DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

DISA INSTRUCTION 100-45-1* 24 March 2017

ORGANIZATION

Office of the Inspector General (OIG)
Defense Information Systems Agency (DISA)

1. **Purpose.** This Instruction describes the mission of and delineates authorities, responsibilities, and relationships for the Office of the Inspector General (OIG) Defense Information Systems Agency (DISA). It advises of disciplinary action and rights of employees. It also advises of hotline office contact information.

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 5106.01, Inspector General of the Department of Defense (IG DoD), 20 April 2012; DoD Instruction 5505.02, Criminal Investigations of Fraud Offenses, 29 August 2013; DoD Instruction 7050.01, Defense Hotline Program, 17 December 2007; and DoD Directive 5505.06, Investigations of Allegations against Senior DoD Officials, 6 June 2013.

4. **References.**

4.1 DISA Instruction 630-85-2, Follow-up on Government Accountability Office (GAO) and Inspector General (IG) Assessments in DISA, 13 December 2013.

4.2 DISA Instruction 630-85-1, External Audits in DISA, 3 October 2013.

4.3 DoD Directive 7050.06, Military Whistleblower Protection, 17 April 2015.

4.4 DoD Instruction 6490.04, Mental Health Evaluations of Members of the Military Services, 4 March 2013.

5. **Mission.** As an independent office within DISA reporting to the Director, DISA, the Office of the Inspector General (IG) conducts, supervises, monitors, and initiates audits, inspections, and investigations relating to programs and operations of DISA. In addition, the OIG operates a Hotline Program and provides assistance to complainants, if appropriate. While not a statutory Inspector General (IG), as established under the provisions of Public Law 95-452 (IG Act of 1978), the responsibilities of the IG complement in nature and scope those of the Inspector General of the Department of Defense (IG DoD), which was established under that law.

6. **IG Authority.** The IG is delegated authority from the Director, DISA, to operate a hotline and to conduct investigations, audits, inspections, special assessments, and audit liaison follow-up activities involving the programs and operations of DISA. The IG reports to and is under the general supervision of the Director, DISA, and is authorized to have direct and prompt access to the Director and Vice Director for any purpose pertaining to the performance of responsibilities assigned in this Instruction. A DISA employee below the level of the Director shall not prohibit the IG from initiating, carrying out, or completing any investigation, audit, inspection, or assessment. The IG will be provided adequate office space at DISA headquarters and field offices, as needed, together with adequate resources (e.g., equipment, office supplies, communications, and funds) to accomplish the IG mission. A DISA organization will not conduct a parallel investigation, audit, inspection, or assessment regarding a subject matter while the OIG is involved in an investigation of that same subject matter. The IG and members of the OIG are authorized the following accesses, security clearances, and authorities:

6.1 Access to all information, records, reports, investigations, audits, reviews, documents, papers, recommendations, and electronic systems and material or other materials available to any DISA organization or activity, as needed, to accomplish the OIG mission. This authority includes access to personnel and physical areas. There is no further written request, other than this Instruction, required for an OIG member to access or receive these items. Unless specifically denied by the Director, pursuant to subparagraph 8.2, no employee or Service member assigned to DISA may deny OIG personnel or officials assigned by the OIG (subject matter experts) access to information or prevent them from conducting an audit, inspection, investigation, or assessment.

6.2 Appropriate security clearance (top secret [TS] is the standard) due to the potential for handling classified information. The OIG staff assigned to the IG Hotline shall have a TS/SCI (sensitive compartmented information) security clearance due to the potential to receive Joint Worldwide Intelligence Communications System (JWICS) Hotlines from DoD IG. In order to provide complete oversight of all Agency activities, OIG personnel will be granted access to all classified programs.

6.3 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., Government Organization and Employees, and applies to all official investigations undertaken by OIG investigators.)

6.4 The authority to directly communicate with personnel at all levels of DISA organizations on matters being reviewed, oversighted, inspected, audited, or investigated by the OIG. (To the extent practicable, a Director of a center or directorate will be informed that the OIG is pursuing a matter within the organization, unless the matter directly involves the personal conduct of those leaders. [For audit and inspection, notifications are generally accomplished by an announcement memorandum. For investigations, a letter (or e-mail) to the Director, Executive, Commander, or Chief is normally provided.])

6.5 The authority to task assistance from DISA organizations, as needed, to complete investigations, examinations, or inquiries stemming from the DoD IG Hotline or DISA IG Hotline. (In such cases, a tasking shall be routed to the Director of the respective center or directorate.)

7. **Responsibilities**.

7.1 **DISA Inspector General (IG)**. 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 audits, investigations, and inspections covered under The Inspector General Act of 1978 relating to the prevention and detection of fraud, waste, abuse, and mismanagement in the programs and operations of the Agency.

7.1.2 Keep the Director fully and currently informed concerning fraud and other serious problems, waste, abuse, mismanagement, and deficiencies relating to programs and operations administered or financed by the Agency. 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, inspections, and assessments in the Agency including all commands and field activities.

7.1.4 Consistent with section 7 of Public Law 95-452, 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, rule, policy, or regulation; mismanagement; gross waste of funds; abuse of authority; or a substantial and specific danger to public health and safety involving the Agency.

7.1.5 Refer all allegations of fraud involving persons affiliated with DoD or any property or programs under Agency control to DCIS, in accordance with DoD Instruction 5505.02, Criminal Investigations of Fraud Offenses (authority document).

7.1.5.1 Establish procedures for the investigation of fraud allegations or other criminal matters that DCIS declines to investigate.

7.1.5.2 Serve as the Agency's designated organization to coordinate and monitor all investigative and corrective activities relating to fraud or corruption, to include being the focal point for Agency-wide fraud awareness.

7.1.6 Coordinate actions between DISA and other DoD entities; Federal agencies, state and local government agencies; and nongovernmental entities with respect to 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 and identification of fraud participants for potential prosecution.

7.1.7 Establish proactive OIG procedures to uncover fraud patterns that will identify and predict future fraud risks.

7.1.8 Ensure adherence to the professional standards promulgated by the Council of Inspectors General for Integrity and Efficiency (CIGIE) and develop internal policies and procedures to implement these standards on a consistent basis.

7.1.9 Act as the Agency's principal point of contact for independent internal audits, attestation engagements, and nonaudit services of DISA organizations, programs, activities, and functions.

7.1.9.1 Establish policy, assign responsibilities, and prescribe procedures for DISA audits and attestation engagements to determine whether internal control systems are properly designed, sufficient, and effective; information is reliable and relevant; applicable laws, regulations, and policies are followed; assets and resources are safeguarded; desired program results are achieved; and operations are effective and efficient.

7.1.9.2 Ensure nonaudit services do not create an impairment to OIG independence. (Nonaudit services are performed to assist management officials in performing tasks that directly support an organization's operations.)

7.1.9.3 Ensure financial statement audits are performed and audit reports are completed in a timely manner, in accordance with Office of Management and Budget (OMB) requirements, as set forth in OMB Bulletin 07-04, Audit Requirements for Federal Financial Statements, amended by M-09-3, Technical Amendments to OMB Bulletin No. 07-04. (This responsibility pertains to audits conducted directly by the OIG staff, as well as audits conducted by independent public accountants [IPAs] under contract.) Ensure the work of nonfederal auditors complies with standards established by the Comptroller General and 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 OMB Bulletin 07-04.

7.1.10 Act as the Agency's principal point of contact and liaison with the IG DoD, Government Accountability Office (GAO), and other external agencies to ensure cooperation in the conduct of audits, inspections, and investigative activity.

7.1.10.1 Evaluate program performance and monitor corrective actions taken by DISA activities in response to DISA IG audits and inspections, audits and inspections conducted by the IG DoD, reviews conducted by the GAO, and other audits conducted by external audit agencies. Report on management's progress in resolving findings issued by internal and external audits and inspections, in accordance with DISA Instruction (DISAI) 630-85-2, Follow-up on Government Accountability Office (GAO) and Inspector General (IG) Assessments in DISA (reference 4.1).

7.1.10.2 Ensure prompt and effective responses to external Agency audit reports. Monitor the activities of the IG DoD and GAO in planning DISA IG reviews to avoid duplication and ensure effective coverage and coordination, in accordance with DISAI 630-85-1, External Audits in DISA (reference 4.2).

7.1.11 Review existing and proposed OIG-related 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.

7.1.12 Serve as the single Agency coordinator for the DISA IG Hotline and perform the following functions:

7.1.12.1 Establish procedures to ensure the prompt receipt, processing, controlling, examining, and reporting of allegations received through DISA IG Hotline channels or referred from the DoD IG Hotline to include hotline complaints received via the Nonsecure Internet Protocol Router Network (NIPRNET), Secret Internet Protocol Router Network (SIPRNET), and Joint Worldwide Intelligence Communications System (JWICS).

7.1.12.2 Ensure necessary controls are in place to provide confidentiality for the identity of hotline users.

7.1.12.3 Ensure hotline allegations against senior officials are handled in accordance with DoD Directive 5505.06, Investigations of Allegations against Senior DoD Officials (authority document), and subparagraph 7.1.16.

7.1.12.4 Prepare DoD IG Hotline completion reports in response to action referrals. Ensure each DoD IG Hotline case file contains documentation that supports the findings and conclusions contained in the DoD IG Hotline completion report.

7.1.13 Task appropriate DISA staff elements or individuals (subject matter experts) 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.

7.1.14 Receive and investigate, consistent with DoD Directive 7050.06, Military Whistleblower Protection (reference 4.3), complaints of military whistleblower reprisal for making disclosures protected by statute. Forward military whistleblower reprisal allegations to the IG DoD for determination as to whether the investigation is warranted. At the direction of the IG DoD, investigate the allegation of reprisal and provide the report to the IG DoD. At the direction of the IG DoD, investigate the allegation made in the member's original protected communication, if necessary.

7.1.15 Forward allegations of civilian whistleblower reprisal to the IG DoD Directorate for Whistleblower Reprisal Investigations (WRI). (The IG DoD manages investigations involving reprisals against government civilians, as the DISA IG is not authorized.)

7.1.16 Serve as the component-designated official (CDO) responsible for Agency compliance with DoD Directive 5505.06 (authority document). Report to the IG DoD, within 5 workdays of receipt, all allegations of misconduct made against DISA senior officials and investigate such

allegations, in accordance with DoD 5505.06 and IG DoD guidance. Provide to the IG DoD, within 1 week of the completion of the investigation, a copy of the report of investigation (with attachments).

7.1.17 Investigate computer intrusion matters affecting the DoD Information Networks (DODIN), in coordination with the DoD IG Law Enforcement and Counter-Intelligence Center (LECIC), as the IG considers appropriate.

7.1.18 Receive and investigate, consistent with DoD Instruction 6490.04, Mental Health Evaluations of Members of the Military Services (reference 4.4), complaints of improper mental health referrals of DISA military members.

7.1.19 Perform local OIG records checks on Presidential award nominees and others, as requested by the Office of Personnel Management (OPM).

7.1.20 Represent the Director on all OIG activities requiring coordination and 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, DISA positions and requirements are properly articulated and known.

7.1.21 Report to the Office of Government Ethics (OGE), using an OGE Form 202: Notice of Conflict of Interest Referral, or equivalent, any case(s) involving possible violations of 18 U.S.C. Sections 203, 205, and 207-209 by current or former General Officers or Senior Executives.

7.1.22 Perform other duties as assigned by the Director which are necessary to accomplish the IG mission.

7.2 **Directors, Executives, Commanders, and Chiefs of Major Organizational Elements**. These individuals will:

7.2.1 Ensure their organizations and employees cooperate fully with DISA OIG audits, investigations, inspections, and audit liaison activities and that OIG personnel 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 and suspected violations of Federal criminal law or the Uniform Code of Military Justice (UCMJ), as well as any allegation of serious misconduct against DoD senior officials, to the DISA IG or IG DoD.

7.2.3 Promptly respond to management referrals and hotline-related taskings from the DISA IG.

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 audit and inspection teams.

7.2.5 Make timely decisions and take responsive actions on audit, inspection, and investigation findings to include recommendations to reduce costs, manage risks, and improve management processes.

7.3 **Workforce Services Executive (WSE)**. The WSE will:

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

7.3.2 Exercise primary responsibility for all administrative security investigations, inquiries, and activities. (This includes investigations of petty crime conducted in conjunction with the cognizant military criminal investigative organization or local police.)

7.4 **General Counsel (GC)**. The 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, nonjudicial, or administrative actions taken by the respective courts martial convening authority in response to OIG reports of investigation.

7.4.3 Keep the IG apprised of contractor suspensions, debarments, litigation, and other remedies resulting from OIG 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 General Officer or Senior Executive.

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

7.5.1 Forward to the IG all GAO inquiries and reviews received that involve DISA but have not been otherwise forwarded to the Director or IG audit liaison.

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

8. **DISA Employee Responsibilities.** DISA employees will**:**

8.1 Promptly report suspected fraud, waste, or mismanagement via the DoD or DISA Hotline Offices. (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. [Refer to paragraph 11 for telephone, mail, e-mail, and Web site contact information.])

8.2 Cooperate fully with any audit, inspection, or investigation being conducted by the IG and not withhold information or documentary materials from the assigned auditor, inspector, or investigator.

8.3 Furnish sworn or affirmed oral, taped testimony, or subscribed statements, upon request, subject to the information on employee rights contained in paragraph 10.

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

8.5 Attempt to first remedy or redress the issue before reporting it to the IG by following mandated processes and procedures, as applicable by laws, regulations, and policies. (Assistance from the IG is usually limited to review of the situation to determine if the complainant was afforded due process provided by law or regulation. If an issue is not appropriate for IG involvement, the IG will provide assistance to refer complainants to the proper channel.)

9. **Relationships**.

9.1 The IG shall carry out designated responsibilities and functions under the general supervision of the Director. If the Director decides to restrict IG access to sensitive or classified information, in accordance with the procedures established in DoD Directive 5106.01, Inspector General of the Department of Defense (IG DoD) (authority document), the Director shall advise the IG DoD of the denial within 15 working days.

9.2 In performance of responsibilities and functions, the IG will:

9.2.1 Give particular regard to the activities of the Resource Management Center (RMC) as they relate to internal management controls, in order to avoid duplication and ensure effective coordination and cooperation. This recognizes the Comptroller's role as DISA primary focal point for internal management control policy under the provisions of the Federal Managers' Financial Integrity Act of 1982.

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

9.2.3 Report to the respective Military Service IG any Uniform Code of Military Justice (UCMJ) violation substantiated by a DISA IG investigation.

9.3 The IG does not normally investigate allegations pertaining to discrimination. Complainants with such allegations are normally referred to the DISA Office of Equality, Diversity, and Inclusion (OEDI), unless allegations are imbedded in an IG formal investigation.

10. **Disciplinary Action and Rights of Employees**.

10.1 Employees have a duty to cooperate fully and completely with IG staff. Disciplinary action may be taken against an employee who does not cooperate in any matter, as outlined in chapter 752, section F, Table of Offenses and Penalties, of DISA Instruction 220-15-55, Civilian Personnel Management Manual.

10.2 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. However, 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 may assert their rights under Article 31(b) of the UCMJ if the individual is suspected of a criminal offense. 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.

10.3 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 investigation.

10.4 Employees may be disciplined for refusing to answer a question following a grant of immunity from criminal prosecution properly obtained from the Department of Justice.

11. **Hotline Office Contact Information.**

11.1 **DoD Hotline Office.**

1-800-424-9098

DoD Hotline
The Pentagon
Washington, DC 20301-1900

Hotline@DoDIG.mil

www.DoDIG.mil/Hotline

11.2 **DISA Hotline Office.**

301-225-6250, DSN 375-6250, or 1-800-266-5173

DISA Office of the Inspector General
P.O. Box 549
Fort Meade, MD 20755-0549

disa.meade.ig.mbx.ig-hotline@mail.mil

ROSENSTEIN.MARK.ERIC.1078644431
Digitally signed by ROSENSTEIN.MARK.ERIC.1078644431
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=ROSENSTEIN.MARK.ERIC.1078644431
Date: 2017.03.23 14:41:12 -04'00'

MARK E. ROSENSTEIN
Colonel, USA
Chief of Staff

SUMMARY OF SIGNIFICANT CHANGES. This revision includes administrative updates.

---

*This Instruction replaces DISAI 100-45-1, 6 December 2012.
OPR: IG - disa.meade.ig.mbx.disa-ig@mail.mil
DISTRIBUTION: Approved for public release; distribution is unlimited.