DCMA Manual 4201-07

Personnel Security

Office of Primary Responsibility	**Talent Management Capability**
Effective:	April 28, 2019
Releasability:	Cleared for public release
Implements:	DCMA-INST 4201, "Civilian Personnel," July 20, 2018
Incorporates and Cancels:	DCMA-INST 555, "Personnel Security," October 22, 2012 DCMA-INST 560, Pre-appointment Investigations Waivers," May 2010
Internal Control:	Process flow and key controls are located on the Resource Page
Labor Codes:	Located on the Resource Page
Resource Page:	https://360.dcma.mil/sites/policy/TM/SitePages/4201-07r.aspx
Approved by:	David H. Lewis, VADM, USN, Director

Purpose: This issuance, in accordance with the authority in DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)," implements policy, assigns responsibility, and establishes procedures for implementing the requirements of DoD Instruction 5200.02, "DoD Personnel Security Program (PSP)," DoD Manual 5200.02, "Procedures For The DoD Personnel Security Program (PSP)," DCMA Instruction 4201, "Civilian Personnel," and other applicable references.

TABLE OF CONTENTS

TABLES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This Manual applies to all DCMA organizations and personnel. This Manual does not address the unique security requirements specifically associated with Special Access Programs.

1.2. POLICY. It is DCMA policy to:

a. Ensure access to classified national security information is strictly controlled and granted only in accordance with applicable DoD policy and this Manual.

b. Implement a Personnel Security (PERSEC) Program that complies with the requirements contained in DoD Directive (DoDD) 5105.64, DoD Instruction (DoDI) 5200.02, DoD Manual (DoDM) 5200.02 and other prescribing directives and DoD issuances.

c. Continuously review position sensitivity for all civilian positions to ensure proper designation in accordance with assigned duties.

d. Ensure position sensitivity is designated in accordance with this Manual and applicable DoD policy.

e. Execute this Manual in a safe, efficient, effective, and ethical manner.

SECTION 2: RESPONSIBILITIES

2.1. DIRECTOR, DCMA. The Director, DCMA will:

a. Ensure the establishment and resourcing of a comprehensive PERSEC Program that complies with the requirements established in DoDI 5200.02, DoDD 5105.64, and other applicable references.

b. Designate a senior agency official with responsibility for the overarching management and oversight of the PERSEC Program.

2.2. DIRECTOR, SECURITY AND COUNTERINTELLIGENCE (CI). The Director, Security and CI will:

a. Serve as the Agency senior PERSEC official responsible for the development, implementation, and oversight of the PERSEC Program.

b. Appoint a Program Manager (PM) to manage the Agency's PERSEC Program.

c. Ensure the PERSEC Program is integrated with other security-related programs in support of an overarching security/mission assurance construct.

d. Advocate for and allocate resources in support of the PERSEC Program.

e. Nominate Agency primary and alternate representatives to the Washington Headquarters Services (WHS), Clearance Appeal Board (CAB).

2.3. PROGRAM MANAGER, PERSEC PROGRAM. The PERSEC PM will:

a. Develop and manage an effective PERSEC Program that meets the spirit and intent of the prescribing directives.

b. Develop and maintain Agency-level PERSEC policy that ensures compliance with the prescribing directives and tailored to the DCMA mission.

c. Identify and manage resources assigned to support the PERSEC Program.

d. Maintain close liaison and coordination with all PERSEC Program stakeholders.

e. Develop and Implement an effective PERSEC assessment program.

f. Implement other requirements listed herein.

2.4. PERSEC TEAM SUPERVISOR. The PERSEC Team Supervisor will:

a. Report to the PERSEC PM and manage all operational aspects of the PERSEC Program.

b. Ensure the effective and efficient execution of PERSEC programs and policies.

c. Ensure required PERSEC Program related training is developed, maintained, implemented, and tracked.

d. Consolidate and report PERSEC Program resource requirements.

e. Implement other requirements listed herein as directed by the PERSEC PM.

2.5. PERSEC SPECIALISTS. PERSEC Specialists will:

a. Provide PERSEC advice, assistance, and support to all levels of the organization.

b. Initiate and submit requests for the conduct of personnel security investigations (PSIs) to the Office of Personnel Management (OPM) for DCMA employees and applicants in accordance with DoDM 5200.02 and this Manual.

c. Comply with all requirements contained in this Manual.

d. Conduct pre-appointment security checks in accordance with this Manual and Part 1400 of Title 5, Code of Federal Regulations (CFR).

e. Certify the clearance eligibility of personnel for access to classified information, enter access into the DoD Joint Personnel Adjudication System (JPAS), and eligibility into the DCMA Automated Listing of Eligibility and Clearances (ALEC).

f. Advise activities on compliance with DoDM 5200.02, to include the conduct of required briefings, debriefings, notices of clearance status, and designations of position sensitivity.

g. Receive and process reports of unfavorable administrative actions.

h. Monitor and report to the PERSEC PM status changes on cases pending adjudication.

i. Out-process JPAS and ALEC records on all personnel departing from the Agency.

j. Provide PERSEC Program training and guidance to Directorate and Contract Management Office (CMO) security representatives.

2.6. OFFICE OF GENERAL COUNSEL (OGC). The OGC will provide legal assistance and advice in support of the PERSEC Program.

2.7. EXECUTIVE DIRECTOR, HUMAN CAPITAL (HC) DIRECTORATE. The Executive Director, HC will:

a. Provide functional advice and assistance in support of the PERSEC Program.

b. Conduct suitability determinations for civilian employees in accordance with the provisions of Part 731 of Title 5, CFR and applicable OPM regulations.

c. Ensure that all civilian positions are officially designated as non-sensitive, non-critical sensitive, critical sensitive, or special sensitive at the time of position classification and classification review.

d. Ensure Job Opportunity Announcements (JOA) for sensitive positions address pre-appointment investigative requirements.

e. Ensure the Army Servicing Team (AST) submits requests for pre-appointment security checks to the DCMA PERSEC staff for all selectees for appointment, transfer, or reinstatement to sensitive positions.

2.8. DCMA COMPONENT HEADS AND COMMANDERS/DIRECTORS OF CONTRACT MANAGEMENT OFFICES (CMO). The DCMA Component Heads and Commanders/Directors of CMOs will:

a. Ensure appropriate position sensitivity is assigned to civilian positions in accordance with DoDD 5105.64, DoDM 5200.02 and this Manual.

b. Review and approve requirements for access to classified national security information in accordance with DoDD 5105.64, DoDM 5200.02 and this Manual.

c. Render decisions to temporarily suspend access to classified national security information in accordance with DoDD 5105.64 and DoDM 5200.02, when the totality of unfavorable information raises doubt as to whether an individual’s continued eligibility for access to classified information or assignment to sensitive duties is in the best interest of national security.

d. Ensure reporting responsibilities are accomplished as directed by this Manual.

e. Ensure supervisor's include discharge of security responsibilities in his or her fitness for performance standards as outlined in DoDM 5200.02, Section 11, paragraph 11.2.a.(2)(c).

f. Appoint a primary and alternate security representative to perform organizational administrative duties associated with the PERSEC Program.

2.9. SECURITY REPRESENTATIVES. Security Representatives will:

a. Provide administrative PERSEC Program support to the assigned organization.

b. Coordinate PERSEC related issues, questions, or concerns with the DCMA PERSEC staff.

c. Brief and debrief employees for access to classified information.

d. Report PERSEC actions taken by the assigned organization to the DCMA PERSEC staff.

2.10. DIRECTOR, SPECIAL PROGRAMS COMMAND (DCMAS). The Director, DCMAS will:

a. Maintain a directorate-specific security staff that is trained and experienced in the execution of the DoD and DCMA PERSEC Programs.

b. Identify and report PERSEC Program resource requirements to the DCMA PERSEC PM.

c. Establish and maintain such directorate-specific policies and procedures to effectively implement the provisions of DoDM 5200.02, this Manual, and any and all Special Access Program (SAP) unique security requirements. Ensure all SAP unique policies and procedures are fully coordinated with the applicable Special Access Program Central Office (SAPCO).

d. Maintain oversight of the directorate's security staff and ensure recurring oversight assessments are conducted to ensure compliance with all PERSEC Program requirements.

2.11. PROGRAM MANAGER, ANTITERRORISM (AT)/PHYSICAL SECURITY PROGRAM. The AT/Physical Security PM will establish processes that ensure an initial security orientation addressing basic PERSEC principles is provided to all new DCMA employees within 60 calendar days of their assignment.

2.12. DCMA PERSONNEL. DCMA personnel will:

a. Complete PERSEC training as prescribed in Section 11 of this Manual.

b. Promptly report to the DCMA PERSEC staff any information meeting the provisions of Security Executive Agent Directive (SEAD) 4, "National Security Adjudicative Guidelines," as outlined in Section 8 of this Manual.

SECTION 3: DESIGNATE POSITION SENSITIVITY

3.1. GENERAL. All DCMA civilian positions shall be assigned an appropriate position sensitivity designation in compliance with DoDM 5200.02 and Parts 731 and 1400 of Title 5, CFR. The position sensitivity designation is used to determine the appropriate type and/or scope of background investigation potential employees must successfully undergo prior to assignment to sensitive duties, access to classified national security information, and/or before any suitability for employment determination is made.

3.2. DETERMINE AND ASSIGN POSITION SENSITIVITY.

a. The responsible manager/supervisor establishing a new civilian position and prior to recruitment for an existing position will carefully evaluate the position duties and requirements to determine if the incumbent will require access to classified national security materials, be assigned to sensitive duties, and/or require access to federal computer systems.

b. In accordance with DoDM 5200.02 and Parts 731 and 1400 of Title 5, CFR, the responsible manager/supervisor will apply the criteria contained in DoDM 5200.02, Section 3, and assign position sensitivity designation to the position. Position sensitivity designations will be limited to one of the following:

- Code 1 – Non-Sensitive
- Code 2 – Non-Critical Sensitive
- Code 3 - Critical Sensitive
- Code 4 - Special Sensitive

c. Managers evaluating positions associated with Federal Computer Systems, Automated Data Processing/Information Technology (ADP/IT-I, ADP/IT-II and ADP/IT-III), shall coordinate with the DCMA Information Assurance Officer prior to assigning position sensitivity.

d. Once the position sensitivity determination is made, the responsible manager will submit a Request for Personnel Action (RPA) to recruit for the position. The RPA will include the appropriate position sensitivity designation.

3.3. CHANGING POSITION SENSITIVITY.

a. Managers will carefully consider any change to the position sensitivity designation once it has been officially established in Agency records and the position is filled. It is important that managers carefully assess a change requiring a higher position sensitivity designation, as it may require the position's incumbent to successfully undergo additional investigative and adjudicative requirements before the individual can assume the new duties warranting the change.

b. In instances where the manager determines a change in the position's duties require a change in position sensitivity in order to properly accomplish the mission, the manager will apply the criteria in paragraph 3.2. to identify the appropriate position sensitivity designation.

c. To change the position sensitivity designation, the manager will prepare an RPA requesting the change and forward it to the AST. The RPA initiates the change in position sensitivity and ensures all official records are updated to reflect the change.

d. Upon receipt of notice from the AST that the change in position sensitivity is officially recorded, the manager will submit a DCMA Form 12.15.1-2, "Determination of Need for Clearance/Position Sensitivity Change" (hereafter referred to as DCMA Form 1-2), to the servicing PERSEC Specialist for processing.

(1) The servicing PERSEC Specialist will review the DoD JPAS and the OPM Central Verification System (CVS) to determine if the incumbent possesses the requisite background investigation and/or security eligibility.

(2) If the incumbent possesses the requisite investigation and/or security eligibility, the PERSEC Specialist will annotate the DCMA Form 1-2 as such, appropriately update the applicable DCMA records/databases, and ensure the DCMA Form 1-2 is filed in the individual's Electronic Personnel Security File (EPSF). The PERSEC Specialist will provide an email notice to the appropriate manager indicating the change in position sensitivity.

(3) If the incumbent does not possess the requisite investigation and security eligibility, the PERSEC Specialist will notify the incumbent of the requirement to complete the Standard Form (SF) 86, "Questionnaire for National Security Position," via the electronic Questionnaires for Investigations Process (e-QIP) system and provide additional information, as required.

e. Under no circumstance will any manager change the position sensitivity designation of an established position in an attempt to expedite recruitment efforts. Any actual or suspected incidents of personnel attempting to manipulate or circumvent federal law, DoD or DCMA PERSEC policy relative to position sensitivity designations will be reported to the DCMA Director of Security and CI and to the DCMA Inspector General for prompt investigation.

3.4. RECORDING POSITION SENSITIVITY. The Executive Director, HC will establish processes that ensure the sensitivity designation of every DCMA civilian position is recorded in the Agency's official records. Such records will include, but not be limited to, position descriptions and in official personnel automated records such as the Defense Civilian Personnel Database System.

SECTION 4: PERSONNEL SECURITY INVESTIGATIONS

4.1. GENERAL. All civilian employees/selectees with a tentative job offer are subject to a pre-appointment security background investigation. The type and/or level of investigation is determined based on the assigned sensitivity designation for the offered position as discussed in Section 3.

4.2. SENSITIVE POSITIONS.

a. Once the hiring manager selects a candidate to fill a sensitive position and a tentative offer of employment is extended, the AST submits a DCMA Form 12.15.1-1, "Pre-appointment Security Form," and other requisite documents (i.e., DD 214, "Certificate of Release or Discharge from Active Duty," SF 50, "Notice of Personnel Action," Optional Form (OF) 306, "Declaration of Federal Employment," and current resume, etc.) to the applicable DCMA Security Office to initiate a pre-appointment security check.

b. The PERSEC Specialist will review all forms submitted to establish if prior federal service exists. In addition, the PERSEC Specialist will review the DoD JPAS and OPM CVS to determine if a previously favorable adjudicated investigation has been performed on the applicant.

(1) Personnel with Previously Adjudicated Investigations.

(a) Applicants shall be deemed eligible for appointment to a sensitive position when:

- There is a valid investigation that has been favorably adjudicated in accordance with DoDM 5200.02 and this Manual
- No non-favorable information has developed subsequent to the most recent favorably adjudicated background investigation
- A reciprocal/recertify clearance has been granted by the servicing DoD Consolidated Adjudications Facility (CAF)

1. Applicants with a previously conducted National Agency Check and Inquiries (NACI), National Agency Check with Law and Credit (NACLC), Single Scope Background Investigation (SSBI), or Tier level investigation equivalent that has been favorably adjudicated within a 5 year timeframe during military or contractor employment, there is not more than a 24-month break in service, and where no unfavorable information has developed subsequent to the most recent favorably adjudicated background investigation will be deemed eligible for appointment to a sensitive position provided that the appropriate investigation has been submitted to OPM.

2. Applicants being deemed initially eligible for appointment in accordance with paragraph 4.2.b(1)(a)1 remain subject to the complete investigative and adjudicative process.

(b) Applicants with identified unfavorable information subsequent to the most recent favorably adjudicated background investigation are deemed ineligible for appointment until such time as the background investigation is completed and a favorable adjudication is rendered.

1. If unfavorable information is developed meeting the criteria of SEAD 4 and the information does not appear to have been previously reviewed by an adjudication facility, the PERSEC Specialist will forward the unfavorable information to the DoD CAF for review and a final eligibility determination.

2. Under such conditions as described in paragraph 4.2.b(1), the PERSEC Specialists will return the DCMA Form 12.15.1-1 to the AST indicating the applicant requires additional security adjudication and is ineligible for appointment to a sensitive position until a favorable determination is received.

(2) Personnel whose records indicate a current or prior affiliation with an intelligence agency, the PERSEC Specialist will request the DoD CAF to conduct a query of Scattered Castles intelligence community database to determine if the applicant has been subject to a favorable adjudicated backbround investigation.

(3) Personnel With No Previously Adjudicated Investigation. Personnel with no previously adjudicated investigation will be processed in accordance with Appendix 4A of this Manual.

(4) In accordance with SEAD 4 and Paragraph 3.4.c.(1) of DoDM 5200.02, an individual's failure to respond with the required security forms or refusal to provide or permit access to the relevant information required by DoD policy within the time limit prescribed by DCMA Security may result in suspension of access to classified information and/or being determined ineligible for assignment to sensitive duties until the investigation is completed and adjudicated.

4.3. NON-SENSITIVE POSITIONS.

a. Once a tentative selection is made for a non-sensitive position, the AST submits a DCMA Form 12.15.1-1 to the applicable DCMA Security Office for processing.

b. The PERSEC Specialist shall notify the selectee of the requirement to complete the SF-85, "Questionnaire for Non-Sensitive Positions," via the e-QIP system and submit SF-87, "Fingerprint Cards." Once the completed fingerprint cards are received from the applicant and favorable fingerprint results returned from OPM, the PERSEC Specialist will then return the DCMA Form 12.15.1-1 to the AST indicating the selectee is cleared for appointment.

c. Within 3 calendar days of the selectee's entry on duty, the PERSEC Specialist shall submit a Tier One (T1) investigation to OPM for processing.

d. Upon completion of the investigation, OPM will forward the investigative results to the DoD CAF for a Suitability for Government Employment determination.

(1) Favorable Decision. The DoD CAF provides DCMA notice of the Suitability determination via the DoD JPAS. Upon receipt of notification of a favorable determination, the PERSEC Specialist will update the DCMA ALEC database.

(2) Unfavorable Decision. If the DoD CAF is unable to make a favorable Suitability determination, the PERSEC Specialist will forward the results to the DCMA HC Directorate, Office of Labor and Employee Relations (LER), who will carefully consider the information contained in the investigative results and render a Suitability for Government Employment decision.

e. The DCMA HC Directorate LER Office will forward their decision to DCMA Security for submission to OPM. In addition, the PERSEC Specialist will ensure the ALEC database is updated to reflect the suitability decision.

4.4. MILITARY PERSONNEL CLEARANCE ELIGIBILITY.

a. The required level of clearance and/or access for Military Personnel is based strictly on need-to-know requirements related to the duties associated with assignment to DCMA.

b. The DCMA Military Personnel Office will validate and record the required level of clearance in the DCMA military billet records to ensure the selection for military assignment orders considers clearance requirements.

c. While responsibility for adjudicating clearance eligibility for military personnel assigned to DCMA remains with the parent military service, the serving DCMA PERSEC Specialist will provide administrative support by processing and submitting required PSIs while the military member is assigned to DCMA.

4.5. SUBMITTING INVESTIGATIONS.

a. Upon receipt of all documentation required for the applicable investigation from the applicant/selectee, the responsible PERSEC Specialist will, within 7 calendar days of receipt, complete a thorough review of the entire investigative package to validate it is complete. Once all documents are validated, the PERSEC Specialist will forward all documentation under a request for investigation to OPM who will conduct the investigation. Should the PERSEC Specialist determine documentation is incomplete, the subject of the PERSEC investigation will be notified and directed to make the required corrections.

b. DCMAS will identify and process all PSIs for personnel assigned to the Command. DCMAS PERSEC Specialists will ensure all non-SAP specific processes established herein or in DoDM 5200.02 are followed.

c. Types of PSIs required. Table 1 lists the types of security investigations required by position designation.

Table 1. Types of Personnel Security Investigations Required

Position Designation	PSI Required
Non-Sensitive Positions, Low Risk, Homeland Security Presiential Directive 12 Credential, ADP/IT III	NACI or T1 equivalent
Noncritical-Sensitive Positions, Secret/Confidential Security Clearance, ADP/IT II	Access National Agency Check and Inquiries (ANACI) or Tier Three (T3) equivalent
Special Sensitive or Critical Sensitive Positions, Top Secret Security Clearance, Sensitive Compartmented Information (SCI), ADP/IT I	SSBI or Tier Five (T5) equivalent

4.6. NON-U.S. CITIZENS EMPLOYED OVERSEAS. Non-U.S. citizens employed in a foreign country by DCMA will be subject to the appropriate records check requirements contained in DoDM 5200.02, Section 4, Paragraph 4.5.

APPENDIX 4A: PRE-APPOINTMENT INVESTIGATIONS WAIVER

4A.1. DoDM 5200.02 and Part 1400 of Title 5, CFR. authorizes the granting of temporary eligibility for access to classified information or assignment to a Critical or Non-Critical Sensitive national security position while the initial investigation is underway but not completed. In accordance with Part 1400 of Title 5, CFR, positions designated as Special Sensitive are prohibited from being granted temporary eligibility. DoDD 5105.64, delegates DCMA the authority to grant termporary eligibility.

4A.2. PREAPPOINTMENT SECURITY CHECK. The guidance documented herein addresses the preappointment security check processes implemented within DCMA.

a. The AST notifies DCMA Security of tentative offers of employment and requests personnel security pre-appointment security checks to determine the applicant's security eligibility to occupy the position for which selected. The AST makes notification to DCMA Security using the DCMA Form 12.15.1-1 (DCMA Form 1-1).

b. Upon receipt of the DCMA Form 1-1, DCMA PERSEC Specialists will review the position sensitivity of the position in question, the DoD JPAS, the OPM CVS, and any other applicable authoritative information sources to determine if the prospective applicant already possesses the requisite investigation and favorable adjudication determination.

(1) All personnel involved in the process documented herein, to include the appeal process, will safeguard personnel security records and information in accordance with DoDM 5200.02, Section 5, and this Manual.

(2) Records and information that contain potentially unfavorable information will not be released outside personnel security channels. The decision authorities listed herein are considered part of the personnel security function.

(3) All personnel security related information that is transmitted via e-mail will be encrypted using the encryption tool in Microsoft Outlook and indicate the message contains personnel security information in the subject line by inserting the following after the subject title "FOR OFFICIAL USE ONLY - Personnel Security Information." Packages transmitted by official mail will be wrapped and mailed in the same manner as required for official use only material.

c. If the selected applicant possesses valid and appropriate investigation, has received a favorable adjudication to that investigation, and no other disqualifying information is known, the PERSEC Specialist will annotate on the DCMA Form 1-1 the applicant's eligibility to occupy the position in question and return it to the AST for further processing.

d. If the review indicates the applicant does not possess appropriate security eligibility to occupy the position for which selected, the PERSEC Specialist will appropriately document the DCMA Form 1-1, forward it back to the AST, and the process documented in paragraph 4A.3. will commence.

4A.3. REQUEST PERSONNEL SECURITY FORMS.

a. The servicing DCMA PERSEC Specialist is responsible for formally notifying and instructing applicants to complete and submit all requisite security forms by an established suspense date.

b. The servicing DCMA PERSEC Specialist will provide the applicant, via e-mail, access to the e-QIP system. Within 2 business days of initially sending the applicant access to the e-QIP system, the servicing DCMA PERSEC Specialist will validate the applicant's receipt of the information, ensure the applicant has obtained access to the e-QIP system, and will answer any questions the applicant might have regarding the completion of forms.

c. If the applicant cannot be contacted within the 2 business day suspense cited above, the PERSEC Specialist will notify the AST and selecting official via email. DCMA Security will make no further effort to contact the applicant until further advised by the AST.

d. Should the applicant not submit the completed forms to DCMA Security within the suspense, the DCMA PERSEC Specialist will submit an email to the applicant requesting prompt completion and submission of the required forms, providing a courtesy copy of the email to both the AST and the selecting official. The AST and/or the selecting official must take immediate action to ensure the completed forms are returned promptly to DCMA Security as no further processing can be accomplished until all forms are received thus causing a significant delay in the hiring process.

4A.4. REVIEW OF FORMS AND GRANTING TEMPORARY ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION OR ASSIGNMENT TO SENSITIVE DUTIES.

a. Upon receipt of the completed security forms via the e-QIP system, a PERSEC Specialist will review the forms to ensure the applicant has provided all required information for processing. The PERSEC Specialist will return incomplete forms to the applicant providing guidance on corrections needed and establishing a completion deadline of 2 calendar days. Should the updated forms not be returned to DCMA Security within the 2-day suspense, the PERSEC Specialist will follow the guidance contained in paragraph 4A.3.d.

b. Once the PERSEC Specialist determines the forms submitted contain all required information, the information submitted is reviewed against the adjudication criteria contained in the National Security Adjudicative Guidelines to determine if the granting of temporary access to classified information or assignment to sensitive duties is in the interest of national security.

c. Upon completion of the forms review, the PERSEC Specialist will submit a waiver

decision package to the Director of Security and CI (all non-DCMAS organizations) or to the Director, DCMAS (DCMAS organizations) who serve as the Agency's approving authorities for granting temporary eligibility for access to classified information. At a minimum, decision packages will contain the following:

- Memorandum of Waiver of Pre-Appointment Investigative Requirements (PIR)
- Justification for recommendation
- All relevant information pertaining to the case including any potential unfavorable information.

d. Upon receipt of a decision package, the approving authority will consider all information contained in the package, using the whole person concept, to render a decision. In accordance with Executive Order (E.O.) 12968 and DoD Personnel Security policy, waivers to the PIR are authorized when determined they are in the interest of national security. The approving authority will resolve any doubts regarding the PIR waiver in the interest of national security.

e. Once a decision is rendered, the approving authority will return the signed package to the servicing PERSEC Specialist for further processing. The PERSEC Specialist will submit an amended DCMA Form 1-1 and a copy of the decision memorandum to the AST for processing. The PERSEC Specialist will also promptly notify the selecting official, via email, of the decision and the process to request an appeal to the decision, if applicable.

f. If temporary eligibility is granted, the servicing PERSEC Specialist will make an expedited adjudication request when submitting forms per EO 12968.

4A.5. APPEAL DENIAL OF TEMPORARY ELIGIBILITY FOR ACCESS OR ASSIGNMENT TO SENSITIVE DUTIES.

a. A selecting official may appeal a decision not to grant temporary eligibility for access to classified information or assignment to sensitive duties if he/she has a critical mission need warranting higher-level consideration. Note that a request for appeal is an exceptional act and should not be a general or automatic practice. Requests for appeal are only considered when the requesting official can clearly articulate a critical mission need that will result in a significant adverse impact to the mission if temporary eligibility is not granted.

b. When the requirements of paragraph 4A.5.a are met and the selecting official or higher-level management determines an appeal is warranted, the selecting official or higher level manager will, within 5 business days of notification of a denial of temporary eligibility decision, notify the DCMA PERSEC Team Supervisor, via e-mail, of the intent to appeal. The notification e-mail will indicate the date when the management official will forward their formal appeal. Failure to meet the above suspense may negatively influence the appeal authority's decision when establishing whether a "critical mission need" truly exists.

c. All requests for appeal will be submitted to the DCMA PERSEC Team Supervisor, via email, for processing.

d. Upon receipt of a request for appeal, the DCMA PERSEC Team Supervisor will forward the appeal package to the Executive Director, HC, who will serve as the Agency's appeal authority. Note that due to the unique security requirements associated with the DCMA Special Programs mission, the decision to grant or deny temporary access to classified information or assignment to sensitive duties rendered by the Executive Director, Special Programs Command, is final. Appeal packages will contain the following:

- Request for Appeal Memorandum submitted by the selecting official
- Waiver Decision Package
- Memorandum of Appeal Decision

e. Upon receipt of a request for appeal, the appeal authority will review the package in its totality and render a decision based on what is in the interest of national security. The entire appeal package is then returned to the DCMA PERSEC Team Supervisor who will notify the requesting management official of the appeal decision and further process the package as required.

4A.6. PROCESS DURING AND AFTER THE APPEAL DECISION.

a. While the Appeal process is taking place, the PERSEC investigative requirements established in DoDM 5200.02 will continue to be processed.

b. If the Appeal is granted, the DCMA PERSEC Team Supervisor will request an expedited investigation. If the Appeal is denied, the investigative requirements established in DoDM 5200.02 will continue to be processed.

c. Any decision to withdraw a tentative offer of employment will not be based on the sole fact that the candidate did not receive temporary eligibility for access or assignment to sensitive duties. Management will ensure all decisions to withdraw offers of employment are processed in accordance with DCMA HC policies/processes.

d. If for any reason an offer of employment is withdrawn by the responsible management official, the AST will notify DCMA Security so the investigative process is halted.

SECTION 5: FAVORABLE ADJUDICATION AND ELIGIBILITY

5.1. ADJUDICATION. The DoD CAF is the sole authority for evaluating personnel security background investigations and making personnel security clearance eligibility determinations for access to classified national security information and/or assignment to sensitive duties for all DCMA Civilian Employees, Military Personnel, and Contractors.

5.2. FAVORABLE DETERMINATIONS.

a. Upon completion of the adjudication process, the DoD CAF will provide DCMA Security notice of an adjudication determination via the DoD JPAS.

b. Upon receipt of notification of a favorable eligibility determination, the responsible PERSEC Specialist shall update the DCMA EPSF and ALEC databases and notify the employee/applicant via email of the determination.

c. If access to classified information is required in the performance of duties, the guidance contained in Section 7, paragraph 7.1. of this Manual shall be followed.

SECTION 6: UNFAVORABLE ELIGIBLITY DETERMINATIONS AND DUE PROCESS

6.1. PRELIMINARY ELIGIBILITY DETERMINATIONS.

a. In the course of the adjudication process when unfavorable or derogatory information is identified that might preclude eligibility for access to national security information or assignment to sensitive duties, the DoD CAF may issue a "Statement of Reasons" (SOR). An SOR is issued to officially notify the applicant/employee of the DoD CAF's preliminary determination to deny or revoke eligibility for access to national security information or assignment to sensitive duties. The DoD CAF submits the SOR to the DCMA Security Office for processing.

b. Processing SORs for Presentation.

(1) Upon receipt of an SOR, the responsible PERSEC Specialist will review the package to ensure it is complete. Additionally, the PERSEC Specialist will update the individual's record in ALEC to reflect a change to clearance eligibility and to indicate a pending reply to the SOR.

(2) The PERSEC Specialist will identify the responsible DCMA Commander/Director (as applicable) and endorse the SOR package to their attention. A copy of the endorsement (not the entire package) will be referred to DCMA HC (Attention: LER) for information/action, as appropriate.

(3) Within 3 calendar days of receipt of the SOR from the DoD CAF, the PERSEC Specialist will mail a complete SOR package to the responsible DCMA Component Head or Commander/Director for presentation to the affected employee. The PERSEC Specialist will ensure the package includes all materials provided by the DoD CAF and guidance on the proper procedures for presenting the SOR. All SOR packages will be double-wrapped to ensure safeguard of the information contained therein.

c. Presenting SORs.

(1) Within 7 calendar days of receipt of an SOR package, the responsible DCMA Commander/Director, Deputy, or other designated management official will present the SOR to the employee concerned following the guidance contained in the SOR package.

(2) If the delivery of the SOR to the employee will be delayed due to the employee's non-availability (i.e., sick or annual leave, temporary duty, etc.), the management official responsible for presentation of the SOR will notify the PERSEC Specialist of the situation and provide a projected delivery date. The PERSEC Specialist will provide additional guidance and ensure the situation is documented in the ALEC.

(3) For applicants who have not yet started duty with DCMA, SORs are presented/ delivered by the PERSEC Specialist. Every effort will be made to ensure such SORs are presented within 7 calendar days of initial receipt.

(4) When presenting the SOR, the management official presenting it will ensure the employee/applicant signs and dates the SOR, "Acknowledgement Receipt and Statement of Intention" at the time of presentation. The employee/applicant must indicate on the SOR receipt their intent to respond in writing or not to respond to the SOR. The acknowledgement receipt will be promptly returned to the servicing PERSEC Specialist for forwarding to the respective CAF. Acknowledgment receipts are due to the CAF within 10 calendar days of the employee/applicant signing the receipt.

d. Post SOR Presentation Actions.

(1) Requests for Extension.

(a) When an employee/applicant elects to provide a written response to the SOR, the response must be submitted to the DoD CAF within 30 calendar days of receipt of the SOR unless an extension is granted, in writing, by proper authority.

(b) Individuals requiring an extension to the initial SOR response timeline (30 calendar days), will submit a written request (e-mail is sufficient), with justification, to the DCMA PERSEC PM for processing and consideration. The request for extension must be received not later than 5 calendar days prior to the established due date for the written response to the SOR. The DCMA Director of Security and CI (or designated representative) is authorized to grant an extension up to an additional 30 calendar days from the original suspense date. The DoD CAF is the sole authority for approving any subsequent request for extension.

(c) Individuals requesting an extension from a DoD CAF will submit a written request for extension, with justification, to the servicing PERSEC Specialist and it must arrive not later than 5 calendar days prior to the expiration of the DCMA granted extension. The serving PERSEC Specialist will submit the request for extension to the DCMA Director of Security and CI for endorsement and forwarding to the DoD CAF for consideration.

(d) All extension decisions rendered by the DoD CAF are routed through the DCMA Security Office to the individual. Upon receipt of a decision notice, the PERSEC Specialist will forward the DoD CAF's decision letter to the employee with guidance that the employee will sign and return the acknowledgement receipt to the PERSEC Specialist. The DoD CAF decision letter will stipulate if the employee has been granted an additional extension and establish a new suspense date (if an extension is granted) for submission of written responses to the SOR.

(2) Suspension of Access or Assignment to Sensitive Duties.

(a) Upon receipt of an SOR, the responsible DCMA Component Head or primary Commander/Director will determine whether to suspend the employee's access to classified information and/or assignment to sensitive duties based upon the level of security risk to the DCMA mission and/or national security. Prior to any decision to enact a suspension, coordination with the OGC and HC Directorate LER Office is required.

(b) When a decision is made to suspend an employee's access or assignment to sensitive duties, the responsible DCMA Component Head or Commander/ Director will provide a copy of the action/determination to the servicing PERSEC Specialist for processing.

(3) Submitting Responses to SORs.

(a) Individuals submitting written responses to SORs will submit the response to the servicing PERSEC Specialist by the established suspense date. The PERSEC Specialist will forward the written response to the PERSEC PM for endorsement and submission to the DoD CAF.

(b) If a written response is not received within 30 calendar days of receipt of the SOR or a request for extension has not been granted by the proper authority, the applicant/employee will be considered to have waived the right to respond. In such cases, the PERSEC PM will provide such notice to the DoD CAF for a final eligibility determination.

(c) Upon receipt of the employee's written response to the SOR, the DoD CAF will carefully weigh all requisite information and render a final eligibility determination nation.

6.2. FINAL ELIGIBILITY DETERMINATIONS.

a. After careful consideration of all available materials and application of the DoD Adjudicative Standards, the DoD CAF will render a final eligibility determination. Notifications of final determinations are submitted to DCMA Security via the DoD JPAS.

b. Favorable Determinations. When the DoD CAF renders a favorable eligibility determination in response to an SOR, the servicing PERSEC Specialist will follow the procedures outlined in paragraph 5.2. of this Manual.

c. Unfavorable Determination.

(1) When the DoD CAF renders an unfavorable determination following the issuance of an SOR, it will document its final eligibility determination in a Letter of Revocation (LOR)/Letter of Denial (LOD) and submit it to the affected individual through DCMA Security and command channels. The DoD CAF LOR/LOD, with instructions, will be processed, presented, and acknowledged in the same manner as outlined in paragraphs 6.1.a(1) and 6.1.a(2).

(2) Upon receipt of the LOR/LOD, the responsible DCMA Component Head or primary Commander/Director will immediately suspend the employee's access to classified information and reassign the individual to non-sensitive duties. Commanders/Directors are encouraged to coordinate with the HC Directorate LER Office for assistance and additional guidance.

(3) The DCMA PERSEC PM will provide a copy of the DoD CAF's final decision letter to the HC Directorate LER Office for situational awareness and/or action.

6.3. DUE PROCESS.

a. In accordance with the guidance outlined in DoDM 5200.02, individuals issued a final determination by the DoD CAF to deny or revoke access to national security information or eligibility for assignment to sensitive positions will be afforded the opportunity to appeal the DoD CAF's decision. Individuals may appeal LORs/LODs through written reply to the serving CAB or request a personal appearance before a Defense Office of Hearing and Appeals (DOHA) Administrative Judge.

(1) Individuals electing to submit a written appeal to the CAB must ensure the appeal is received by the CAB within 30 calendar days of signing the LOR/LOD acknowledgement receipt.

(2) When an individual elects a personal appearance before a DOHA Administrative Judge, representatives of the DOHA will contact the individual directly and coordinate a scheduled court date. At the conclusion of the individual's appearance, the DOHA will forward a written transcript of the proceedings and a recommendation to the DoD CAB for consideration.

b. The CAB will consider all information in the appeal and will render a final eligibility determination decision.

c. Favorable Appeal Determination.

(1) The CAB will notify DCMA Security by official correspondence of any decision to overturn the DoD CAF's final revocation/denial decision and coordinate with the serving DoD CAF to document the appeal decision in the DoD JPAS.

(2) The servicing PERSEC Specialist shall follow the procedures outlined in paragraphs 5.2.b through 5.2.c of this Manual and provide written notice of the CAB's decision to the responsible DCMA Componen Head or Commander/Director.

d. Unfavorable Appeal Determination.

(1) A CAB decision to sustain a DoD CAF's final denial/revocation decision is documented in a CAB letter that is routed through the DCMA Security Office and addressed to the individual concerned. The CAB's denial decision concludes the employee's administrative due process rights.

(2) Upon receipt of a CAB's letter indicating it has sustained a DoD CAFs final denial/revocation decision, the following actions will be completed:

(a) The servicing PERSEC Specialist will notify the responsible DCMA Component Head or Commander/Director of the CAB's decision.

(b) When the individual concerned is a current DCMA employee occupying a position designated as sensitive, the responsible DCMA Component Head or

Commander/Director will coordinate a personnel action with the HC Directorate LER Office to remove the individual from the sensitive position. No request for personnel action will be initiated to appoint or reassign such an employee to any position designated as sensitive. If the action concerns an applicant, no request for personnel action will be generated to appoint the applicant to any position within DCMA which is designated as sensitive.

(c) The HC Directorate LER Office will provide the servicing PERSEC Specialist a copy of the notice of the removal or reassignment action.

(d) The PERSEC Specialist will update the applicable records in the JPAS, ALEC, and EPSF databases.

6.4. RECONSIDERATION OF FINAL UNFAVORABLE DETERMINATIONS. All requests for reconsideration of a final unfavorable determination will comply with DoDM 5200.02, paragraph 10.6.

SECTION 7: ACCESS

7.1. GRANTING ACCESS TO CLASSIFIED INFORMATION.

a. The granting of clearance eligibility by a DoD CAF in and of itself does not authorize any individual access to classified national security information. In addition to clearance eligibility, individuals requiring access to classified national security information for the accomplishment of the DoD mission must also be granted access to that information. The granting of access is a managerial decision based on an approved security eligibility determination and a valid mission requirement. Before any individual is granted access to classified national security information, all of the following will be completed and validated:

(1) The individual concerned must have a valid security clearance eligibility determination for the level of information for which access is being considered.

(2) The individual concerned must possess a valid mission-related need to know.

(3) The individual must complete an SF-312, "Classified Information Nondisclosure Agreement (NDA)"

b. The following steps will be used to process an individual for access to classified information.

(1) Step 1. The responsible management official will carefully review the duties of the individual in question to determine if the assigned duties require access to classified information and the specific information required.

(2) Step 2. Once the above is verified, the management official will complete, sign, and submit a DCMA Form 1-2 to the servicing PERSEC Specialist. The DCMA Form 1-2 will indicate the level of classified information required to support that duties assigned.

(3) Step 3. Upon receipt of a DCMA Form 1-2, the responsible PERSEC Specialist will validate clearance eligibility via the DoD JPAS.

(a) When the appropriate clearance eligibility exists, request the employee complete an SF-312. An electronic copy of the SF-312 Briefing Booklet will be provided to the employee for review prior to executing the SF-312. Execution of the SF-312 will be witnessed and signed by a DCMA government employee in the appropriate section of the form. The PERSEC Specialist will sign the acceptance block of the SF-312 and ensure it is filed in the Official Personnel File as a long term document.

(b) When the appropriate clearance elgibilty does not exist, the action will be returned to the management official advising the individual does not possess the requisite clearance eligibility.

(c) SF-312s executed on Military personnel will be forwarded to the respective Military Service with a copy filed in the DCMA EPSF database. In accordance with EO 13526, a legally enforceable copy of the SF-312 must be retained for 50 years from date of execution.

(d) Document the level of access to classified information authorized and the date the SF-312 was executed on the DCMA Form 1-2, in ALEC and in the DoD JPAS. A copy of the completed DCMA Form 1-2 will be retained in the employee's EPSF.

(e) Provide email notice to the requesting manager advising that the employee's access to classified information has been granted. If clearance eligibility cannot be validated or any of the above required actions are not accomplished, the PERSEC Specialist will notify the requesting management official that the employee is denied access until the requirement of this section are met.

7.2. INTERIM ACCESS.

a. Interim access to classified national security information may be granted when an individual's official duties necessitate access prior to completion of the personnel security background investigation and adjudication process.

b. DoDM 5200.02, Section 7, paragraph 7.16., establishes the criteria for granting interim eligibility access to classified information. DoDD 5105.64, enclosure 2, provides DCMA the authority to grant interim access. Access to SAPs will be governed by applicable DoD and SAPCO policy.

c. In accordance with DoDD 5105.64, the responsible DCMA Component Head or primary CMO Commander/Director may suspend an employee's interim access authorization at any time if notified by the DCMA PERSEC staff that unfavorable information has developed in the course of the background investigation or adjudication. Prior to rendering any decision to suspend interim access, DCMA Component Heads or Commanders/Directors will coordinate the action with the OGC and HC Directorate LER Office.

7.3. ONE-TIME ACCESS.

a. Circumstances may arise where an urgent operational or contractual need exists for cleared DoD personnel to have one-time or short duration access to classified information at a higher level than that authorized by the existing security eligibility determination.

b. DoDM 5200.02, Section 8, establishes the criteria by which one-time access may be granted. The cited DoD guidance will be followed by DCMA without deviation.

7.4. TEMPORARY ACCESS.

a. Under unique and limited circumstances an individual may require a temporary upgrade in access to accomplish a specific mission or requirement. For example, a military member assigned to DCMA is authorized to access classified information at the Secret level; however,

the military member is scheduled to attend a military professional development course that requires Top Secret access. Under such a situation, a temporary upgrade in access may be granted.

b. Qualifications for a temporary upgrade in access include:

- Security clearance eligibility at the higher level must already exist
- The responsible manager must validate the requirement for the temporary upgrade

c. If the qualifications listed above exist, the responsible manager will submit a DCMA Form 1-2 to the servicing DCMA PERSEC staff requesting a temporary upgrade. The mission or imminent requirement justifying the upgrade will be stated in Section II of the DCMA Form 1-2.

d. Upon receipt of a request for upgrade, the servicing PERSEC Specialist will validate the clearance eligibility via the DoD JPAS and process the DCMA Form 1-2 in accordance with subparagraph 7.1(b)(3).

e. Listed below are the approving officials by level for temporary access upgrades:

- Confidential, Secret and Top Secret: DCMA Component Heads or primary CMO Commander/ Directors
- Sensitive Compartment Information (SCI): Executive Director, Special Programs Command

7.5. LIMITED ACCESS AUTHORIZATION (LAA). The guidance contained in DoDM 5200.02, Section 6, will be followed when considering any LAA. Questions regarding LAAs will be forwarded to DCMA PERSEC staff.

7.6. PRESIDENTIAL SUPPORT PROGRAM.

a. Commanders and Directors with missions supporting the DoD Presidential Support Program will ensure only the most suitable and qualified individuals are selected for and retained in Presidential Support duties to ensure optimum Presidential security and support.

b. Commanders and Directors will use the guidance contained in DoDD 5210.55, "Department of Defense Presidential Support Program," and DoDI 5210.87, "Selection of DoD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities (PSAs)," when selecting personnel to perform Presidential Support Program duties.

c. When considering personnel for nomination to the Presidential Support Program, Commanders/Directors will ensure employees nominated are assigned to a position with a critical-sensitive designation and the employee possesses Top Secret security clearance eligibility.

d. Presidential Support Program Nomination Procedures.

(1) Once all requirements outlined in paragraph 7.6.a. through c are met and verified, the responsible Commander/Director will submit a DCMA Form 1-2 to the DCMA PERSEC Office requesting validation of position sensitivity and clearance eligibility, along with a nomination letter for Presidential support duties assignment.

(2) Nomination packages for active duty military personnel must also include a medical certification completed by a competent medical authority attesting that there are no physical or mental disorders noted in the service member's record that would adversely affect the individual's reliability and judgment.

(3) Upon receipt of nominations for the Presidential support assignment, the servicing PERSEC Specialist will validate completeness of the package.

(4) Once validation is complete, the PERSEC Specialist will contact the OPM to request a copy of the current completed and adjudicated PSI.

(5) Upon receipt of the PSI, the PERSEC Specialist will assemble the entire nomination package and forward it to the DCMA PERSEC PM for review and submission to the Executive Secretary, Office of the Secretary of Defense (OSD), for consideration. Nomination packages not meeting all requirements will be returned to the respective organization for action.

(6) Upon approval of a nomination, the Executive Secretary, OSD, submits a letter to DCMA Security documenting the official approval and date. The PERSEC PM will endorse the approval letter and forward it to the responsible Commander/Director and the responsible PERSEC Specialist. The PERSEC Specialist will ensure nomination approvals are documented in the DCMA ALEC and EPSF.

e. Presidential Assignment Termination. Commanders/Director will promptly notify the DCMA PERSEC Staff, in writing (email is sufficient), when personnel assigned Presidential duties are terminated from the program. The notification will include the date Presidential participation was terminated.

7.7. SPECIAL ACCESS PROGRAM (SAP).

a. A SAP is any program designed to control access, distribution, and protection of particularly sensitive information pursuant to EO 13526 and prior Executive Orders.

b. Within DCMA, access to all SAP is governed by the unique requirements established by the DCMAS, the applicable DoD SAPCO, or the information owner. Refer questions regarding SAP access to the DCMAS Program Security Office (PSO).

7.8. ACCESS TO NORTH ATLANTIC TREATY ORGANIZATION (NATO) CLASSIFIED INFORMATION.

a. The requirements associated with accessing NATO classified information are contained in DoDM 5200.02 and DoDM 5200.01, Volume 1.

b. Commanders/Directors with a valid mission-related requirement for accessing NATO classified information will verify all the requirements in the cited policy are met. Once verified, a DCMA Form 1-2 will be submitted to the DCMA PERSEC Staff requesting access to NATO classified information. The specific level of NATO access must be identified.

c. Upon receipt of the request, the responsible PERSEC Specialist will ensure the individual possesses a valid, equivalent U.S. clearance. Once verified, the PERSEC Specialist will provide the requisite NATO briefing and update the individual's status in the DoD JPAS.

7.9. ACCESS TERMINATION DEBRIEFING.

a. Upon termination of employment, departure from DCMA, administrative withdrawal of a security clearance, a management determination that access to classified is no longer required, or there is a suspension of access to classified information, the responsible Manager/Supervisor will submit a completed DCMA Form 1-2 to the DCMA PERSEC staff reporting the termination.

b. Upon notification, the responsible PERSEC Specialist will ensure the individual concerned (military or civilian) completes the required debriefings on the DCMA Form 12.15.2-6, "Security Termination Statement," and SF-312 and sign both forms. Should the individual refuse to complete the debriefings or sign the forms, the PERSEC Specialist will verbally debrief the individual and record the refusal on both forms.

SECTION 8: CONTINUOUS EVALUATION PROGRAM

8.1. GENERAL. In accordance with DoDM 5200.02, Section 11, all individuals with clearance eligibility for access to classified information or assignment to sensitive duties are subject to continuous evaluation (CE). CE involves the uninterrupted assessment of a person for retention of security eligibility or continuing assignment to sensitive duties and is necessary to evaluate an individual's post-adjudication activities (the period of time after clearance is adjudicated and before a Periodic Reinvestigation (PR) is due). An effective CE program relies on all DCMA personnel reporting questionable or unfavorable information that may be relevant to a security eligibility determination.

8.2. PERIODIC REINVESTIGATION (PR).

a. In accordance with DoDM 5200.02, Section 3, DCMA personnel in national security positions designated as Special Sensitive, Critical Sensitive, and Noncritical Sensitive are subject to a periodic reinvestigation on a recurring basis. Specific reinvestigation requirements are detailed in the following paragraphs.

b. Special Sensitive and Critical Sensitive Positions. Civilian and military personnel occupying positions designated as Special Sensitive or Critical Sensitive are subject to a PR on a 5-year recurring bases. The types of PRs required of Special Sensitive and Critical Sensitive positions are the Phased Periodic Reinvestigation (PPR) and the SSBI-PR or T5 Reinvestigation (T5R) equivalent.

(1) Phased Periodic Reinvestigation (PPR). In accordance with the Under Secretary of Defense Memorandum, a PPR is submitted on personnel occupying Special Sensitive or Critical Sensitive positions when information submitted on the SF-86 does not reveal a security concern.

(2) SSBI-PR. The SSBI-PR is submitted on employees in all cases where the PPR is not warranted.

c. Non-Critical Sensitive Positions. All personnel assigned to positions designated as Non-Critical Sensitive are subject to a PR on a 5-year recurring basis. The NACLC or T3 Reinvestigation (T3R) equivalent is the sole investigation submitted for these positions.

d. Non-Sensitive Positions. The DoD policy does not require a recurring reinvestigation of personnel assigned to non-sensitive positions.

e. PR Submission Procedures.

(1) The PERSEC staff will review the DCMA ALEC database on a quarterly basis to identify individuals requiring a PR. Reinvestigation requirements will be based on the date of the last completed investigation. PRs will be submitted no earlier than 3 months before the respective anniversary date of the the last completed invesgation. Personnel for whom PR requests are initiated will have at least 12 months remaining in-service or employment with DCMA.

(2) The PERSEC staff will notify and direct individuals requiring reinvestigation to complete the requisite reinvestigation forms via the e-QIP system. Upon return of forms, the PERSEC Specialist will review the submitted forms for completeness and accuracy, will submit completed forms to OPM for investigation, and will document the action in the ALEC database.

(3) An individual's access to classified information and/or assignment to sensitive duties will not be suspended or downgraded solely because the PR is not completed within the required timeframe unless the employee refuses to submit the personnel security questionnaire and there are no valid extenuating circumstances that preclude submission.

(a) Responsible supervisors/managers will support and enforce PR requirements. The servicing PERSEC Specialist will notify the appropriate manager/supervisor of all cases where the employee has failed to submit the required reinvestigation forms by the established suspense date. In such situations, the supervisor/manager will take immediate action to ensure the employee completes and submits the required forms.

(b) After involvement by management, should an employee refuse to complete the requisite personnel security investigation forms, the servicing PERSEC Specialist will contact the responsible DCMA Component Head or CMO Commander/Director and advise them to suspend access to classified information and/or assignment to sensitive duties until the requirement is met. The responsible Commander/Director will forward a copy of the suspension letter to the servicing PERSEC Specialist for processing and provide notice to the HC Directorate LER Office.

8.3. REPORTING REQUIREMENTS.

a. All DCMA personnel granted with eligibility for access to classified information or assigned to sensitive duties must report any security issues that fall under the 13 categories of adjudicative criteria identified in SEAD 4.

b. Management Responsibilities.

(1) Commanders/Directors and other management and supervisory personnel will continuously assess their employees having sensitive duties for reliability and trustworthiness. The intent of this assessment is to determine if an employee’s continued security clearance eligibility is consistent with the interests of national security.

(2) Any question concerning an employee's continued reliability and trustworthiness should be immediately discussed with the DCMA PERSEC staff. Based on the totality of the circumstances, the responsible Commander/Director will make a determination as to whether an employee's assignment to sensitive duties and/or access to classified information should be temporarily suspended pending any required investigation and/or adjudication of unfavorable information. When making such determinations, the interests of national security, the DCMA mission, and the safety of employees will be the first concern.

c. Individual Responsibilities.

(1) The ultimate responsibility for maintaining eligibility for access to classified information and/or assignment to sensitive duties rests with the individual. Employees are required to notify their respective supervisors/managers and/or the DCMA Security Office to seek assistance regarding any incident or situation that could potentially affect their continued eligibility for access to classified information and/or assignment to sensitive duties.

(2) Co-workers have an equal obligation to advise their supervisors or the DCMA Security Office when they become aware of information with potentially serious security significance regarding someone with access to classified information or employed in a sensitive position.

d. Reportable Behaviors. This paragraph contains a list of behaviors that must be reported to management or to the DCMA Security Office if observed in individuals with access to national security information or assigned to sensitive duties. (This list is not all inclusive.)

(1) Alcohol Abuse. Arrests, treatments, counseling, and failure to follow any court ordered treatment.

(2) Criminal Conduct. All arrests, knowledge of a criminal act by another cleared individual, attempted coercion or blackmail.

(3) Drug Involvement. Illegal use of narcotics, prescription drugs or controlled substances, drug rehabilitation treatment, etc.

(4) Financial Concerns. Excessive indebtedness, liens, judgments, bankruptcies, home foreclosures, garnishments, misuse of Government Travel Card or unexplained affluence.

(5) Foreign Travel (Business or Personal). Foreign travel must be reported in advance and follow-up with the servicing Security Office is required upon return.

(6) Foreign Influence/Contact. Any attempt by a foreign national to solicit sensitive/classified information or any other contact that is regarded as suspicious, close and continuing contact with a foreign national, dual citizenship, foreign monetary interests, etc.

(7) Misuse of Information Technology Systems or Computers. Unauthorized entry into an Automated Information System, password misuse, etc.

(8) Personal Conduct. Conduct involving questionable judgment, untrustworthiness, unreliability or unwillingness to comply with rules and regulations, or unwilling to cooperate with security clearance processing.

(9) Psychological/Mental Health. An opinion by a credentialed mental health professional of a condition or treatment that may indicate a defect in judgment, reliability, or stability; failure to follow appropriate medical advice relating to treatment; apparent high risk, irresponsible, aggressive, anti-social or emotional unstable behavior.

(10) Security Incidents. Security violations or infractions.

e. Security Office Responsibilities. Upon receipt of information meeting the reporting requirements of the CE Program, the servicing PERSEC Specialist will submit all supporting documents to the DCMA PERSEC PM for review and submission to the DoD CAF in accordance with the procedures outlined in DoDM 5200.02, Section 9, paragraph 9.2.(2), and document the pending action in the individual's record within the ALEC database.

8.4. PERSONNEL SECURITY ACTIONS.

a. Derogatory information developed that may be characterized as within the meaning and/or intent of the criteria set forth in DoDM 5200.02, Section 11, and this Manual will be promptly referred by the responsible management official to DCMA Security.

b. In accordance with DoDD 5105.64 and based on the totality of the circumstance and information known, DCMA Component Heads or Commanders/Directors will determine whether to suspend an individual's access to classified information or reassign the individual to non-sensitive duties pending a review of the unfavorable information and a final eligibility determination by the servicing DoD CAF. Such determinations will be based on what is in the best interest of national security. Prior to rendering any decision to enact a suspension, DCMA Component Heads or Commanders/Directors will coordinate the action with the OGC and HC Directorate LER Office.

c. Should the responsible management official decide to temporarily suspend access or remove an individual from sensitive duties, that official will following the proedures outlined in DoDM 5200.02, Section 9, paragraphs 9.4(d) and 9.4(e) and notify the employee in writing of the decision and the reasons for rendering the decision.

d. The official directing the suspension of access will forward a copy of the notice to the DCMA Security Office for processing within the same calendar day.

e. Upon receipt of the suspension of access memorandum, the servicing PERSEC Specialist will forward information on the action to the servicing DoD CAF via the DoD JPAS within the same calendar day it is received as outlined in DoDM 5200.02, Section 9, paragraph 9.4(c). If the action involves a DCMA contractor, the information will be reported to the Defense Security Service via JPAS. In addition, the PERSEC Specialist will notify the responsible Contracting Officer Representative.

f. Once initiated, the suspension of access will remain in effect until the DoD CAF issues a favorable determination regarding clearance eligibility.

SECTION 9: RECORDS MANAGEMENT

9.1. SAFEGUARDING PERSEC RECORDS AND INFORMATION.

a. Access. Due to the personal nature and sensitivity of PERSEC-related information, PERSEC records, files, correspondence, and other related information and materials will be strictly controlled to those security and management officials that clearly demonstrate a valid PERSEC related mission requirement for access. Prior to the disclosure of any PERSEC-related information, PERSEC Specialists will verify the mission related need-to-know of the person to whom information is being disclosed. Additionally, only that information specifically required for the mission objective will be disclosed. Any question regarding the disclosure of PERSEC information will be referred to the PERSEC PM for clarification.

b. Safeguarding Procedures. The following safeguards will apply to all PERSEC correspondence, investigative reports, personnel security folders (PSF), and other related files/documents.

(1) Marking. All PERSEC correspondence will bear the "FOR OFFICIAL USE ONLY" marking at the top and bottom of each page and prominently display the Privacy Act Warning.

(2) Packaging. All PERSEC correspondence (background investigation reports, PSFs, and other related files/documents) being mailed via the U.S. Postal Service will be double-wrapped using opaque Government envelopes. The inside envelope containing the correspondence will be marked front and back "FOR OFFICIAL USE ONLY."

(3) Addressing. The inner and outer packaging envelopes, discussed in paragraph 9.1.b(2), will be addressed specifically to the intended recipient.

(4) Transmittal. To the greatest extent possible, PERSEC correspondence will be transmitted via encrypted email using the encryption tool in Microsoft Outlook. The subject line of the email message will be marked "FOR OFFICIAL USE ONLY – Personnel Security Information" after the subject title. PERSEC packages transmitted by official mail via the U.S. Postal Service will be wrapped and addressed as outlined in paragraphs 9.1.b(2) and 9.1.b(3).

(5) Storage. PERSEC Specialists will ensure PERSEC files and unclassified PERSEC Reports of Investigation (ROIs) are stored in key or cipher-locked cabinets or rooms where supplemental access controls allow only authorized access to the area where the files are stored. Supplemental controls may consist of an office area where access is controlled by the PERSEC Specialist.

9.2. PERSONNEL SECURITY FOLDER (PSF) CONSTRUCT.

a. PERSEC Specialists will create and retain PSFs for all Agency employees. PERSEC forms, records of adjudication, and related correspondence will be retained in the individual's PSF.

b. PSFs will be marked "FOR OFFICIAL USE ONLY" and bear Privacy Act Warnings. PSFs will include the following documents and in the order of precedence listed:

(1) Most recent completed SF-86, SF-85P, or SF-85.

(2) DCMA Form 12.15.1-2.

(3) DCMA Form 12.15.1-1.

(4) SF-312.

(5) DCMA Form 12.15.2-6 and all special access debriefing certificates.

(6) Copies of applicable correspondence and record copies thereof relating to the processing of personnel security actions including:

- Pre-appointment security checks
- Investigative tracers and resubmissions
- Exceptions to investigative standards for appointment and/or clearance for access
- Correspondence forwarding personnel security reports of investigation or relating to personnel security determinations

(7) Special debriefings for unauthorized access, foreign contact or travel, and record copies of correspondence relating to duty and travel restrictions, security duty assignments, special security authorizations (original classification authority, courier authority, authorization to conduct classified meetings, etc.), and notifications of clearance status.

9.3. RECORDS DISPOSITION.

a. Reports of Investigation (ROI).

(1) ROIs requested and received by PERSEC Specialists from an Investigative Service Provider (ISP) may be retained only for the period necessary to complete the purpose for which it was originally requested. Such reports are considered to be the property of the ISP and are not authorized for retention in DCMA PERSEC files.

(2) The PERSEC Specialist will ensure ROIs are destroyed when the record is no longer required or authorized. ROIs will be destroyed using a DCMA approved crosscut shredder or burning procedure.

b. Other PERSEC Records. Non-ROI PERSEC records will be retained for a period of 2 years from the date of the employee's departure from the Agency. At the conclusion of the 2-year period, all records will be destroyed in the same manner as described in paragraph 9.3.a(2).

SECTION 10: ASSESSMENT AND REPORTING

10.1. ASSESSMENT.

a. The objective of the DCMA PERSEC Assessment Program is to evaluate program effectiveness and to measure compliance with established standards. The PERSEC Program is assessed though Program Reviews conducted by the PERSEC PM.

b. The PERSEC PM will conduct Program Reviews at least annually. Assessments are conducted using the DCMA PERSEC Program Review Benchmarks, which were derived from the requirements outlined in DoD and DCMA PERSEC policies.

c. The PERSEC PM will document the results of all Program Reviews in a formal report. Reports will document findings, concerns, issues, and best practices as well as a comprehensive recommended remedy to correct the issue identified. Copies of Program Review Reports are distributed to the Director of Security and CI and to the Director, DCMAS for reviews involving DCMAS organizations. Upon receipt of a Program Review Report, the responsible management official will take the requisite action to correct findings. The PERSEC PM will track findings until the issues identified have been resolved.

10.2. REPORTING REQUIREMENTS.

a. Fiscal Year (FY) PSIs Projection Report. The PERSEC PM and the DCMAS PSO will, not later than March 30 annually, identify and document the projected PSI requirements for the upcoming FY using the PSI Projection Report Template located on the resource page for this Manual. The PERSEC PM will consolidate the information into a single Agency level report, which will be submitted to the Office of the Deputy Under Secretary of Defense for Intelligence and Security.

b. Pre-appointment Waiver of Investigative Requirements Report. The PERSEC PM and the DCMAS PSO will jointly develop an annual report detailing the number of approved and disapproved Pre-appointment Investigation Waivers issued over the previous FY. This report is due annually not later than October 31. A sample format of this report is located on the resource page for this Manual.

c. Presidential Support Program Quarterly Report. In accordance with DoDI 5210.87, the PERSEC PM will submit a quarterly PSP Report to the OSD Presidential Support Program Office. This report will document DCMA personnel participating in the PSP by Presidential Support Activity location and include any additions, deletions, or other changes in status. Reports are due within 15 calendar days of the end of the quarter. Reports will be marked "FOR OFFICIAL USE ONLY" and will be assigned Report Control Symbol (DD-SD(Q)934).

SECTION 11: TRAINING

11.1. PERSONNEL SECURITY SPECIALISTS.

a. The PERSEC PM will ensure the Agency's PERSEC staff are adequately trained to perform their duties and responsibilities.

b. The Defense Security Service's Center for Development of Security Excellence (CDSE) will serve as the primary training provider for PERSEC training.

c. Listed below are the minimum and mandatory training requirements for PERSEC Specialists assigned to the DCMA Personnel Security mission. These training courses are available on-line through the CDSE and will be completed prior to the assumption of duties.

- Introduction to DoD Personnel Security Adjudication (PS001.18)
- Introduction to National Security Adjudications (PS170.16)
- Introduction to Personnel Security (PS113.16)
- JPAS/Joint Clearance and Access Verification System (JCAVS) Virtual Training for Security Professionals (PS183.16)
- OPSEC Fundamentals (IO-OP101.16)
- Introduction to Information Security (IF011.16)
- Personally Identifiable Information (PII) (DS-IF101.06)

11.2. SECURITY REPRESENTATIVES. PERSEC Specialists will provide all designated Security Representatives for which they support a Basic PERSEC Program Orientation within 5 business days of assignment to duties. This orientation is designed to ensure new Security Representatives are knowledgeable of and can perform the PERSEC portion of their assigned duties.

11.3. AWARENESS TRAINING.

a. Initial Security Orientation.

(1) Within 60 calendar days of assignment, all new employees to DCMA will undergo a comprehensive, integrated initial security orientation, provided by a DCMA Security Specialist, that addresses the personnel security training requirements established in DoD policy.

(2) Managers and supervisors will ensure employee availability to complete the initial security orientation within the established timeline.

b. Annual Refresher Training. Annual PERSEC training requirements are integrated into the annual Information Security Training Program. This annual training is accomplished through the use of a Computer Based Training (CBT) Program that alerts individual employees to their training requirement, provides the training, and then tracks training completion using a centralized database. The DCMA Information Security Team tracks and ensures training completion.

GLOSSARY

G.1. DEFINITIONS.

All definitions relative to this Manual are contained in DoDM 5200.02, Glossary, Part II - Definitions.

GLOSSARY

G.2. ACRONYMS.

ADP	automated data processing
ALEC	Automated Listing of Eligibility and Clearances
AST	Army Servicing Team
AT	Antiterrorism
CAB	Clearance Appeal Board
CAF	consolidated adjudications facility
CDSE	Center for Development of Security Excellence
CE	continuous evaluation
CFR	Code of Federal Regulations
CI	counterintelligence
CMO	Contract Management Office
CVS	Central Verification System
DCMA FORM 1-1	DCMA Form 12.15.1-1, "Pre-appointment Security Form"
DCMA FORM 1-2	DCMA Form 12.15.1-2, "Determination of Need for Clearance/Position Sensitivity Change"
DCMA FORM 2-6	DCMA Form 12.15.2-6, "Security Termination Statement"
DCMAS	DCMA Special Programs Command
DoDD	DoD Directive
DoDI	DoD Instruction
DOHA	Defense Office of Hearing and Appeals
DODM	DoD Manual
E.O.	Executive Order
EPSF	Electronic Personnel Security File
e-QIP	Electronic Questionnaires for Investigations Processing
FY	fiscal year
HC	Human Capital
ISP	investigative service provider
IT	information technology
JPAS	Joint Personnel Adjudication System
LAA	limited access authorization
LER	labor and employee relations
LOD	letter of denial
LOR	letter of revocation
NACLC	National Agency Check with Law and Credit

NACI	National Agency Check and Inquiries
NATO	North Atlantic Treaty Organization
OGC	Office of General Counsel
OPM	Office of Personnel Management
OSD	Office of Secretary of Defense
PERSEC	personnel security
PIR	pre-appointment investigative requirements
PM	program manager
PR	periodic reinvestigation
PPR	Phased Periodic Reinvestigation
PSF	Personnel Security Folders
PSI	personnel security investigation
PSO	Program Security Office
PSP	Personnel Security Program
RPA	request for personnel action
ROI	report of investigation
SAP	special access program
SAPCO	Special Access Program Central Office
SEAD	Security Executive Agent Directive
SF Form 85	Questionnaire for Non-Sensitive Positions
SF Form 86	Questionnaire for National Security Position
SF Form 312	Classified Information Nondisclosure Agreement
SOR	statement of reasons
SSBI	Single Scope Background Investigation
T1	Tier One
T3	Tier Three
T5	Tier Five

REFERENCES

Code of Federal Regulation, Title 5, Part 1400. "National Security Positions", as amended
DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)", January 10, 2013
DoD Directive 5210.55, "Department of Defense Presidential Support Program", December 15, 1998
DoD Instruction 5200.02, "DoD Personnel Security Program," April 9, 1999 *March 21, 2014*
DoD Instruction 5210.87, "Selection of DoD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities (PSAs)", November 30, 1998
DoD Manual 5200.02, "Procedures for the DoD Personnel Security Program", April 3, 2017.
DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012
DoD Regulation, "Department of Defense Privacy Program", May 14, 2007
Executive Order 10450, "Security Requirements for Government Employment", April 27, 1953, as amended
Executive Order 12968, "Access to Classified Information", August 2, 1995
Executive Order 13526, "Classified National Security Information", January 5, 2010
Security Executive Agent Directive 4, "National Security Adjudicative Guidelines," June 12, 2017
Under Secretary of Defense Memorandum, "Single Scope Background Investigation- Periodic Reinvestigations (SSBI-PR)", March 5, 2005