



## DEFENSE INFORMATION SYSTEMS AGENCY

P. O. Box 4502  
ARLINGTON, VIRGINIA 22204-4502

DISA INSTRUCTION 100-45-1

17 March 2006

*Last Certified: 11 April 2008*

### ORGANIZATION

Inspector General of the Defense Information Systems Agency

1. **Purpose.** This Instruction establishes the mission of the Office of the Inspector General (OIG), Defense Information Systems Agency (DISA) and delineates its responsibilities, functions, authorities, and relationships.
2. **Applicability.** This Instruction applies to all DISA activities.
3. **Authority.** This Instruction is published in accordance with the authority contained in Public Law 95-452, Inspector General Act of 1978, as amended; DoD Directive 5106.1, Inspector General of the Department of Defense (IG,DoD), 13 April 2006; DoD Instruction 5505.2, Criminal Investigations of Fraud Offenses, 6 February 2003; DoD Instruction 7050.01, Defense Hotline Program, 17 December 2007; and DoD Directive 5505.6, Investigations of Allegations Against Senior Officials of the Department of Defense, 10 April 2006.
4. **References.**
  - 4.1 DoD Directive 7050.5, Coordination of Remedies for Fraud and Corruption Related to Procurement Activities, 7 June 1989.
  - 4.2 OMB Bulletin No. 01-02, Audit Requirements for Federal Financial Statements, 16 October 2000.
  - 4.3 DISA Instruction 630-85-2, Follow-up on GAO and Inspector General Assessments in DISA, 25 September 2003.
  - 4.4 DISA Instruction 630-85-1, External Audits in DISA, 25 September 2003.

4.5 DoD Directive 1401.3, Reprisal Protection for Nonappropriated Fund Instrumentality Employees/Applicants, 16 October 2001.

4.6 DoD Directive 7050.6, Military Whistleblower Protection, 23 July 2007.

4.7 DoD Directive 6490.1, Mental Health Evaluations of Members of the Armed Forces, 1 October 1997.

5. **Mission.** As an independent office within DISA reporting to the Director, the Office of the Inspector General (OIG) conducts, supervises, monitors, and initiates audits, inspections, and investigations relating to programs and operations of DISA. While not a statutory Inspector General (IG), as established under the provisions of Public Law 95-452, the duties and responsibilities of the OIG complement in nature and scope the DoD IG, which was established under that law.

6. **IG Authority.** The IG is delegated authority from the Director, DISA to conduct investigations, audits, inspections, assessments, and audit liaison and follow-up activities involving the programs and operations of DISA. The IG shall report to and be under the general supervision of the Director/Vice Director, DISA, and is authorized to have direct and prompt access to the Director/Vice Director for any purpose pertaining to the performance of responsibilities under this Instruction. No officer below the Director/Vice Director shall prohibit the IG from initiating, carrying out, or completing any investigation, audit, inspection or assessment. The OIG shall be provided adequate office space at DISA HQS and field office locations as needed, together with adequate resources (e.g., equipment, office supplies, and communications) to accomplish the OIG mission. The IG and members of the OIG are authorized the following accesses and authorities:

6.1 Access to all information, records, reports, investigations, audits, reviews, documents, papers, recommendations, electronic systems/material, or other materials available to any DISA organization or activity as needed to accomplish the IG mission. This authority includes access to personnel and physical areas and to receive clearances, as needed.

6.1.1 Except as specifically denied by the Director DISA pursuant to paragraph [8.1](#), no officer, employee, or Service member assigned to DISA may deny the IG, or officials assigned

by the IG, access to information or prevent them from conducting an audit, inspection, or investigation

6.1.2 OIG members shall possess proper access security clearance when sensitive classified information is requested.

6.2 The authority to administer oaths and affirmations in conjunction with sworn statements; sworn, taped testimony; and affidavits. This authority is derived from 5 U.S.C. 303 and applies to all official investigations undertaken by officially assigned DISA OIG investigators.

6.3 The authority to directly communicate with personnel at all levels of DISA organizations on matters related to IG inquiries. To the extent practicable, the principal directors of strategic business units, directors and chiefs of shared services units, direct reports, and special advisors, Headquarters, DISA, and commanders of DISA combatant command field offices shall be informed that the IG is pursuing a matter within the organization. For audits and inspections, this is generally accomplished by an announcement memorandum.

6.4 The authority to task assistance from DISA organizations as needed to complete investigations, examinations, or inquiries stemming from the Defense Hotline or DISA Hotline. In such cases, taskings shall be routed to the head of the respective strategic business unit, shared services unit, direct report, or special advisor.

## **7. Responsibilities.**

7.1 **DISA Inspector General.** The DISA IG, subject to the direction, control, and authority of the Director, shall:

7.1.1 Serve as the principal advisor to the Director on all audits, investigative, and inspection matters covered under Public Law 95-452 and all matters relating to the prevention and detection of fraud, waste, abuse, and mismanagement in the programs and operations of DISA.

7.1.2 Keep the Director fully and currently informed concerning fraud and other serious problems, waste, abuse, mismanagement, and deficiencies relating to the programs and operations administered or financed by DISA. Recommend corrective actions concerning such problems, abuse, and deficiencies, and report on the progress made in implementing such corrective actions.

7.1.3 Initiate, conduct, and supervise audits, investigations, and inspections in DISA, including all commands and field activities.

7.1.4 Consistent with section 7 of Public Law 95-452 and DoD Directive 7050.1, and in coordination with the Defense Criminal Investigative Service (DCIS), receive and investigate complaints or information concerning the possible existence of any activity constituting a violation of law, rules, or regulations; mismanagement; gross waste of funds; abuse of authority; or a substantial and specific danger to the public health and safety involving DISA.

7.1.5 Promptly refer all allegations of fraud involving persons affiliated with the DoD or any property or programs under Agency control to DCIS in accordance with DoD Instruction 5505.2, Criminal Investigations of Fraud Offenses. Establish procedures for the investigation of fraud allegations that DCIS declines to investigate. Serve as the Agency's designated organization to coordinate and monitor all investigative and corrective activities relating to fraud or corruption in accordance with DoD Directive 7050.5(reference [4.1](#)).

7.1.6 Coordinate actions between DISA and other DoD entities, Federal agencies, state and local government agencies, and nongovernmental entities with respect to the following:

7.1.6.1 All matters relating to the promotion of economy and efficiency in the administration of, or the prevention and detection of, fraud, waste, abuse, or mismanagement in, programs and operations administered or financed by DISA.

7.1.6.2 The identification and prosecution of participants in such fraud or abuse.

7.1.7 Recommend policies for other activities carried out or funded by DISA that promote economy and efficiency in the administration of, or prevention and detection of fraud and abuse in, Agency programs and operations.

7.1.8 Ensure adherence to the professional standards promulgated by the President's Council on Integrity and Efficiency and develop internal policies and procedures to implement these standards on a consistent basis.

7.1.9 Ensure that financial statement audits are performed and audit reports completed in a timely manner and in accordance

with OMB requirements as set forth in OMB Bulletin 01-02 (reference [4.2](#)). (This responsibility pertains to audits conducted directly by IG staff as well as to audits conducted by independent public accountants (IPAs) under contract.) Ensure that the work of non-Federal auditors complies with standards established by the Comptroller General; obtain or conduct quality control reviews of audits made by IPAs and provide the results, when appropriate, to other interested organizations. Monitor and report on management's progress in resolving audit findings related to financial audits made pursuant to reference [4.2](#).

7.1.10 Develop policy, evaluate program performance, and monitor corrective actions taken by all DISA activities in response to DISA OIG audits and inspections; audits and inspections conducted by the DoDIG; and reviews conducted by the Government Accountability Office (GAO). Report on management's progress in resolving findings issued by internal and external audits and inspections in accordance with DISA Instruction 630-85-2 (reference [4.3](#)).

7.1.11 Act as principal point of contact and liaison with DoDIG and GAO to ensure cooperation with them in conduct of their duties, and prompt, clear, and effective response to their reports. Monitor and give particular regard to the activities of the DoDIG and GAO in planning DISA OIG reviews to avoid duplication and ensure effective coverage and coordination in accordance with DISA Instruction 630-85-1 (reference [4.4](#)).

7.1.12 Review existing and proposed legislation and regulations relating to DISA programs and operations and make recommendations to the Director concerning their impact on economy and efficiency or on the prevention and detection of fraud and abuse in DISA programs and operations.

7.1.13 Serve as the single Agency coordinator for both the Defense and DISA Hotline Programs and perform the following functions:

7.1.13.1 Establish procedures to ensure the prompt receipt, processing, controlling, examining, and reporting of all allegations received through the DISA Hotline or referred from the Defense Hotline.

7.1.13.2 Task appropriate staff elements or individuals with the necessary professional or technical skills to assist in or

to conduct examinations or inquiries under the supervision of the responsible audit, inspection, or investigative division.

7.1.13.3 Ensure necessary controls are in place to provide maximum protection for the identity of all hotline users. The IG shall not, after a receipt of a complaint or information from an employee, disclose the identity of the employee without the consent of the employee, unless the IG determines such disclosure is unavoidable during the course of the investigation. Any employee who has authority to take, direct or threaten to take any personnel action, shall not, with respect to such authority take or threaten to take any action against any employee as a reprisal for making a complaint or disclosing information to the IG.

7.1.13.4 Ensure hotline allegations against senior officials are handled in accordance with DoD Directive 5505.6 and paragraph [7.1.15](#) of this instruction.

7.1.13.5 Prepare Defense Hotline Completion Reports and submit to the Defense Hotline within 90 days (180 days for criminal investigations) from the date the complaint was transmitted from the Defense Hotline. Ensure each Defense Hotline case file contains documentation that supports the findings and conclusions contained in the Defense Hotline Completion Report.

7.1.13.6 Ensure that OIG records retention standards specify retention of completed Defense Hotline and DISA Hotline case files for at least 2 years after the inquiry is officially closed

7.1.14 Receive and investigate, consistent with DoD Directives 1401.3 and 7050.6 (references [4.5](#) and [4.6](#), respectively), complaints of reprisal for making disclosures protected by statute. Forward whistleblower allegations originating from military members to the DoDIG for determination of whether investigation is warranted. At the request of the DoDIG, investigate the allegation of reprisal and provide the report to the DoDIG with 180 days of the request. At the request of the DoDIG, investigate the allegation made in the member's original protected communication.

7.1.15 Serve as the component-designated official (CDO) responsible for Agency compliance with DoD Directive 5505.6, Investigations of Allegations Against Senior Officials of the Department of Defense. Report to the DoDIG, within 5 workdays of receipt, all allegations of misconduct made against DISA

senior officials and investigate such allegations in accordance with the directive and DoDIG guidance. Provide to the DoDIG, within 1 week of the completion of the investigation, a copy of the report of investigation (with attachments).

7.1.16 In concert with the DoDIG's Law Enforcement and Counter-Intelligence Center (LECIC), investigate computer intrusion matters affecting the Global Information Grid as the IG considers appropriate.

7.1.17 Receive and investigate, consistent with DoD Directive 6490.1 (reference [4.7](#)), complaints of improper mental health referrals of DISA military members.

7.1.18 Perform local IG records checks on Presidential Award nominees and others as requested by the Office of Personnel Management.

7.1.19 Represent the Director on all OIG activities requiring coordination and or collaboration with outside IGs (i.e., DoD, National Security Agency (NSA), Defense Intelligence Agency (DIA), Department of State, military services, etc.). Ensure, through official and personal interaction with these senior officials, that DISA positions and requirements are properly articulated and known and that the Agency's best interests are served.

7.1.20 Report to the Office of Government Ethics (OGE), using an OGE Form 202 or equivalent, any case(s) involving possible violations of 18 U.S.C. Sections 203, 205, 207-209 by current or former Executive Branch employees.

7.1.21 Perform other duties as assigned by the Director or which are necessary, but not explicitly stated, to accomplish the OIG mission.

**7.2 Principal Directors of Strategic Business Units, Directors and Chiefs of Shared Services Units, Direct Reports, and Special Advisors, Headquarters, DISA, and Commanders of DISA Combatant Command Field Offices.** These individuals will:

7.2.1 Ensure that their organizations and employees cooperate fully with DISA IG audits, investigations, and inspections and that members of the OIG are provided with expeditious and unrestricted access to all information, personnel, facilities, records, reports, investigations, audits, reviews, documents, papers, recommendations, or other material available to any DISA

organization or activity.

7.2.2 Ensure the prompt reporting of all allegations of fraud, all suspected violations of Federal criminal law or the UCMJ, as well as any allegation of serious misconduct against senior officials of the DoD, to the DISA IG.

7.2.3 Respond to management referrals and hotline-related taskings from the DISA OIG.

7.2.4 Provide qualified personnel with the necessary professional and technical skills to assist the IG and the OIG staff in carrying out its activities, to include the augmentation of OIG teams as required.

7.2.5 Submit a report indicating the results of assigned examinations or inquiries along with required supporting documentation through the DISA Assistant IG for Investigations not later than the suspense given.

**7.3 Director for Manpower, Personnel, and Security (MPS).** The Director, MPS will:

7.3.1 Keep the IG apprised of disciplinary or administrative actions resulting from IG investigations.

7.3.2 Exercise primary responsibility for all administrative security investigations, inquiries, and activities. This includes investigations of petty crime done in conjunction with the cognizant Military Criminal Investigative Organization or local police.

**7.4 General Counsel (GC).** The DISA GC will:

7.4.1 Provide advice, counsel, and legal reviews as requested by the DISA IG.

7.4.2 Keep the IG apprised of judicial, non-judicial, or administrative actions taken by the respective Courts Martial Convening Authority in response to IG reports of investigation.

7.4.3 Keep the IG apprised of contractor suspensions, debarments, litigation and other remedies resulting from IG investigations.

7.4.4 Keep the IG apprised of any case(s) involving possible violations of 18 U.S.C. Sections 203, 205, or 207-209 by any



current or former Executive Branch employees.

**7.5 Congressional Affairs (Code CA).** Congressional Affairs will:

7.5.1 Forward to the OIG all GAO inquiries and reviews received that involve DISA but has not been otherwise forwarded to the Director or OIG Audit Liaison.

7.5.2 Forward to the OIG for review legislation that potentially impacts the economy and efficiency of DISA programs and operations or is relevant to the prevention and detection of fraud, waste, and abuse in Agency programs and operations.

**7.6 DISA Employees.** DISA employees will:

7.6.1 Promptly report suspected fraud, waste, or mismanagement via the DoD or DISA Hotline offices indicated below by telephone, mail, email, or website. Individuals who initiate a complaint or provide information to a hotline within the DoD are not required to discuss their complaint or related information with anyone other than the investigator.

7.6.1.1 DoD

1-800-424-9098, (703) 604-8569, or DSN 664-8546

Defense Hotline  
The Pentagon  
Washington, D.C. 22301-1900

hotline@dodig.osd.mil

www.dodig.osd.mil/hotline

7.6.1.2 DISA.

(703) 607-6317 or DSN 327-6317

DISA Office of the Inspector General  
P.O. Box 4502  
Arlington, VA 22204-4502

IG-HOTLINE@disa.mil

7.6.2 Cooperate fully with any audit, inspection, or investigation being conducted by the OIG and shall not withhold

information or documentary materials from the assigned auditor, inspector, or investigator.

7.6.3 Furnish sworn or affirmed oral, taped testimony or subscribed statements upon request, subject to the information on employee rights contained in paragraph [9](#).

7.6.4 Answer questions relating to their employment or matters that have come to their attention in their official capacity or by reason of their employment.

## **8. Relationships.**

8.1 The IG shall carry out designated responsibilities and functions under the general supervision of the Director, DISA. If the Director, DISA decides to restrict IG access to sensitive or classified information, in accordance with the procedures established in DoD Directive 5106.1, the Director shall advise the DoDIG of the denial within 15 working days.

8.2 In performance of assigned responsibilities and functions, the IG will:

8.2.1 Give particular regard to the activities of the Corporate Financial Executive and Comptroller as relates to internal management controls with a view toward avoiding duplication and ensuring effective coordination and cooperation. This recognizes the Comptroller's role as DISA's primary focal point for internal management control policy under the provisions of the Federal Managers' Financial Integrity Act of 1982.

8.2.2 Report expeditiously to the Attorney General, through the DoDIG, whenever the IG has reasonable grounds to believe there has been a violation of Federal criminal law.

8.2.3 Report to the respective Military Service IG any UCMJ violation substantiated by a DISA IG investigation.

8.3 The IG does not investigate allegations pertaining to discrimination. Complainants with such allegations will be referred to the EEO Officer.

8.4 There are many situations for which law or regulation provide employees and military members a remedy or means of redress. They must seek remedy or redress before an IG can provide assistance. Once the complainant has used the available redress procedures, IG assistance is limited to review of the

situation to determine if the complainant was afforded due process provided by law or regulation. Although an issue may not be proper for IG involvement, an IG will provide assistance in referring complainants to the appropriate channel.

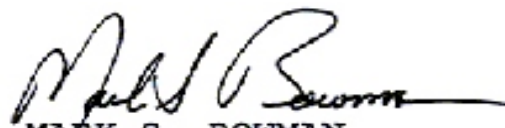
**9. Disciplinary Action and Rights of Employees.** Disciplinary action may be taken against an employee who refuses to cooperate in any of the matters outlined in subparagraph [7.6](#), which details the responsibilities of DISA employees. Employees may assert their Fifth Amendment rights to refuse to answer questions on the grounds that answers might be used against them in a criminal proceeding. Fifth Amendment rights may not be legitimately invoked when the matter being investigated has no connection to a criminal statute or to criminal penalties. Military personnel rights may assert their rights under Article 31(b) of the Uniform Code of Military Justice (UCMJ) if the matter being investigated would constitute a violation of the UCMJ.

9.1 When criminal- or UCMJ-related issues are involved, an employee who asserts Fifth Amendment or Article 31 rights against self-incrimination may not be disciplined solely for remaining silent.

9.2 Employees belonging to a union may invoke their right to have a union representative present under the Weingarten Act if the employee has a reason to believe that he or she may be disciplined as a result of the matter under investigation.

9.3 An employee may be disciplined for refusing to answer a question following a grant of immunity from criminal prosecution properly obtained from the Department of Justice by the OIG.

FOR THE DIRECTOR:



MARK S. BOWMAN  
Brigadier General, USA  
Chief of Staff

\*This Instruction cancels DISAI 100-200-3, 3 June 1994, DISAI 630-125-5, 9 June 1995, and DISAI 220-50-46, 11 June 1996.

OPR: IG

Distribution: Y

---

**Return to:**

[Top of DISA Instruction 100-45-1](#)

[DISA Publications Listing](#)

[DISA Home Page](#)

---

***IGDISA@ncr.disa.mil*** - Last Revision: 11 April 2008

---