act	DCS, G–2 (request through OGC for Attorney General approval and coordinate with the Central Intelligence Agency (CIA))	Not authorized	DoDM 5240.01, para 3.7e(3)
		CG, INSCOM (request through OGC for Attorney General approval and coordinate with CIA)		
8. Searches of mail and the use of mail covers	Request emergency physical searches of mail directed against active duty military personnel under Foreign Intelligence Surveillance Act (note 3)	DCS, G–2 (request through OGC for Attorney General approval)	Not authorized	DoDM 5240.01, paras 3.8c(1) and 3.8c(2); DoDM 5240.01, para 3.7c(3)

Table 2–1
Army intelligence oversight approval authorities—Continued

Procedure number	Item number	Approving officials	Authority to delegate	Reference
		CG, INSCOM (request through OGC for Attorney General approval)		
	Request emergency physical searches of mail of persons other than active duty military personnel or their property inside the United States under Foreign Intelligence Surveillance Act (note 3)	DCS, G–2 (request through OGC for Attorney General approval and FBI execution)	Not authorized	DoDM 5240.01, para 3.8c(1); DoDM 5240.01, para 3.7d(3)
		CG, INSCOM (request through OGC for Attorney General approval and FBI execution)		
	Request emergency physical searches of mail of persons other than active duty military personnel or their property outside the United States under Foreign Intelligence Surveillance Act (note 3)	DCS, G–2 (request through OGC for Attorney General approval and coordinate with CIA)	Not authorized	DoDM 5240.01, para 3.8c(2); DoDM 5240.01, para 3.7e(3)
		CG, INSCOM (request through OGC for Attorney General approval and coordinate with CIA)		
	Request mail cover for mail in United States Postal Service channels in accordance with Section 233.3(e)(2), Title 39, Code of Federal Regulations	DCS, G–2 (request only)	Not authorized	DoDM 5240.01, para 3.8d(1)
		CG, INSCOM (request only)		
	Request a mail cover for mail that is to or from a U.S. person in foreign postal channels consistent with appropriate law and procedure of the foreign government and the provisions of any applicable status of forces agreement	DCS, G–2 (request only)	Not authorized	DoDM 5240.01, para 3.8d(2)
		CG, INSCOM (request only)		
9. Physical surveillance	Approve nonconsensual physical surveillance in the U.S.	DCS, G–2 (must coordinate with FBI except when surveillance of	Yes (note 1)	DoDM 5240.01, paras 3.9c(1)(c) through 3.9c(1)(d)

Table 2–1
Army intelligence oversight approval authorities—Continued

Procedure number	Item number	Approving officials	Authority to delegate	Reference
		active-duty military person on military installation)		
		CG, INSCOM (must coordinate with FBI except when surveillance of active-duty military person on military installation)		
	Approve nonconsensual physical surveillance of a U.S. person outside the U.S.	DCS, G–2 (must coordinate with CIA except when surveillance on a military installation)	Yes (note 1)	DoDM 5240.01, para 3.9c(2)(c)
		CG, INSCOM (must coordinate with CIA except when surveillance on a military installation)		
10. Undisclosed participation in organizations	Approve specific types of undisclosed participation in organizations	DCS, G–2	Yes (note 1)	DoDM 5240.01, para 3.10f(2)
		CG, INSCOM		
	Approve specific types of sensitive undisclosed participation in organizations (that is, collection of specific USPI inside the U.S. for counterintelligence purposes)	DCS, G–2	Yes, single delegee only (note 1)	DoDM 5240.01, para 3.10f(3)
		CG, INSCOM		
11. Contracting for goods and services	Contracts with academic institutions in which DoD intelligence affiliation is revealed	DCS, G–2	Not applicable	DoD 5240.1–R, para C1.2.1
		CG, INSCOM		
	Contracts with commercial organizations, private institutions, and individuals without revealing DoD intelligence affiliation	DCS, G–2 upon written determination (note 4)	Not applicable	DoD 5240.1–R, para C1.2.2
		CG, INSCOM upon written determination (note 4)		

Table 2–1
Army intelligence oversight approval authorities—Continued

Procedure number	Item number	Approving officials	Authority to delegate	Reference
12. Provisions of assistance to law enforcement authorities	Cooperation with civilian law enforcement authorities (note 5)	DCS, G–2	Not applicable	DoD 5240.1–R, para C12.2.1
		CG, INSCOM		
13. Experimentation on human subjects for intelligence purposes	Experimentation on human subjects conducted by or on behalf of a DoD intelligence component (notes 6 and 7)	SECARMY (note 8)	Not applicable	DoD 5240.1–R, para C3.3
		Undersecretary of the Army (note 8)		

Note 1. Delegations are authorized only by the DCS, G–2 or the CG, INSCOM and must be in writing. Units requesting delegations will request them by name, position, grade, or function and must balance the need for timely decision making with the need for experienced judgment. Delegees will be no lower than the grade of O–6/General Government (GG)–15 or equivalent. Units requesting delegations will provide a copy of any approved delegations to the Army SIOO.
Note 2. The CG, INSCOM and all delegees must inform the DCS, G–2, through the chain of command, when approving action under this rule. The DCS, G–2 will notify, through the Army SIOO, the DoD SIOO of all special circumstances collections.
Note 3. All searches of mail in United States Postal Service channels must comply with applicable postal regulations. This applies to mail both in and outside the United States.
Note 4. Requires a written determination by the SECARMY or Undersecretary of the Army that the sponsorship of an Army intelligence component must be concealed to protect the activities of the Army intelligence component concerned.
Note 5. Consistent with the limitations contained in DoDI 3025.21 and DoDD 5200.27 or the policy of the supported agency.
Note 6. Only with the informed consent of the subject, in accordance with guidelines issued by the Department of Health and Human Services, setting out conditions that safeguard the welfare of such subjects.
Note 7. Must be conducted in accordance with AR 70–25.
Note 8. All requests from Army intelligence elements for Procedure 13 approvals must be forwarded to the DCS, G–2 for concurrence and coordination.

Chapter 3
Individual Responsibilities

3–1. General
All Army personnel will conduct intelligence activities in accordance with applicable laws, EOs, Presidential directives, and DoD and Army policies.

3–2. Professional conduct
In carrying out intelligence activities, all personnel acting under SECARMY authority and subject to this regulation—

a. Are authorized to collect, retain, and disseminate USPI and otherwise conduct intelligence activities only in accordance with DoDM 5240.01, DoD 5240.1–R, and this regulation.

b. Must carry out all activities in all circumstances in accordance with the Constitution and laws of the United States.

c. Are prohibited from using their access to intelligence capabilities and databases for purposes other *than* to support an authorized intelligence activity or other official DoD mission.

d. May not investigate U.S. persons or collect or maintain information about them solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States.

e. Will not participate in or request any person or entity to undertake any intelligence activities that are not properly authorized and consistent with EO 12333, DoDM 5240.01, DoD 5240.1–R, or this regulation.

f. Must report any activity or conduct that qualifies as either a QIA, S/HSM, or violation of Army-specific intelligence policy without waiting for substantiation, completion of an investigation, formal adjudication, or final resolution of the issue. Reporting will adhere to the procedures in DoDD 5148.13 and this regulation.

g. Must report Federal crimes in accordance with the 1995 DOJ Memorandum of Understanding for the Reporting of Information Concerning Federal Crimes and this regulation—

(1) Facts or circumstances that reasonably indicate to the employee that an employee of an intelligence agency has committed, is committing, or will commit a violation of Federal criminal law.

(2) Facts or circumstances that reasonably indicate to the employee that a non-employee has committed, is committing, or will commit one or more of the specified crimes listed in paragraph 5–3 of this regulation.

h. Must be familiar with the authorities, restrictions, and procedures established in this regulation, DoDD 5148.13, DoDD 5240.01, DoDM 5240.01, DoD 5240.1–R, and all other applicable intelligence community directives, DoD issuances, and Army policies governing intelligence activities.

3–3. Training

All personnel assigned to an Army intelligence element or other Army organizations conducting, supervising, or providing staff oversight of intelligence activities must—

a. Complete intelligence oversight training specified in *paragraph 1–21g* of this regulation within specified timeframe listed below and annually thereafter.

(1) Within 30 days upon assignment or attachment for Regular Army personnel, Reserve Component personnel ordered to active duty for more than 179 days, full-time National Guard duty, and Active Guard and Reserve.

(2) Within 90 days upon assignment or attachment for ARNG and U.S. Army Reserve personnel not fitting the criteria in para 3–3a(1).

b. Complete intelligence discipline specific training required for the conduct of intelligence activities.

Chapter 4
Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters

4–1. General

This chapter provides Army intelligence elements and employees the procedures for identifying, investigating, reporting, and resolving allegations of QIAs and S/HSMs in accordance with DoDD 5148.13. Leaders at all levels have an obligation to encourage reporting and support compliance with intelligence oversight responsibilities. Whenever in doubt as to whether an activity should be reported under this chapter, the activity must be reported for resolution.

4–2. Identification and initial reporting of a questionable intelligence activity or significant or highly sensitive matter

All Army intelligence employees must identify any QIA or S/HSM to their chain of command or supervision immediately. If it is not practical to report the identification of a QIA or S/HSM to the chain of command or supervision, Army intelligence element employees may report the identification of a QIA or S/HSM through legal counsel or inspector general channels.

4–3. Reporting procedures and timelines

a. This section describes the three reporting chains that apply and depend on the authority for the activity. Refer questions about the proper reporting chain to the AIOPM. These QIA and S/HSM reports will be used in addition to other reporting requirements (for example, a serious incident report (SIR), Army counterintelligence incidents, or security violations).

b. Army operational chain of command QIA and S/HSM reports.

(1) Allegations of a QIA or S/HSM involving Army intelligence elements or employees associated with an intelligence or intelligence-related activity conducted under the authority of the SECARMY are an internal Army operational chain of command reporting responsibility.

(2) Army intelligence elements or employees must provide a written report of an Army QIA occurring as part of an intelligence or intelligence-related activity conducted under the authority of the SECARMY within 5 days of discovery through the Army chain of command to TIG, Army SIOO, and AIOPM.

Note. This regulation defines QIA more broadly than DoDD 5148.13 to include violations of Army policy and other unlawful or unauthorized activities. Any activity meeting the QIA definition in this regulation

must be reported to the DAIG. The Army SIOO, TIG, and AIOPM will review the reports to determine those QIAs that must be forwarded to the DoD SIOO in accordance with DoDD 5148.13.

(3) Army intelligence elements and employees must immediately report S/HSM involving intelligence or intelligence-related activities conducted under the authority of the SECARMY through the chain of command to TIG, Army SIOO, and AIOPM. Such reports may be made by any secure means.

(4) Oral QIA or S/HSM reports will be documented with a written report as soon as possible thereafter. Initial reports will be supplemented as additional information becomes available. Supplemental reports will be identified in such a manner that they can be accurately related to the relevant initial reports.

(5) Army intelligence elements must also provide periodic updates to TIG, Army SIOO, and AIOPM on any open Army operational QIA or S/HSM every 30 days after initial reporting until relieved of this obligation by the AIOPM or Army SIOO.

c. Army administrative chain of command QIA and S/HSM reports.

(1) Allegations of a QIA or S/HSM involving Army intelligence personnel while they are not conducting intelligence or intelligence-related activities (for example, misuse of an intelligence system to collect USPI for personal gain or misuse of badge and credentials to support personal activities) is an internal Army administrative chain of command reporting responsibility.

(2) Army intelligence elements must provide a written report of an Army QIA that is not associated with an intelligence or intelligence-related activity conducted under the authority of the SECARMY within 5 days of discovery through the Army administrative chain of command to TIG, Army SIOO, and AIOPM.

(3) Army intelligence elements must immediately report an Army S/HSM associated with Army intelligence personnel who are not conducting an intelligence or intelligence-related activity through the Army chain of command to TIG, Army SIOO, and AIOPM. Such reports may be made by any secure means.

(4) Oral QIA or S/HSM reports will be documented with a written report as soon as possible thereafter. Initial reports will be supplemented as additional information becomes available. Supplemental reports will be identified in such a manner that they can be accurately related to the relevant initial reports.

(5) Army intelligence elements must also provide periodic updates to TIG, Army SIOO, and AIOPM on an open QIA or S/HSM every 30 days after initial reporting until relieved of this obligation by the AIOPM or Army SIOO.

d. Combatant command or intelligence agency QIA and S/HSM reports. Allegations of a QIA or S/HSM involving Army intelligence elements or employees associated with intelligence or intelligence-related activities conducted under the authority of a combatant commander or intelligence agency must be reported through combatant command or intelligence agency reporting channels. Army ASCCs IOOs will provide courtesy copies of all QIAs and S/HSMs involving Army intelligence personnel to the Chief, INSCOM Intelligence Oversight Office, TIG, Army SIOO, and AIOPM to inform the Army's intelligence train, man, and equip responsibilities.

e. DA personnel responsible for drafting the performance requirements (statement of work) for any contract under which contractor personnel will be conducting intelligence or intelligence-related activities or supporting those efforts under SECARMY authority will ensure the contract requires contractor personnel to report any QIA or S/HSM to appropriate Government officials identified in the contract.

4–4. Reports and investigations of questionable intelligence activities and significant or highly sensitive matters

a. In accordance with DoDD 5148.13, reports will provide the following information:

(1) Incident Description.

(2) Timeline: Indicate when the incident occurred, when it was initially reported within the Army, and when it was reported to the AIOPM; if applicable, explain any delay in reporting.

(3) Reason for Report: For a QIA, identify the specific paragraph of the law or policy violated. For an S/HSM, identify the rationale for reporting as such.

(4) Cause: initial report – To Be Determined; final report - indicate how or why the incident occurred.

(5) Impact on National Security or International Relations: initial report – To Be Determined; final report – assess the impact (low, medium, or high) and concisely explain the supporting analysis.

(6) Impact on Civil Liberties or Privacy: initial report – To Be Determined; final report – assess the impact (low, medium, or high) and concisely explain the supporting analysis.

(7) Remedial Action: initial report – immediate actions taken or To Be Determined; final report – plan for final actions.

(8) Additional Information: Provide any additional information required to fully inform the Secretary of Defense (SECDEF), the Deputy Secretary of Defense, the Intelligence Oversight Board, and the DNI, or provide context about the incident.

(9) Status: Indicate whether the incident is open or closed. If open, provide the status of the ongoing investigation. If closed, include a notation indicating whether any allegations were substantiated or not substantiated.

Note. QIA and S/HSM reports must adhere to any additional guidance and formats provided by TIG.

b. Each report of a QIA or S/HSM will be investigated to the extent necessary to determine the facts and to assess whether the activity is legal and consistent with applicable policies. At a minimum, investigations will provide a written report that addresses each element of *paragraph 4–4a*.

c. Army intelligence elements must expeditiously conduct investigations. Unless referred to a counterintelligence or criminal investigative agency, Army intelligence elements should ordinarily complete investigations of a QIA or S/HSM within 60 days of the initial report, unless extraordinary circumstances dictate a longer period.

d. Army intelligence elements must conduct investigations in accordance with AR 15–6.

4–5. Quarterly reporting requirements

TIG will submit a quarterly report to the DoD SIOO describing all QIAs, S/HSMs, and crimes required by EO 12333 to be reported to the U.S. Attorney General that were identified during the quarter and previously reported incidents that have not been resolved. These reports must conform to the standards within DoDD 5148.13. TIG will coordinate quarterly reports with the Army SIOO and AIOPM prior to releasing the report to the DoD SIOO. TIG will provide the Army SIOO, AIOPM, the DCS, G–2 and the CG, INSCOM with a copy of the DoD SIOO-approved quarterly reports.

a. To assist TIG in preparing this report, the AIOPM, and the Commanders of ACOMs, ASCCs, INSCOM, and 650th MI Group will provide contributions within 5 days following the end of the quarter. These contributions will be forwarded to TIG for inclusion in the quarterly report to the DoD SIOO.

b. All reports made pursuant to paragraph 4–3 that involve a possible violation of Federal criminal law will be reviewed by the Army General Counsel in accordance with chapter 5 of this regulation.

Chapter 5
Reporting Federal Crimes

5–1. General

This chapter implements the 1995 Memorandum of Understanding: Reporting of Information Concerning Federal Crimes between the Intelligence Community and DOJ for reporting of information concerning Federal crimes. All Army intelligence element employees must report information concerning possible Federal crimes by employees of an Army intelligence element or violations of specified Federal criminal laws by any other person, which information was collected by it during the performance of its designated intelligence activities, as those activities are defined in EO 12333. This report is in addition to existing investigative, judicial, or command authority and reporting requirements.

5–2. Reporting requirements

a. Reporting channel. Reports of information concerning possible Federal crimes involving employees of an Army intelligence element will be forwarded through command channels to the DCS, G–2; the PMG; and the Director, U. S. Army Criminal Investigation Division.

b. Timeline. Reports will reach the DCS, G–2 not later than 3 working days following the discovery or receipt of information regarding the Federal crime.

c. Contents. The following will be included in the report:

(1) The fullest possible identification of the person committing the alleged Federal crime, including the name, rank or civilian grade, social security or DoD identification number, military or civilian occupational specialty code, security clearance and present access, unit of assignment and unit of employment, attachment or detail, and duties at the time of the activity.

(2) When and where the crime occurred.

(3) A description of the Federal crime that may have been violated.

(4) Identity of the law enforcement or counterintelligence agency receiving the report and investigating the incident.

(5) If the report originated outside of the affected command, whether or not the command submitted its own report per this chapter or under the provisions of AR 190–45.

d. Reports flow. The DCS, G–2 will transmit reports received under this chapter simultaneously to OTJAG and OGC. The OGC senior national security legal advisor will review and transmit reports received under this chapter pursuant to procedures adopted by the DOJ.

e. Unknown suspect. When the identity of the suspect is unknown, as much detail as possible will be provided about the alleged crime. Clearly state that the suspect has not yet been identified and which agency is investigating. "John Doe" or other false names will not be used to refer to unknown suspects. An additional report will be submitted when the suspect is identified.

f. Restricted cases. Restricted cases, defined in AR 381–20 and formerly referred to as "bigoted" cases, are normally only reported by the Army Counterintelligence Coordinating Authority. If the FBI has an open investigation and is temporarily withholding the suspect's identity (known as a restricted case), the suspect will be identified as "John Doe 1," "John Doe 2," and so on. In cases where the FBI has an open case and will report to the DOJ, an Army report will be rendered regarding the crimes listed in paragraph 5–3, whether or not it is a restricted case.

g. Serious incident reports. If a crime is reportable under the provisions of AR 190–45, an additional report under this chapter is not required. The DCS, G–2; TJAG; and the General Counsel will be included as SIR addressees. Ensure that the report meets AR 190–45 timelines.

h. Additional reports. Units will report federal crimes that are also QIAs or S/HSMs with an explanation of why the activity meets both criteria. If the unit initially reported per AR 190–45, the SIR date time group will be provided or a copy attached.

5–3. Reportable Federal crimes

Army intelligence element employees must report facts or circumstances that reasonably indicate that an employee of an intelligence agency has committed, is committing, or will commit a violation of Federal criminal law. Additionally, Army intelligence element employees must report allegations concerning criminal activities by non-employees if they pertain to one or more of the following specified violations of Federal criminal law:

a. Crimes involving intentional infliction of threat of death or serious physical harm. These include, but are not limited to homicide, kidnapping, hostage taking, assault (including sexual assault), or threats or attempts to commit such offenses, against any person in the United States or a U.S. national or internationally protected person (as defined in 18 USC 1116(b)(4)), whether in the United States or abroad.

b. Crimes, including acts of terrorism, that are likely to affect the national security, defense, or foreign relations of the United States, whether in the United States or abroad. These may include, but are not limited to—

(1) Espionage.

(2) Sabotage.

(3) Unauthorized disclosure of classified information.

(4) Seditious conspiracies to overthrow the Government of the United States.

(5) Fund transfers violating the International Emergency Economic Powers Act.

(6) Providing material or financial support to terrorists.

(7) Unauthorized traffic in controlled munitions or technology.

(8) Unauthorized traffic in, use of, or contamination by nuclear materials, chemical or biological weapons, or chemical or biological agents.

(9) Fraudulent entry of persons into the United States, the violation of immigration restrictions, or the failure to register as a foreign agent or an intelligence trained agent.

(10) Offenses involving interference with foreign governments or interference with the foreign policy of the United States whether occurring in the United States or abroad.

(11) Acts of terrorism anywhere in the world that target the U.S. Government or its property, U.S. persons, or any property in the United States; or in which the perpetrator is a U.S. person.

(12) Aircraft hijacking, attacks on aircraft or international aviation facilities, or maritime piracy.

(13) The unauthorized transportation or use of firearms or explosives in interstate or foreign commerce.

c. Crimes involving foreign interference with the integrity of U.S. governmental institutions or processes. Such crimes may include—

(1) Activities to defraud the U.S. Government or any federally protected financial institution, whether occurring in the United States or abroad.

(2) Obstruction of justice or bribery of U.S. officials or witnesses in U.S. proceedings, whether occurring in the United States or abroad.

(3) Interference with U.S. election proceedings or illegal contributions by foreign persons to U.S. candidates or election committees.

(4) Perjury in connection with U.S. proceedings or false statements made in connection with formal reports or applications to the U.S. Government, or in connection with a formal criminal or administrative investigation, whether committed in the United States or abroad.

(5) Counterfeiting U.S. obligations or any other governmental currency, security, or identification documents used in the United States, whether committed in the United States or abroad; and transactions involving stolen governmental securities or identification documents or stolen or counterfeit non-governmental securities.

d. Crimes related to unauthorized electronic surveillance in the United States or to tampering with or unauthorized access to computer systems.

e. Violations of U.S. drug laws including the cultivation, production, transportation, importation, sale, or possession (other than possession of user quantities) of controlled substances; and the production, transportation, importation, and sale of precursor or essential chemicals.

f. The transmittal, investment, or laundering of the proceeds of any of the unlawful activities listed in this paragraph, whether committed in the United States or abroad.

g. Any conspiracy or attempt to commit a crime reportable under this paragraph must be reported if the conspiracy or attempt itself meets the applicable reporting criteria.

h. Information about the commission of other serious felony offenses by non-employees (for example, violations of U.S. environmental laws relating to ocean and inland water discharging or dumping, drinking water contamination, or hazardous waste disposal, and crimes involving interference with the integrity of U.S. governmental institutions or processes that would not otherwise be reportable under paragraph *5–3a* or *5–3b* when acquired by an Army intelligence element's otherwise routine collection of information while conducting an intelligence activity).

5–4. Non-reportable Federal crimes

The following are examples of crimes that do not meet the intent of this chapter:

a. Reportable information collected and disseminated to Army intelligence elements by another agency, unless Army intelligence was the sole recipient.

b. Crimes committed by non-Army intelligence employees who are under investigation by a criminal investigative organization.

c. Crimes against property totaling $500 U.S. dollars or less for intelligence employees or $1,000 U.S. dollars or less for other personnel.

d. Other than homicide or espionage, crimes that were committed more than 10 years before the Army intelligence element became aware of them.

Chapter 6
Requests for Identities of U.S. Persons in Disseminated Intelligence and Counterintelligence Reports

6–1. General

a. This chapter implements Intelligence Community Policy Guidance (ICPG) 107.1 and prescribes policies, procedures, and responsibilities for responding to a requesting entity, other than Army intelligence elements, for post-publication release and dissemination of masked U.S. person identity information contained in disseminated intelligence or counterintelligence reports. These requirements were developed in consultation with the DNI, the U.S. Attorney General, and the SECDEF.

b. This chapter applies to all Army personnel performing intelligence activities under the authority of the SECARMY. This chapter applies exclusively to requests from a requesting entity, other than Army intelligence elements, for post-publication release and dissemination of nonpublic U.S. person identity

information that was masked in a disseminated Army intelligence or counterintelligence report. These requirements do not apply in circumstances where a U.S. person has consented to the dissemination of information or of communications to, from, or about the U.S. person. These requirements do not affect any minimization procedures established pursuant to the Foreign Intelligence Surveillance Act of 1978, 50 USC 1801, EO 12333, or other provisions of law. These requirements do not affect the requirements established in Intelligence Community Directive 112.

6–2. Definitions

The following definitions are specific to this chapter:

a. Requesting entity is an entity of the U.S. Government or a state, local, tribal, or territorial government that makes a covered request.

b. Masked is an enhanced safeguard for U.S. person identity information that uses alternative or generic wording to render the U.S. person identity information so that the reader may not ascertain the identity of that U.S. person.

c. U.S. person is as defined in EO 12333 or the Foreign Intelligence Surveillance Act of 1978, as appropriate.

d. Identity information is information that identifies U.S. persons by name or by individually identifying titles or characteristics.

e. Exigent circumstances are circumstances when there is a reasonable basis to believe that there is imminent danger to a person's life or physical safety or when there are time-critical needs that pose significant risks to important U. S. interests.

6–3. Roles and responsibilities

a. The DCS, G–2 will—

(1) Ensure that documentation for requests that are covered by this policy includes information required by paragraphs *6–4a*, 6–4f(1), 6–4f(2), and 6–4f(3) and that such documentation is retained for not less than 5 years, as required by *paragraph 6–4c*.

(2) Consider for approval and approve as appropriate, or further delegate such authority to consider and approve as appropriate, requests that are covered by this policy that meet the requirements as specified in *paragraph 6–4b*.

(3) Ensure that approval of requests that are covered by this policy are subject to General Counsel concurrence, as specified in paragraph 6–4e(4).

(4) Notify the congressional intelligence committees of approval of requests that are covered by this policy, as specified in paragraph 6–4e(5).

(5) Annually submit a report to the DNI, the congressional intelligence committees, and, through the DoD SIOO to the SECDEF, as specified in *paragraph 6–4f*.

(6) Ensure that requesting entities, when submitting requests that are covered by this policy, provide the information necessary for documentation as required by paragraphs *6–4a*, 6–4e(1), and 6–4e(3).

(7) Create and retain records as required by *paragraph 6–4c* and AR 25–400–2.

(8) Compile and provide to the information necessary to fulfill the reporting requirement to the DNI, the congressional intelligence committees, and the SECDEF, as specified in *paragraph 6–4f*.

b. The General Counsel, or in the absence of the General Counsel, the Principal Deputy General Counsel, will consider for concurrence, and as appropriate concur on, requests that are covered by this policy as specified in paragraph 6–4e(4).

c. The Chief of Legislative Liaison will transmit and ensure receipt by the congressional intelligence committees of Army intelligence notifications relating to the approval of requests covered by this policy, as specified in paragraph 6–4e(5), and information necessary to fulfill the reporting requirement, as specified in *paragraph 6–4f*.

d. The DCS, G–2, in coordination with the Army Civil Liberties, Privacy, and Transparency official, will work with the DNI to review the reporting numbers in *paragraph 6–4f* and, consistent with the intelligence community's Principles of Intelligence Transparency and, where appropriate, the requirements of EO 13526 to ensure the protection of national security information, will report the total numbers submitted annually for inclusion in the Office of the Director of National Intelligence Annual Statistical Transparency Report.

6–4. Procedures

a. With respect to requests covered by this chapter, the approval authority will document, in writing, at the time of the request the following information—

(1) The name or title of the individual who is making the request in an official capacity on behalf of the requesting entity.

(2) Information that identifies the report serial numbers or for unserialized products and reports the document date, title, and originating Army organization that contains the requested U.S. person identity information.

(3) The name or title of each individual who will receive the U.S. person identity information at the time of release.

(4) A fact-based justification describing why such U.S. person identity information is required by each individual identified in paragraph 6–4a(3) to carry out the duties of the individual.

b. Requests covered by this policy will be approved only by the DCS, G–2 or a designee to whom the DCS, G–2 has delegated such authority in writing. The approving official will coordinate with the legal office advising them prior to releasing any requested U.S. person identity information. When an intelligence community element, other than Army intelligence, originated information in an Army intelligence report that is subject to a request that is covered by this policy, the Army intelligence element receiving the request will promptly refer the request to the intelligence community element that masked the U.S. person identity information and inform the requestor of the referral.

c. The DCS, G–2, or a designee to whom the DCS, G–2 has delegated authority to approve the requests, will retain all records with respect to any request covered by this policy, including the disposition of such requests, as required by AR 25–400–2, as permanent records. Active records will be retained for not less than 5 years prior to being moved to archival status. Such records include, with respect to approved and denied requests, the name or title of the individual who approved or denied such requests.

d. In the event of exigent circumstances or where a delay could negatively impact intelligence activities, an immediate disclosure by the approving authority described in *paragraph 6–4b* to a requesting entity of U.S. person identity information may be approved based on the rationale provided by the requesting entity. The rationale may be provided orally or in writing. Within 5 business days after such a disclosure, the requesting entity will provide the basis for making the request, in accordance with *paragraph 6–4a*.

e. With respect to any request that is covered by this policy that is made during a period beginning on the date of a general election for President of the United States of America and ending on the date on which such President is inaugurated—

(1) The SECARMY will require the individual of a requesting entity who is making the request to assert in writing whether or not they have knowledge or belief that any U.S. person identity information sought by the request is of an individual who is a member of the transition team as identified by the President-elect or Vice President-elect.

(2) The approving authority, described in *paragraph 6–4b*, will assert in writing whether or not, based on the face of the reports to which the request pertains, they have knowledge or reasonable belief that any U.S. person identity information sought by the request is of an individual who is a member of the transition team, as identified by the President-elect or Vice President-elect.

(3) The documentation required under *paragraph 6–4a* will include such assertions made pursuant to paragraphs 6–4e(1) and 6–4e(2).

(4) If a requesting entity has asserted that it has knowledge or belief pursuant to paragraph 6–4e(1) or the approving authority as described in *paragraph 6–4b* has asserted that they have knowledge or reasonable belief pursuant to paragraph 6–4e(2), the approval made pursuant to *paragraph 6–4a* will be subject to the concurrence of the Army General Counsel (or in the absence of the General Counsel, the Principal Deputy Army General Counsel) that the dissemination of such U.S. person identity information is in accordance with the procedures under *paragraph 6–4a*.

(5) Consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters, the DCS, G–2, in consultation with the DNI, will notify the chairpersons and ranking minority members of the congressional intelligence committees of any approval described in *paragraph 6–4e* not later than 14 days after the date of such approval.

f. Not later than 1 March of each year, beginning in 2020, the DCS, G–2 will submit to the DNI, the congressional intelligence committees, and, through the DoD SIOO to the SECDEF, a report documenting the following information with respect to the preceding calendar year:

(1) The total number of requests covered by this policy that Army intelligence received.

(2) Of the total, the number of requests approved.

(3) Of the total, the number of requests denied.

(4) For each number calculated under paragraphs 6–4f(1) through 6–4f(3), the sum total by each requesting entity.

6–5. Request routing process

a. Unless delegated otherwise by the DCS, G–2, Army intelligence elements responding to a requesting entity's request for the post-publication release and dissemination of masked U.S. person identity information contained in disseminated Army intelligence or counterintelligence reports must forward all such requests to their respective ACOM, ASCC, or DRU IOO for processing.

b. The ACOM, ASCC, and DRU IOOs will submit all requests to the DCS, G–2 or delegee for coordination and approval.

c. Once a request is approved or disapproved, the DCS, G–2 or delegee will forward a copy of the response to the respective ACOM, ASCC, or DRU IOO. It is the responsibility of the SIO of the ACOM, ASCC, or DRU to disseminate USPI resulting from an approved request to the requesting entity.

d. All actions taken under this chapter must expeditiously be forwarded to the DCS, G–2 AIOPM for retention as permanent records.

Appendix A

References

Section I

Required Publications

Unless otherwise indicated, all Army publications are available on the Army Publishing Directorate website at https://armypubs.army.mil. DoD publications are available on the ESD website at https://www.esd.whs.mil. EOs are available at https://www.archives.gov/. U.S. Code sections are available at https://uscode.house.gov/.

AR 11–2
Managers' Internal Control Program (Cited in the title page.)

AR 15–6
Procedures for Administrative Investigations and Boards of Officers (Cited in *para 4–4d*.)

AR 20–1
Inspector General Activities and Procedures (Cited in *para 1–9a*.)

AR 25–400–2
The Army Records Information Management System (ARIMS) (Cited in para 6–3a(7).)

AR 70–25
Use of Volunteers as Subjects of Research (Cited in table 2–1.)

AR 190–45
Law Enforcement Reporting (Cited in *para 1–14a*.)

AR 381–20
Army Counterintelligence Program (Cited in *para 5–2f*.)

DoD 5240.1–R
Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons (Cited in the title page.)

DoDD 5148.13
Intelligence Oversight (Cited in the title page.)

DoDD 5200.27
Acquisition of Information Concerning Persons and Organizations Not Affiliated With the Department of Defense (Cited in table 2–1.)

DoDD 5240.01
DoD Intelligence Activities (Cited in the title page.)

DoDI 3025.21
Defense Support of Civilian Law Enforcement Agencies (Cited in table 2–1.)

DoDM 5200.02
Procedures for the DoD Personnel Security Program (Cited in terms.)

DoDM 5240.01
Procedures Governing the Conduct of DoD Intelligence Activities (Cited in the title page.)

EO 12333
United States Intelligence Activities (Cited in the title page.)

EO 13355
Strengthened Management of the Intelligence Community (Cited in para B–4a(1).)

ICPG 107.1
Requests for Identities of U.S. Persons in Disseminated Intelligence Reports (Available at https://www.dni.gov/files/documents/icpg/icpg-107.1.pdf.) (Cited in *para 6–1a*.)

Section II

Prescribed Forms

This section contains no entries.

Appendix B

Internal Control Evaluation

B–1. Function

The function of this evaluation is to ensure effective implementation of the Army's intelligence oversight program.

B–2. Purpose

The purpose of this evaluation is to assist commanders and intelligence oversight officials in evaluating the key management controls outlined below, using the process in AR 11–2. It does not cover all controls, but focuses upon those that are essential for ensuring effective implementation of the intelligence oversight program.

B–3. Instructions

Answers must be based upon actual testing of key management controls using the methods specified on DA Form 11–2 (Internal Control Evaluation Certification). Answers must be Yes, No, or Not Applicable, with narrative explaining the answer, if needed. Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These management controls must be evaluated annually. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification). All Army elements subject to the intelligence oversight program will develop and implement an intelligence oversight inspection program. This appendix may serve as a base for inspections, with additional questions as determined by the agency or command performing the inspection. In addition, Internal Control Evaluations may reveal QIAs or S/HSMs which must be separately reported; units are reminded that leaders at all levels have an obligation to support reporting.

B–4. Test questions

a. General—Deputy Chief of Staff, G–2.

(1) Does the DCS, G–2, in coordination with the General Counsel and TJAG, promulgate policy, procedures, and programs necessary for implementing EO 12333, EO 13355, DoDD 5148.13, DoDD 5240.1, DoDM 5240.01 and DoD 5240.1–R?

(2) Does the DCS, G–2 monitor and evaluate the administration of the intelligence oversight program?

(3) Does the DCS, G–2 ensure ACOM, ASCC, and DRUs and other agencies establish and maintain an ongoing self-inspection program, including periodic reviews and assessments of files and databases containing USPI?

b. General—Commanders of U.S. Army organizations that conduct intelligence activities.

(1) Does the commander have the mission to conduct intelligence activities?

(2) Does the commander ensure unit personnel understand the unit's authorized intelligence mission?

(3) Has the organization (down to battalion level or separate operating detachment or activity) designated an IOO of appropriate grade and experience with overall responsibility for assisting the commander with the command's intelligence oversight program?

(4) Are the intelligence officer's duties delineated?

(5) Does the IOO have access to all intelligence and intelligence-related programs, files networks, and information for operations or activities conducted by the organization?

(6) Is there anyone else who has some intelligence oversight responsibility such as the unit staff judge advocate? If so, what are their roles?

(7) Is there a unit intelligence oversight standard operating procedure (typically addressed at brigade level or higher) to ensure centralized processes may be included in unit policy?

(8) Other than appropriate administrative files, as required, do any files (automated, operational, working, and so forth) contain information about U.S. persons? If yes, does the organization have authority to collect, retain, and disseminate such USPI?

(9) Is authorization documentation current?

(10) Is USPI being retained longer than the authorized period in accordance with DoDM 5240.01?

(11) If retained, is access to retained information controlled?

(12) Has an auditing process been implemented to ensure retention of USPI in intelligence databases is maintained in accordance with DoDM 5240.01?

(13) Have reporting procedures been implemented for QIA, S/HSM, Federal crimes, and violations of Army-specific intelligence policies in accordance with this regulation?

c. Training.

(1) Do personnel and leadership receive intelligence oversight training on an annual basis?

(2) Does the IOO maintain records documenting compliance with intelligence oversight training?

(3) Has the commander training tailored to the unit's mission and adequate in content?

(4) Is training effectiveness evaluated?

(5) Are new unit personnel briefed as part of in-processing?

(6) Are measures in effect to ensure personnel detailed outside or on temporary loan to the unit receive intelligence oversight training? Explain the measures and cross check training records.

(7) Has intelligence oversight been incorporated into the unit's organizational inspection program?

(8) Are any personnel in the unit exempted from intelligence oversight training?

(9) What is the basis for the exemption?

(10) Who made the decision?

(11) Based on personnel interviews, are organization personnel aware of what constitutes a U.S. person?

(12) Based on personnel interviews, are organization personnel aware of what constitutes a QIA and S/HSM?

(13) Based on personnel interviews, are organization personnel aware of what obligation they must report QIAs and S/HSM?

(14) Based on personnel interviews, are organization personnel aware of to whom they report QIAs and S/HSM?

(15) Based on personnel interviews, are organization personnel aware of the fact that no retaliatory action can be taken for reporting QIAs and S/HSM?

(16) Based on personnel interviews, are organization personnel aware of where to find applicable directives, regulations, and policies or whom to ask for guidance?

(17) Based on personnel interviews, are organization personnel aware of how the intelligence oversight program is advertised in the organization?

d. Oversight mechanisms.

(1) Does the organization conduct annual internal self-assessments or inspections of the intelligence oversight program?

(2) Are assessments conducted using the procedures in AR 11–2 and this Appendix?

(3) Are intelligence oversight concerns effectively considered in unit operational planning and conduct and do appropriate people participate?

(4) Do approval authorities take appropriate actions to resolve concerns prior to approving plans?

(5) If the unit's mission allows, is the unit conducting intelligence operational activities requiring the use of special collection techniques (Procedures 5 through 10), and do those activities comply with applicable rules?

(6) If the unit provided support to law enforcement agencies since the last intelligence oversight inspection, did the requests receive a legal review and were they approved by the appropriate command authority?

(7) If the unit participates in any intelligence special access programs or other restricted access programs, does the unit have appropriate mechanisms to ensure intelligence oversight training of personnel and reporting QIAs and S/HSMs?

(8) Do the servicing legal office and Inspector General have appropriate access to leadership to provide effective oversight?

(9) Do the servicing legal office and Inspector General have appropriate access to information, including classified information as necessary, to provide effective oversight?

(10) Do the servicing legal office and Inspector General have adequate training or do they know from whom to seek higher headquarters support?

(11) Does the organization have documented internal policies and procedures concerning collection, retention, and dissemination of USPI?

(12) Does the organization have adequate procedures and supporting technical systems to monitor the status of USPI held for temporary evaluation for retention?

(13) If the organization had any external intelligence oversight inspections, were corrective actions taken on findings or observations?

e. Reporting procedures.

(1) Are QIAs and S/HSMs submitted in a timely manner and with the required information?

(2) Are QIAs and S/HSMs appropriately and timely investigated?

(3) Are QIA and S/HSM remedial actions completed?

f. Inspectors General.

(1) Has each inspector general identified all intelligence components subject to intelligence oversight inspection by the command?

(2) Is intelligence oversight included as part of the command's organizational inspection program?

(3) Are there procedures for determining if intelligence and supporting Staff Judge Advocate personnel of organizations understand and comply with the procedures in this regulation?

(4) Are procedures in place for determining if all intelligence personnel are trained in intelligence oversight upon initial assignment and annually thereafter?

(5) Are procedures in place for determining if intelligence files are reviewed periodically?

(6) Are QIAs, S/HSMs, and Federal crimes committed by intelligence personnel reported as required?

(7) Are procedures in place to ensure that follow-up is conducted?

B–5. Supersession

This evaluation replaces the evaluation format for the Army's intelligence oversight program previously published in AR 381–10, dated 3 May 2007.

B–6. Comments

Help make this a better tool for evaluating management controls. Submit any comments to the DCS, G–2 AIOPM (DAMI–CDC), 1000 Army Pentagon, Suite 2D350, Washington, DC 20310–1000.

Glossary of Terms

Army Intelligence element employee
For the purposes of this regulation, a person employed by, assigned or detailed to, or who otherwise conducts intelligence activities on behalf of an Army Intelligence element, except that this term does not include a human source. *Note.* This term is synonymous with “MI employee” and “MI personnel.”

Army Intelligence elements
For the purposes of this regulation, the Regular Army, Army Reserve, and ARNG elements that perform foreign intelligence or counterintelligence missions or functions consisting of—
a. Headquarters, Department of the Army, DCS, G–2.
b. INSCOM and subordinate units.
c. 650th MI Group, Supreme Headquarters Allied Powers Europe.
d. SIOs and staff of ACOMs, ASCCs, DRUs, and other commands and organizations while conducting an intelligence activity under SECARMY authorities, intelligence training, and Army-specific reporting requirements for QIAs and S/HSMs.
e. G–2 and S–2 offices at all levels of organization while conducting an intelligence activity under SECARMY authorities, intelligence training, and Army-specific reporting requirements for QIA and S/HSM.
f. Installation, organization, facility, or program security offices when carrying out intelligence activities.
g. MI units while conducting an intelligence activity under SECARMY authorities, intelligence training, and Army-specific reporting requirements for QIA and S/HSM.
h. ICoE and other organizations conducting intelligence training.
i. Intelligence systems developers when developing or testing systems.
j. Contractors supporting any Army entity when conducting intelligence activities as defined in DoDM 5240.01.
k. Any other Army entity when conducting intelligence activities as defined in DoDM 5240.01 under the authority of the SECARMY.

Collection
Defined in DoDM 5240.01

Concealed monitoring
Defined in DoDM 5240.01.

Consent
Defined in DoDM 5240.01.

Contract
For purposes of this regulation, includes all contracts, other transaction agreements, cooperative research and development agreements, grants, and similar arrangements under which non-federal personnel (other than human sources) conduct Army intelligence or intelligence-related activities.

Counterintelligence
Defined in DoDM 5240.01.

Derogatory information
Information that reflects on the integrity or character of an individual, or circumstances that suggests that their ability to safeguard national security information may be impaired, that their access to classified or sensitive information clearly may not be in the best interest of national security, or that their activity may be in conflict with the personnel security standards or adjudicative guidelines. (See DoDM 5200.02)

Detail
Defined in DoDM 5240.01.

Dissemination
Defined in DoDM 5240.01.

Electronic surveillance
Defined in DoDM 5240.01.

Force protection
Preventive measures taken to mitigate hostile actions against MI personnel (to include Family members), resources, facilities, and critical information (see JP 3–0).

Foreign intelligence
Defined in DoDM 5240.01.

Foreign power
Defined in DoDM 5240.01.

Imagery
Defined in DoDM 5240.01.

Intelligence
Defined in DoDM 5240.01.

Intelligence activities
Defined in DoDM 5240.01.

Intelligence Community
Defined in DoDM 5240.01.

International terrorism or international terrorist activities
Defined in DoDM 5240.01.

Mail cover
Defined in DoDM 5240.01.

Multinational intelligence activities
For the purposes of this regulation, Intelligence activities conducted by deployed multinational units or task forces, such as North Atlantic Treaty Organization Allied MI activities.

Organization
Defined in DoDM 5240.01.

Organization in the United States
Defined in DoDM 5240.01.

Organization outside the United States that constitutes a U.S. person
Defined in DoDM 5240.01.

Overhead reconnaissance
Defined in DoDM 5240.01.

Participation
Defined in DoDM 5240.01.

Permanent resident alien
Any person not a citizen of the United States who is living in the U.S. under legally recognized and lawfully recorded permanent residence as an immigrant. Also known as, “legal permanent resident,” “resident alien permit holder,” and “Green Card holder.” (See U.S. Citizenship and Immigration Services Glossary.)

Physical search
Defined in DoDM 5240.01.

Physical surveillance
Defined in DoDM 5240.01.

Publicly available information
Defined in DoDM 5240.01.

Questionable intelligence activity
Any intelligence or intelligence-related activity when there is reason to believe such activity may be unlawful or contrary to an EO, Presidential directive, Intelligence Community Directive, or applicable DoD or Army policy governing that activity. For the purposes of this regulation, a questionable intelligence activity also includes any unauthorized access or use of information that has been collected for an intelligence

purpose, or any unlawful or unauthorized use of a resource or capability researched and developed to support the conduct of intelligence or intelligence-related activity (see DoDD 5148.13 as modified herein).

Reasonable belief
Defined in DoDM 5240.01.

Reasonable expectation of privacy
Defined in DoDM 5240.01.

Retention
Defined in DoDM 5240.01.

Significant or highly sensitive matter
An intelligence or intelligence-related activity (regardless of whether the intelligence or intelligence-related activity is unlawful or contrary to an EO, Presidential directive, Intelligence Community Directive, or DoD policy), or serious criminal activity by intelligence personnel, that could impugn the reputation or integrity of the Intelligence Community, or otherwise call into question the propriety of intelligence activities. Such matters might involve actual or potential—
a. Congressional inquiries or investigations.
b. Adverse media coverage.
c. Impact on foreign relations or foreign partners.
d. Systemic compromise, loss, or unauthorized disclosure of protected information (see DoDD 5148.13).

Special collection techniques
For the purposes of this regulation, the collective term refers to the use of electronic surveillance, concealed monitoring, physical searches, searches of mail and the use of mail covers, physical surveillance, or undisclosed participation in an organization in support of an intelligence activity.

U.S. person
Defined in DoDM 5240.01.

U.S. Person Information
Defined in DoDM 5240.01.

Undisclosed participation
Defined in DoDM 5240.01.

United States
Defined in DoDM 5240.01.

SUMMARY of CHANGE

AR 381–10
The Conduct and Oversight of U.S. Army Intelligence Activities

This major revision, dated 27 January 2023—

- Changes title from “U.S. Army Intelligence Activities” to “The Conduct and Oversight of U.S. Army Intelligence Activities” (title page).

- Specifies the Office of the General Counsel senior national security legal advisor as the Army’s senior intelligence oversight official (para 1–7).

- Creates the Army intelligence oversight program manager under Deputy Chief of Staff, G–2 (para 1–12).

- Defines responsibilities for intelligence oversight officers (para 1–22).

- Specifies Army policy for collecting, retaining, and disseminating Special Circumstances Collection containing U.S. person information (para 2–4).

- Incorporates implementation of Intelligence Community Policy Guidance 107.1 (chap 6).

- Incorporates the DoDM 5240.01 and DoD 5240.1–R (throughout).

- Incorporates DoDD 5148.13 intelligence oversight requirements and reporting requirements for a questionable intelligence activity and significant or highly sensitive matter (throughout).