



NYARNG Personnel Security

Standard Operating Procedure

New York Army National Guard J-2

JFHQ-NY-J2

9 August 2019

This page intentionally left blank

Table of Contents

| | |
|--------------------------------------------------------------------------------|-----------|
| CHAPTER 1 – OVERVIEW | 1 |
| 1.1 – PURPOSE..... | 1 |
| 1.2 – REFERENCES | 1 |
| 1.3 – TERMS, ACRONYMS AND ABBREVIATIONS..... | 1 |
| CHAPTER 2 – RESPONSIBILITIES | 1 |
| 2.1 – STATE J2 PERSONNEL SECURITY (PERSEC) OFFICE..... | 1 |
| 2.2 – STATE J2 SPECIAL SECURITY OFFICE (SSO) | 2 |
| 2.3 – DIVISION SECURITY MANAGEMENT OFFICE (SMO) | 2 |
| 2.4 – BRIGADE SMO | 2 |
| 2.5 – BATTALION SMO | 2-3 |
| 2.6 – UNIT FULL-TIME STAFF, COMMANDER, FIRST SERGEANT AND LEADERS..... | 3 |
| 2.7 – INDIVIDUAL | 3 |
| CHAPTER 3 – JPAS ADMINISTRATIVE PROCESSING | 3 |
| 3.1 – IN-PROCESSING PERSONNEL IN JPAS | 3 |
| 3.2 – OUT-PROCESSING PERSONNEL IN JPAS | 3-4 |
| CHAPTER 4 – SECURITY CLEARANCE PROCEDURES | 4 |
| 4.1 – DETERMINING SECURITY CLEARANCE REQUIREMENTS..... | 4-5 |
| 4.2 – DEFINING THE TYPE OF INVESTIGATION REQUEST..... | 6-8 |
| 4.3 – ADMINISTRATIVE REQUIREMENTS FOR INVESTIGATION. | 8-10 |
| 4.4 – INVESTIGATION REQUEST RESUBMISSION DUE TO TERMINATED E-QIP | 10-11 |
| CHAPTER 5 – TYPES OF ADJUDICATION | 11 |
| 5.1 – OVERVIEW | 11 |
| 5.2 – ADJUDICATION AND ACCESS TYPES EXPLAINED..... | 11-15 |
| CHAPTER 6 – REQUESTING INTERIM ELIGIBILITY | 16 |
| 6.1 – OVERVIEW | 16 |
| 6.2 – GENERAL INTERIM GUIDANCE..... | 16 |
| CHAPTER 7 – REQUESTING AN EXPEDITED INVESTIGATION OR ADJUDICATION | 16 |
| 7.1 – OVERVIEW | 16-17 |
| 7.2 – ADMINISTRATIVE REQUIREMENTS FOR AN EXPEDITE REQUEST..... | 17 |
| CHAPTER 8 – INDOCTRINATING AND DEBRIEFING ACCESS | 17 |
| 8.1 – OVERVIEW | 17-18 |
| 8.2 – ACCESS TYPES | 18 |
| 8.3 – INDOCTRINATING ACCESS | 18-19 |

| | |
|------------------------------------------------------------------------------------------------|-----------|
| 8.4 – DEBRIEFING ACCESS | 19 |
| CHAPTER 9 – SECURITY CLEARANCE VERIFICATION | 19 |
| 9.1 – OVERVIEW | 19 |
| 9.2 – VERIFICATION PROCESS | 19-20 |
| CHAPTER 10 – DOD CONSOLIDATED ADJUDICATIONS FACILITY (DOD CAF) CORRESPONDENCE | 20 |
| 10.1 – CORRESPONDENCE OVERVIEW | 20 |
| 10.2 – CORRESPONDENCE TYPES..... | 21-22 |
| 10.3 – RESPONSE PROCEDURES | 22-23 |
| 10.4 – SOLDIERS PENDING ETS/SEPARATION | 23 |
| 10.5 – APPEAL PROCESS | 23-24 |
| CHAPTER 11 – RECONSIDERATION PROCESS..... | 24 |
| 11.1 – OVERVIEW | 24-25 |
| 11.2 – RECONSIDERATION PROCEDURE | 25 |
| CHAPTER 12 – INCIDENT REPORTING | 25 |
| 12.1 – OVERVIEW | 25-26 |
| 12.2 – INCIDENT REPORTING PROCESS..... | 26 |
| 12.3 – INCIDENT REPORTING REQUIREMENTS..... | 26-27 |
| 12.4 – ETS AND SEPARATION..... | 27 |
| CHAPTER 13 – CONTINUOUS EVALUATION (CE) | 27 |
| 13.1 – OVERVIEW | 27 |
| 13.2 – CE PROCESSING | 27-28 |
| CHAPTER 14 – REQUESTS FOR ACTION (RFA) | 28 |
| 14.1 – RFA OVERVIEW..... | 28 |
| 14.2 – RFA TYPES..... | 28-29 |
| CHAPTER 15 – FOREIGN TRAVEL | 29 |
| 15.1 – OVERVIEW | 29 |
| 15.2 – FOREIGN TRAVEL POLICY..... | 29-30 |
| 15.3 – FOREIGN TRAVEL REPORTING PROCESS..... | 30 |
| CHAPTER 16 – MAINTAINING A SECURITY CLEARANCE ACCESS ROSTER (SCAR)..... | 30 |
| 16.1 – OVERVIEW | 30 |
| 16.2 – SCAR MAINTENANCE | 30 |

| | |
|---------------------------------------------------------------------------------------------------|--------------|
| CHAPTER 17 – SYSTEMS AND AUTHORITIES | 31 |
| 17.1 – SYSTEMS WITHIN PERSEC..... | 31 |
| 17.2 – AUTHORITIES..... | 31 |
| CHAPTER 18 – REQUESTING JPAS ACCESS | 32 |
| 18.1 – STEPS FOR REQUESTING ACCESS | 32 |
| 18.2 – JPAS Rules..... | 32 |
| CHAPTER 19 – PERSONNEL SECURITY REQUIREMENTS FOR SOLDIER READINESS PROCESS (SRP) | 32 |
| 19.1 – OVERVIEW | 32 |
| 19.2 – J2 PERSEC RESPONSIBILITIES FOR SRP..... | 33 |
| CHAPTER 20 – VISIT REQUESTS | 33 |
| 20.1 – OVERVIEW..... | 33 |
| 20.2 – VISIT REQUEST PROCESS | 33 |
| APPENDIX A – References..... | 35 |
| APPENDIX B – Terms and Acronyms..... | 36-38 |

Chapter 1 – Overview

1.1 – Purpose

a. The purpose of this Standard Operating Procedure (SOP) is to establish policy and clear insight into how the NYARNG manages personnel security from the individual level up to the State Personnel Security Office (JFHQ-J2-PERSEC). This SOP applies to all battalion, brigade, division, TDA and State personnel security managers performing the duties described in this SOP.

b. Department of the Army established the personnel security program in order to ensure compliance with all Department of Defense (DoD) directives pertaining to the security of classified information and the governing of those who are, or wish to be, authorized to view and maintain such information.

1.2 – References

All external references can be found in Appendix A of this SOP.

1.3 – Terms, Acronyms and Abbreviations

All terms, acronyms and abbreviations can be found in Appendix B of this SOP.

Chapter 2 – Responsibilities

2.1 – State J2 Personnel Security (PERSEC) Office

a. The J2 PERSEC Office shall remain responsible for the following:

1. Input all requests for investigation using the PSIR (military and civilian/contractor) once received from subordinate echelons.
 2. Review and action all Joint Personnel Adjudications System (JPAS) user account requests and manage JPAS access.
 3. Review and recommend on all exceptions to policy in terms of personnel security for reasons of promotion, appointment, MOS reclassification, etc.
 4. Distribute all Department of Defense Consolidated Adjudications Facility (DoD CAF) correspondence to the subordinate levels as well as forward appropriate documentation back to the DoD CAF.
 5. Process all reports of derogatory information and incident reports.
 6. Ensure all Soldiers are processed into and out of JPAS upon accession and separation as the owning relationship.
 7. Develop, maintain, review and distribute policy as it pertains to personnel security.
 8. Process visit requests in JPAS.
 10. Approve electronic system access authorization requests (DD 2875/DMNA 2875).
 11. JPAS administrative processing.
 12. Train, assist and advise all subordinate commands.
 13. Suspend access per commander's recommendation, as appropriate.
- b. These responsibilities may be delegated as appropriate.

2.2 – State J2 Special Security Office (SSO)

- a. The J2 SSO shall remain responsible for the following:
 - 1. Maintain security clearance caveats to include the scheduling of read-ons.
 - 2. Partnering with the J2 PERSEC Office to develop training focused on subordinate PERSEC managers.
 - 3. JPAS administrative processing.
 - 4. Train, assist and advise all subordinate commands.
- b. These responsibilities may be delegated as the J2 deems appropriate.

2.3 – Division/Troop Command Security Management Office (SMO)

- a. The division/troop command SMO shall remain responsible for the following:
 - 1. Ensuring the appointment of security managers throughout the subordinate commands. There may be 2 security managers per battalion and 2 per brigade. Of the 2, 1 may be a traditional M-Day Soldier. Exceptions may be made due to mobilization, exercises, etc.
 - 2. Maintaining security clearance standards within the Headquarters and Headquarters Battalion, 42nd Infantry Division/ 53rd Troop Command. The division/troop command will also retain the responsibility to report derogatory information pertaining to Soldiers within their command.
 - 3. Process, build and complete security clearance verification statements upon request.
 - 4. Develop policy applying to subordinate commands based on this SOP and references listed in Appendix A of this SOP.
- b. These responsibilities may be delegated as appropriate.

2.4 – Brigade SMO

- a. The brigade SMO shall remain responsible for the following:
 - 1. Ensuring the appointment of security managers throughout the subordinate commands.
 - 2. The brigade will also retain the responsibility to report derogatory information pertaining to Soldiers within their command.
 - 3. Maintaining security clearance standards within brigade headquarters.
 - 4. Process, build and complete security clearance verification statements upon request.
 - 5. Develop policy applying to subordinate commands based on this SOP, references listed in Appendix A of this SOP and policy developed by higher headquarters, to include a flow of work in reference to personnel security investigation requests (PSIR) and other security requests for action.
- b. These responsibilities may be delegated as appropriate.

2.5 – Battalion SMO

- a. The battalion SMO shall remain responsible for the following:
 - 1. Maintaining security clearance standards throughout the battalion.
 - 2. The battalion will also retain the responsibility to report derogatory information pertaining to Soldiers within their command.
 - 3. Process, build and complete security clearance verification statements upon request.

4. Develop policy applying to subordinate units based on this SOP, references listed in Appendix A of this SOP and policy developed by higher headquarters, to include a flow of work in reference to PSIR's and other security requests for action.

b. These responsibilities may not be further delegated except in the instance of identifying those who are required to be investigated/reinvestigated.

2.6 – Unit Full-Time Staff, Commander, First Sergeant and Leaders

a. The unit will remain responsible for the following:

1. Ensuring their Soldiers are compliant with all directives from higher headquarters to include PSIR's, completion of their electronic questionnaires and security requirements.

2. The unit will also retain the responsibility to report derogatory information pertaining to Soldiers within their command.

3. Units are responsible for development and maintenance of their security clearance access report (SCAR) with the assistance of their higher headquarters.

b. It is expected that the units take initiative to contact their battalion SMO's for personnel security training.

2.7 – Individual

a. Individuals are responsible for timely submission of all personnel security documentation to include documents requested by their unit & higher headquarters as well as responses to DoD CAF correspondence.

b. It is the individual's responsibility to keep the unit informed of any matter that may preclude them from meeting any established timelines.

c. The individual also maintains the obligation to report any developed derogatory information regarding themselves or other personnel within in the NYARNG IAW Chapter 12 of this SOP.

Chapter 3 – JPAS Administrative Processing

3.1 – In-processing Personnel in JPAS

a. Proper in-processing of personnel within JPAS is a pertinent piece of maintaining SCAR's, establishing a workload for need of investigation and reinvestigation as well as quick reference for inspections and training requirements.

b. In-processing requires verification of true membership in the NYARNG as well as the reported unit of assignment.

c. A servicing relationship in JPAS pulls the referenced Soldier into the unit's hierarchy. As a result, the security manager will be able to compile reports from JPAS that are as accurate as the servicing relationships.

3.2 – Out-processing Personnel in JPAS

a. When a Soldier leaves a unit, they should be released from their previous command and control so that the new unit may take a servicing relationship, if applicable. This also applies to other States and other components/branches of service.

b. Out-processing steps are as follows:

1. Verify true departure from the current unit of assignment.

2. Ensure all debrief procedures are followed. See chapter 8 for further debriefing instructions.
- c. Upon out-processing of personnel, they will no longer appear on reports generated from JPAS.

Chapter 4 – Security Clearance Procedures

4.1 – Determining Security Clearance Requirements

a. Duty Position (DPOS)

1. All personnel in DPOS's coded as requiring security clearance eligibility will be investigated commensurably. To find position coding, refer to the applicable unit manning roster (UMR), the report on Personnel Readiness Indicators, Metrics, and Evaluations (PRIME) or Standard Installation/Division Personnel System (SIDPERS).

- a. Use the SIDPERS Data Reference Manual to interpret SIDPERS codes in the system itself, located on the UMR.

- b. If a Soldier is found ineligible to hold the clearance corresponding with the DPOS, they may not be retained in that DPOS.

2. DPOS coding is strict. Security clearance requirements for particular para/lines are non-waiverable.

b. Military Occupational Specialty (MOS)

1. Utilize DA PAM 611-21 MOS Smartbook located at <https://login.milsuite.mil/?goto=https%3A%2F%2Fwww.milsuite.mil%3A443%2Fbook%2Fgroup%2Fsmartbookdapam611-21> for MOS specifications. This regulation is updated frequently and should be referred to when questioning whether or not any Soldier requires a security clearance.

2. Ensure to always reference the Smartbook and UMR. Although a DPOS may not be coded as requiring a security clearance, the MOS associated with that DPOS may and vice versa.

3. Be cognizant of Additional Skill Identifiers (ASI) and Skill Qualification Identifiers (SQI). For example, although an 11B (infantryman) does not require a security clearance, an 11B with an ASI of B4 (sniper) does.

c. DoD Civilians

1. All State and Federal technicians require, at a minimum, a suitability for federal employment background check. A more in depth background investigation may be necessary as stated by their Position Description (PD).

2. If a civilian's PD does not state that they require a clearance, they are not authorized to be investigated on behalf of the NYARNG for eligibility beyond that of suitability. See Homeland Security Policy Directive – 12 (HSPD-12) for more information. See Chapter 4.3 of this SOP for civilian clearance investigation guidance.

d. Contractors employed within the sponsorships of the NYARNG

1. All contractors assigned to the NYARNG require a suitability for federal employment background check. No additional background check is authorized for contractors. Should anything more in depth be required for their duties, their contracting agency is responsible for the investigation.

2. See HSPD-12 in Appendix A of this SOP for more information. See chapter 5 of this SOP for contractor investigation submission guidance.

e. General Officers

1. All Colonels in the NYARNG being considered for Brigadier General and beyond require security clearance eligibility at the Top Secret (TS)/Sensitive Compartmented Information (SCI) level.

2. In anticipation of this requirement, any O-6 may be submitted for an investigation required by the stated clearance level.

f. Commissioned Officers

1. All commissioned officers are required to obtain and maintain, at a minimum, secret eligibility throughout their commission.

2. All S-6 signal branch battalion and brigade level officers are expected to obtain and maintain TS/SCI eligibility.

3. Always refer to DA PAM 611-21 for further security clearance requirements pertaining to commissioned officers and particular Areas of Concentration (AOC).

g. Warrant Officers

1. All warrant officers are required to obtain and maintain, at a minimum, secret eligibility throughout their commission.

2. Warrant officers holding or volunteering to attend 255A, 255N or 255S are required to obtain and maintain TS/SCI eligibility.

3. Always refer to DA PAM 611-21 for further security clearance requirements pertaining to warrant officers and particular AOC's.

h. By Exception

1. Soldiers may be investigated at the Tier 3 (T3) level for the purpose of TOC access, handling of classified equipment in vehicles, etc, even if their MOS or DPOS do not require such a level.

2. Soldiers cannot be investigated for TS/SCI eligibility simply for ease of access. However, they may be investigated for the following exceptions:

(a). Reclassification to a military intelligence (35 AOC) MOS. The Soldier must already be in the MI DPOS upon requesting investigation.

(b). Additional duty appointment as a COMSEC custodian. The additional duty appointment memorandum must accompany the investigation requested.

(c). Soldiers assigned as intelligence sergeants on the UMR but not in a 35 series DPOS.

(d). As needed for mobilization. Supporting documentation must accompany the investigation request. For example, a letter from the commander-in-place as well as the commander of the Soldier being mobilized.

i. Deployed Personnel

1. In most cases, deployed personnel are unable to be investigated. This is due to the fact that if questions should arise or a personal interview is required (Tier 5 (T5)), PSI-CoE nor OPM will be able to contact the subject.

2. Deployed personnel that require investigation or reinvestigation in the case that their eligibility expires during mobilization, should not request to be investigated while deployed. Instead, new investigations should be accomplished prior to mobilizations and reinvestigations should be accomplished post-mobilization. Expired investigations due to mobilization should be considered valid up until 90 days after mobilization concludes, during in which the subject should be submitted for reinvestigation.

4.2 – Defining the Type of Investigation Request

a. Initial investigation

1. Initial investigation nomenclature and definitions. An investigation is only considered initial if there is no evidence of the sought-after investigation in JPAS or there has been a greater than 2 year break in federal service since the particular investigation type has closed. For reinvestigations, see chapter 4.2b of this SOP.

(a). T1

(1). T1 investigations replaced National Agency Checks (NAC) and National Agency Checks with Inquiries (NACI). T1 investigations are only used for suitability for federal employment checks for federal and State civilians as well as contractors. Uniformed personnel are not authorized to be investigated at this level.

(2). T1 investigations are non-clearance producing investigations. This type is only used for common access card issuance and RCAS account creation.

(b). T2

(1). T2 investigations replaced the moderate risk background investigation (MBI). This investigation type is used for federal and State civilians being utilized in positions coded as *moderate risk*, such as a SHARP representative.

(2). T2 investigations are potentially clearance producing investigations. This type is not authorized to be used for uniformed personnel.

(c). T3

(1). T3 investigations replaced the National Agency Check with Law and Credit (NACLC) and Advanced National Agency Check with Inquiries (ANACI) investigations. This investigation type is used for ALL personnel in DPOS's requiring secret eligibility.

(2). T3 is the minimum investigation type authorized for uniformed personnel.

(d). T4

(1). T4 investigations replaced the civilian Background Investigation (BI). T4 investigations are top secret clearance producing investigations.

(2). T4 investigations are not used in the NYARNG nor are they authorized for uniformed personnel.

(e). T5

(1). T5 investigations replaced the Single Scope Background Investigation (SSBI). This investigation type is a top secret clearance, as well as caveat (i.e. SCI) producing investigation.

(2). All uniformed personnel in DPOS's or with MOS's requiring top secret or top secret with SCI clearances must be investigated at this level.

2. No evidence of previous investigation

(a). When checking JPAS for any previous investigations, if there is no evidence that the Soldier or Civilian has been investigated at the commensurate level, their investigation should be considered initial. Ensure to expand their investigations and adjudications outside of the personnel summary.

(b). If the subject has been investigated at the requested level previously and a new investigation is submitted, it will be rejected by the Personnel Security Investigations Center of Excellence (PSI-CoE).

3. Non-federal break in service

(a). If the subject has had greater than a 2 year break in federal service the investigation is considered null and an initial investigation should be opened. For example – a Soldier was a 31B (MP) on active duty from February 2011 until March 2014. In June 2016, they entered service in the NYARNG. Because they had a civilian break in service from March 2014 until May 2016, their investigation is no longer valid.

(b). These situations should be looked at like the nulled investigation never existed. Investigate these subjects using an initial request.

b. Reinvestigations

1. T1 – Reinvestigations are not authorized at the T1 level. If there has been a greater than 2 year break in service, consider it an initial investigation.

2. T2 – Reinvestigations for T2 level investigations are required every 10 years. Reinvestigation dates should be considered from the day that the previous investigation closed. Only personnel serving in Sexual Assault Response Coordinator and Sexual Harassment/Assault Response and Prevention positions are authorized to be reinvestigated.

3. T3 – Reinvestigations for this level are required every 10 years. Reinvestigation dates should be considered from the day that the previous investigation closed. Requests for reinvestigation cannot be submitted to the J2 PERSEC office any earlier than 30 prior to the current investigation expiring. As long as the subject has had a commensurate investigation for this level (previously NACLC, ANACI or downgraded SSBI ONLY) and there has not been a greater than 2 year break in service, a follow-on investigation will always be considered a reinvestigation, regardless of the lapse of the previous investigation.

4. T5 – Reinvestigations for this level are required every 5 years to maintain TS or TS/SCI eligibility. Reinvestigation dates should be considered from the day that the previous investigation closed. T5 investigations outside of their 5 year window should be considered to have been downgraded for secret eligibility and are appropriate at that level for an additional 5 years. As long as the subject has had a commensurate investigation for this level (previously SSBI, PPR, PR or SBPR ONLY) and there has not been a greater than 2 year break in service, a follow-on investigation will always be considered a reinvestigation, regardless of the lapse of the previous investigation.

(a). Due to the backlog of investigations at Office of Personnel Management (OPM) T5 investigations will be extended to 6 years until further notice.

5. Continued access.

(a). Continued access is defined as the lapsing period between when a subject's previous investigation closed and when a current, in progress investigation opens.

(b). A subject is granted continued access when a reinvestigation has been submitted for the subject, they have completed all administrative requirements to include their e-QIP and OPM has officially opened the investigation. This only applies to those who have previously had an investigation completed and was adjudicated for the level in which they are now being investigated. Note that personnel fitting this description must not have had a two year break in federal service that affected their investigation.

(c). For example – SGT John Doe's current secret clearance investigation closed May 2006. In April 2016, his security manager submitted the appropriate paperwork to have him reinvestigated. Two weeks later, he completed his e-QIP and his investigation was officially opened. By the definition of continued access, his clearance did not lapse and he continues to have access at the secret level due to him doing everything within his power and regulatory guidance to comply with security clearance standards.

c. Fingerprints

1. In JPAS, fingerprint checks are identified as Special Agreement Checks (SAC).
2. Fingerprints are required for any NEW investigation.
3. Additionally, fingerprints are required for any investigation under the new Tier (T) naming convention if evidence of fingerprints within the last 120 days is not present in JPAS.
4. If it is identified that the subject being investigated requires fingerprints, they may be accomplished (preferably) at any Army National Guard recruiting station or armory that has a recruiter present. The fingerprints will then be electronically submitted to OPM and will be present in JPAS within a 24-48 hour period.

(a). The alternate method for submitting fingerprints is via the fingerprint card or SF 87. These may be accomplished at any law enforcement or FBI post.

(b). Once complete, the fingerprint card must be mailed by certified mail to:
Department of the Army
Joint Force Headquarters – New York
Attn: J2 PERSEC
330 Old Niskayuna Rd.
Latham, NY 12110

(c). Upon mailing the paper copy fingerprints, J2 PERSEC must be contacted via e-mail with the following information:

- (1). Tracking number for the package.
- (2). Location in which the package was mailed from.

(d). Note that paper fingerprint cards should only be utilized in **extenuating** circumstances.

4.3 – Administrative Requirements for Investigation.

These requirements stand whether the investigation is an initial one or a reinvestigation.

a. T1 investigation

1. Civilian

(a). Completed, in its entirety to include two phone numbers and two email addresses, MN 1998-E.

(b). Appropriate citizenship documentation. Accepted forms of citizenship documentation include, and are limited to:

(1). Birth certificate (complete with a seal from the State in which it was issued in and the signature of the registrar or other authorized personnel).

- (2). United States issued passport
- (3). Report of birth abroad (FS 240)
- (4). Certificate of citizenship
- (5). Certificate of naturalization
- (6). Certificate of birth (DS 1350)
- (7). Certificate of birth (FS 545)

(c). Completed and wet-signed copy of an OF 306.

(d). A Completed copy of the request for background investigation. All sections should be completed prior to submission with the exception of the ARNG DISPOSITION section. The CERTIFICATION section is only to be signed by the J2 representative O-5 or higher.

2. Contractor

(a). Completed, in its entirety to include two phone numbers and two email addresses, MN 1998-E.

(b). Appropriate citizenship documentation. Accepted forms of citizenship documentation include, and are limited to:

(1). Birth certificate (complete with a seal from the State in which it was issued in and the signature of the registrar or other authorized personnel).

- (2). United States issued passport
- (3). Report of birth abroad (FS 240)
- (4). Certificate of citizenship
- (5). Certificate of naturalization
- (6). Certificate of birth (DS 1350)
- (7). Certificate of birth (FS 545)

(c). Completed and wet-signed copy of an OF 306.

(d). A Completed copy of the request for background investigation. All sections should be completed prior to submission with the exception of the ARNG DISPOSITION section, to include the CERTIFICATION section. The CERTIFICATION section must be completed by the first O5 or GS-13 in the contractor's chain of command.

b. T2 investigation

1. Civilian

(a). Completed, in its entirety to include two phone numbers and two email addresses, MN 1998-E.

(b). Appropriate citizenship documentation. Accepted forms of citizenship documentation include, and are limited to:

(1). Birth certificate (complete with a seal from the State in which it was issued in and the signature of the registrar or other authorized personnel).

- (2). United States issued passport
- (3). Report of birth abroad (FS 240)
- (4). Certificate of citizenship
- (5). Certificate of naturalization
- (6). Certificate of birth (DS 1350)
- (7). Certificate of birth (FS 545)

(c). Completed and wet-signed copy of an OF 306.

(d). A Completed copy of the request for background investigation. All sections should be completed prior to submission with the exception of the ARNG DISPOSITION section. The CERTIFICATION section is only to be signed by the J2 representative O-5 or higher.

(e). A copy of the subject's PD stating the need for security clearance eligibility.

c. T3 investigation

1. Military

(a). Completed, in its entirety to include two phone numbers and two email addresses, MN 1998-E.

(b). Appropriate citizenship documentation. Accepted forms of citizenship documentation include, and are limited to:

(1). Birth certificate (complete with a seal from the State in which it was issued in and the signature of the registrar or other authorized personnel).

- (2). United States issued passport
- (3). Report of birth abroad (FS 240)
- (4). Certificate of citizenship
- (5). Certificate of naturalization
- (6). Certificate of birth (DS 1350)
- (7). Certificate of birth (FS 545)

2. Civilian

(a). Completed, in its entirety to include two phone numbers and two email addresses, MN 1998-E.

(b). Appropriate citizenship documentation. Accepted forms of citizenship documentation include their birth certificate (complete with a seal from the State in which it was issued in and the signature of the registrar or other authorized personnel), United States issued passport, report of birth abroad (FS 240), certificate of citizenship, certificate of naturalization, certificate of birth (DS 1350) or certificate of birth (FS 545). No other forms of citizenship documentation will be accepted.

(c). A copy of the subject's resume.

(d). Completed and wet-signed copy of an OF 306.

(e). (State Civilians Only) A Completed copy of the request for background investigation. All sections should be completed prior to submission with the exception of the ARNG DISPOSITION section. The CERTIFICATION section is only to be signed by the J2 representative O-5 or higher.

(f). A copy of the subject's position description (PD) stating the requirement for a secret clearance. The request will NOT be processed without such.

d. T5 investigation

1. Completed, in its entirety to include two phone numbers and two email addresses, MN 1998-E.

(a). Appropriate citizenship documentation. Accepted forms of citizenship documentation include, and are limited to:

(1). Birth certificate (complete with a seal from the State in which it was issued in and the signature of the registrar or other authorized personnel).

(2). United States issued passport

(3). Report of birth abroad (FS 240)

(4). Certificate of citizenship

(5). Certificate of naturalization

(6). Certificate of birth (DS 1350)

(7). Certificate of birth (FS 545)

(b). Additional Investigation requirements

1. Regardless of the investigation type or clearance eligibility required, all applicants are required to have at least one year remaining in their contract, RSO or prior to their ETS/MRD.

2. Personnel not meeting this requirement will not be investigated until they extend or, in the case of officers approaching their MRD, are waived to remain in service.

3. QRB'd/SRB'd personnel who are only retained for one year are not authorized to be investigated unless there is greater than one year before they appear before another board.

4.4 – Investigation Request Resubmission Due to Terminated e-QIP

a. If the applicant fails to complete their e-QIP in the allotted timeline, they fail to make appropriate corrections as identified by PSI-CoE in the timeline or they fail to have fingerprints completed in the timeline, their investigation will be terminated and the J2 PERSEC office, unit security manager and subject will be notified.

b. A subsequent investigation request may be submitted, in its entirety, with command assurance that it will be completed the second time.

c. Should the subject fail to complete e-QIP a second time for any of the reasons stated in 4.4a, a third request may be submitted, in its entirety, with a counseling statement and command assurance that the subject will complete e-QIP the third time around.

d. Additional submissions of investigation requests beyond the third time will be at the discretion of the NYARNG-J2.

Chapter 5 – Types of Adjudication

5.1 – Overview

a. There is a vast difference between investigation, adjudication and access. Investigations gather necessary information to make a determination whether or not someone is suitable for security clearance eligibility. Adjudication actually makes that determination by having a trained personnel security technician evaluate a subject using the whole person concept reviewing their investigation. Access physically grants someone permission to handle information at their adjudicated level, based on their need-to-know.

b. Adjudication can determine if someone is eligible for a clearance, deny them such a privilege or some other administrative action.

5.2 – Adjudication and Access Types Explained

a. Sensitive Compartmented Information (SCI) Caveat

1. SCI is one of the many caveats that can be made available to a subject being investigated for top secret eligibility. This caveat is required of all military intelligence AOC Soldiers as well as many other MOS's and DPOS's. However, just because someone is investigated for a top secret clearance does not mean they were also investigated for SCI.

2. SCI is governed by the Director of Central Intelligence and subsequently the directive DCID 6-4. All personnel being given such eligibility should review the stated directive and become familiar with the burden they will carry.

3. All SCI actions are coordinated through JFHQ-J2 SSO to include being read-on and appropriate debriefing. Please direct any questions regarding SCI to the mentioned directorate.

4. Interim SCI eligibility can be granted by DoD CAF for reasons of mobilization, training attendance or promotion. The following steps should be followed:

(a). A current investigation for the purpose of SCI eligibility must be open.

(b). The Soldier and BN/BDE/DIV security manager must complete the SCI questionnaire.

(c). A memorandum for record signed by the first O5 in the Soldier's chain of command must be submitted outlining the justification for need of interim eligibility, as well as the Soldier's personal identifiers.

(d). Submit the SCI questionnaire and memorandum to the J2 PERSEC office for action.

b. Top Secret (TS)

1. TS eligibility is rarely given without the SCI caveat however, there are instances that subjects are investigated only at the TS level because of mission requirements. TS is a prerequisite of SCI but not the other way around.

2. Adjudication for TS eligibility happens in the tiered system. The T5 spans the last 10 years of a subject's life, since the closing of their last TS granting investigation or since their 18th birthday, whichever is shortest.

3. TS access can be granted by the J2 PERSEC office. The following steps should be followed:

(a). The Commander should determine that there is a genuine need-to-know.

(b). The Soldier must read and sign an SF 312 Non-Disclosure Agreement (NDA).

(c). The security manager must sign the NDA as a witness.
(d). Forward the completed NDA to J2 PERSEC so the State security manager may sign as the acceptor. Access will then be granted.

(e). The completed and actioned form will be returned to the unit security manager for permanent filing in the Soldier's iPerms record.

4. Upon termination of need-to-know/access level or the Soldier moves on from the unit that initiated granting them access, the second portion of the original NDA needs to be read and signed by the Soldier. This is called the Non-Disclosure Statement (SF-312). Once completed, forward it once again to the State security manager for action. The State security manager will debrief the Soldier's access and return to the unit security manager for filing in the Soldier's iPerms record.

5. Interim TS eligibility

(a). Interim TS eligibility can only be granted by DoD CAF. The following procedures should be adhered to:

(1). A current TS producing investigation must be open and the NAC on the investigation completed or a valid NACLIC or T3 completed and adjudicated within the last 5 years of request.

(2). The first O5 in the Soldier's chain of command must write a memorandum for record to the J2 PERSEC office outlining the justification for interim eligibility. The memorandum must also contain the Soldier's personal identifiers.

c. Secret eligibility

1. A favorable NACLIC or T3 is the standard for all uniformed personnel and is a requirement of most MOS's, DPOS's, additional duties, TOC access or systems access.

2. Secret eligibility, and access, are the minimum requirement for SIPRNET access.

3. The J2 PERSEC office may grant secret access using the following procedure:

(a). The Commander should determine that there is a genuine need-to-know.

(b). The Soldier must read and sign an SF 312 Non-Disclosure Agreement (NDA).

(c). The unit security manager must sign the NDA as a witness.

(d). Forward the completed NDA to J2 PERSEC so they State security manager may sign as the acceptor. Access will then be granted.

(e). The completed and actioned form will be filed in the Soldier's iPerms record by the soldiers unit.

4. Upon termination of need-to-know or the Soldier moves on from the unit that initiated granting them access, the second portion of the original NDA needs to be read and signed by the Soldier. This is called the Non-Disclosure Statement. Once completed, forward it once again to the State security manager for action. The State security manager will debrief the Soldier's access and return to the security manager for filing in the Soldier's iPerms record.

5. Interim secret eligibility

(a). Interim secret eligibility may be granted by the J2 PERSEC office following these procedures:

(1). A current secret producing investigation must be open.

(2). A validated SF86 from PSI-CoE must be present, as well as a local records check by the J2 PERSEC office.

(3). The first O5 in the Soldier's chain of command must write a memorandum for record to the J2 PERSEC office outlining the justification for interim eligibility. The memorandum must also contain the Soldier's personal identifiers.

(b). Interim eligibility is not required if the subject falls under continued access.

d. No Determination Made (NDM)

1. NDM may be granted for one or several reasons. This should be considered a final, not favorable or unfavorable adjudication that may be requested to be upgraded to an eligibility commensurate with the investigation that was performed.

(a). This eligibility may have been given due to the Soldier not requiring a clearance at the time of investigation, the soldier is a non- U.S. citizen, or other reason. As a result, the DoD CAF did not review the investigation files for eligibility and issued NDM.

(1). In order to upgrade this type of determination to a level commensurate with their investigation:

(a). Verify that the scope of the investigation is still valid. Secret producing = 10 years, TS/SCI producing = 6 years.

(b). Submit an e-mail to the J2 PERSEC office requesting upgrade of the Soldier's NDM eligibility. Include the Soldier's investigation information found in JPAS.

(2). If the Soldier's secret producing investigation is still in scope (not expired) but greater than 5 years old, the Soldier must sign new release of information pages from the SF 86. This will authorize the DoD CAF to pull a new credit report and attempt to locate any new legal information on the Soldier. The signature pages include the following:

(a). Authorization for Release of Information

(b). Authorization for Release of Medical Information

(c). Fair Credit Reporting Disclosure and Authorization

(3). This eligibility may also have been issued due to the presence of derogatory information in the investigation but the Soldier did not have a need for clearance eligibility at the time of investigation. For instance, if an 11B was investigated for secret eligibility but they were issued a Statement of Reasons that they failed to respond to, the DoD CAF would have issued NDM.

e. Pending Reply to Statement of Reasons (SOR)

1. Pending reply to SOR is an eligibility placeholder within JPAS. This means that the DoD CAF has sent an SOR or Request for Information (RFI) through channels to the Soldier.

2. Before responding to the SOR or RFI, the Soldier will first need to submit the SOR/RFI acknowledgement receipt contained in the packet. This is due within 10 days of receipt of the documents.

3. Failure to respond, or failure to respond completely, to the SOR or RFI will ultimately result in either an issuance of Denied eligibility, Revoked eligibility or No Determination Made (if eligibility is not actually required).

4. Instructions to respond to correspondence can be found listed in the appropriate letter from the CAF.

(a). Every item in the SOR/RFI should be addressed in detail. The response should be in letter form and come from the subject in which they were directed. For example; if the DoD CAF asked for more information about 7 specific delinquent accounts on the Soldier's credit report, the response from the Soldier should have 7 different paragraphs or bullets detailing the situations surrounding the delinquencies.

(b). Also contained in the response should be supporting documentation. For instance, if the Soldier has set up a payment plan with 4 different creditors, then the Soldier should attach 4 different letters from those creditors stating the terms of the payment plan. Also considered as supporting documentation are things such as receipts, ARD discharge certificates, bankruptcy documents, etc.

5. Complete response to the RFI/SOR is due within 30 days of receipt. Extension of these timelines may be requested in writing to the J2 PERSEC office.

6. If the Soldier has responded to the RFI/SOR in complete detail and all security concerns are mitigated, their eligibility will revert to the clearance that is commensurate with their investigation.

f. Loss of Jurisdiction eligibility

1. Loss of jurisdiction typically happens when the Soldier comes from another branch of service and joins the NYARNG. They would have been originally investigated by another branch of service and require the NYARNG to take ownership of them in JPAS. As long as ownership was taken in a timely manner, their eligibility would have remained as it was in their previous service (as long as there wasn't a greater than 2 year break in service). However, if the security managers within the Soldier's chain of command fail to take ownership or a servicing relationship, loss of jurisdiction will be issued.

2. To correct this loss of jurisdiction:

(a). Verify that there was not a greater than 2 year break in federal service.

(b). Submit an e-mail to the J2 PERSEC office containing the Soldier's investigation information and personal identifying information. The J2 PERSEC office will submit a request to the DoD CAF for reconsideration.

g. Eligibility Administratively Withdrawn

1. Much like loss of jurisdiction, eligibility administratively withdrawn is a product of the security managers within the Soldier's chain of command not taking proper ownership or a servicing relationship of the Soldier in JPAS. The difference is that the Soldier typically was never in a different branch of service but perhaps a different component such as the transition from Active Duty to the National Guard.

2. To correct eligibility administratively withdrawn:

(a). Verify that there was not a greater than 2 year break in federal service.

(b). Submit an e-mail to the J2 PERSEC office containing the Soldier's investigation information and personal identifying information. The J2 PERSEC office will submit a request to the DoD CAF for reconsideration.

h. Eligibility Denied

1. An eligibility of denied is issued when a subject is in a DPOS or MOS that requires particular eligibility, they are investigated for such but the investigating authority discovers derogatory information during the investigation.

2. The investigating and adjudicating authorities will never issue an eligibility of denied prior to due process. They will always afford an opportunity to the subject to respond and rectify the discovered derogatory information. Even if the response is inadequate and their eligibility is still denied, the subject still has an opportunity to appeal the decision.

(a). Appeals should be accomplished IAW the documentation that is sent from the adjudicating authority (typically the DoD CAF) to the subject.

(b). Once an appeal is initiated, the J2 PERSEC office is taken completely out of the process and cannot obtain any information about the case. The Personnel Security Appeals Board (PSAB) will communicate directly with the subject.

3. If the subject chooses not to appeal, the denied adjudication becomes final. If PSAB determines enough mitigating information is not present, the denied adjudication becomes final. In either situation, the subject may have their case reconsidered once per year, every year, beginning with 365 days after the original letter of determination (LOD) is issued from the adjudicating authority.

(a). To have a final determination of denied reconsidered, the following steps must be followed:

(1). The original SOR/RFI must be responded to in its entirety. The unit security manager should review the response for clarity and completeness. If the response is incomplete, it will not be sent forward by J2 PERSEC. The response should be written in memorandum format by the Soldier and address every issue stated in the SOR/RFI.

(2). Attach to the letter any and all supporting documentation relating to the incident including receipts, updated credit report, community service documentation, letters from judges, etc.

(3). A letter of recommendation attesting to the Soldier's character and ability to maintain security clearance eligibility should be written by the Soldier's commander. If it is feasible from several commanders within the Soldier's chain of command to write letters, that is highly recommended.

(4). Finally, ensure that it has been at least 1 year since the denied eligibility was issued or the previous request for reconsideration was completed.

(5). Submit the response, supporting documentation and letter(s) of recommendation to the J2 PERSEC office for forwarding to the adjudicating authority.

i. Revoked

1. Eligibility of revoked is issued when a subject's investigation is closed, they have security clearance eligibility then derogatory information is discovered. The most common of these instances are unreported arrests that the DoD CAF becomes aware of or even reported arrests that the subject fails to complete their rehabilitation process or submit supporting documentation through security channels proving as such. Revoked eligibility is the result of due process.

2. The investigating or adjudicating authorities will never revoke a subject's eligibility prior to due process. Once the derogatory information is discovered, they will first give the subject an opportunity to respond. It is only if the subject fails to respond or they respond inadequately which results in a determination of revoked. Even when revoked, the subject will still have an opportunity to appeal.

(a). Appeals should be accomplished IAW the documentation that is sent from the adjudicating authority (typically the DoD CAF) to the subject.

(b). Once an appeal is initiated, the J2 PERSEC office is taken out of the process and cannot obtain any information about the case. The Personnel Security Appeals Board (PSAB) will communicate directly with the subject.

3. If the subject chooses not to appeal, the revoked adjudication becomes final. If PSAB determines enough mitigating information is not present, the revoked adjudication becomes final. In either case, the subject may have their case reconsidered once per year, every year, beginning with 365 days after the original letter of determination (LOD) is issued from the adjudicating authority.

(a). To have a final determination of revoked reconsidered, the following steps must be followed:

(1). The original SOR/RFI must be responded to in its entirety. The unit security manager should review the response for clarity and completeness. If the response is incomplete, it will not be sent forward by J2 PERSEC. For this response, it should be written in memorandum format by the Soldier and address every issue stated in the SOR/RFI.

(2). Attach to the letter any and all supporting documentation relating to the incident including receipts, an updated credit report, community service documentation, letters from judges, etc.

(3). A letter of recommendation attesting to the Soldier's character and ability to maintain security clearance eligibility should be written by the Soldier's commander. If it is feasible from several commanders within the Soldier's chain of command to write letters, that is highly recommended.

(4). Finally, ensure that it has been at least 1 year since the revoked eligibility was issued or the previous request for reconsideration was completed.

(5). Submit the response, supporting documentation and letter(s) of recommendation to the J2 PERSEC office for forwarding to the adjudicating authority.

Chapter 6 – Requesting Interim Eligibility

6.1 – Overview

- a. Interim eligibility at any level is able to be accomplished for reason of promotion, training, commissioning, mobilization, ETS or other by exception.
- b. Specific interim requirements may be found in Chapter 5 of this SOP by first defining the level of clearance eligibility required. General rules can be found in this Chapter below.
- c. All correspondence to the DoD CAF, including memorandums for record, reconsideration packets, requests for interim eligibility and appeals, should be addressed to: Commander, Department of Defense Consolidated Adjudications Facility, Army Division, Building 600, 10th Street Suite 200, Fort George G. Meade, Maryland 20755-5250.

6.2 – General Interim Guidance

- a. All interim requests must be justified by the first O5 in the Soldier's chain of command. Interims are only authorized for clearances, NOT suitability checks for civilian or contractor employees.
 - 1. The justification must be in writing, in memorandum format, digitally signed by the O5.
 - 2. Delegated signature authority is not authorized. Wet signatures and .jpg signatures will not be accepted.
- b. An investigation commensurate with the eligibility interim requested must currently be open.
 - 1. The Soldier requiring the interim must have completed their e-QIP.
 - 2. An email from PSI-CoE must have been received by the Soldier stating "All documentation from the subject has been received; no further action required."
 - 3. Finishing the e-QIP and being in receipt of the above stated email is the indicator that the investigation is officially opened. This can be confirmed by verifying in JPAS. JPAS will read an open investigation date and type.
- c. Once all of the above prerequisites are met, as well as any prerequisite stated in Chapter 5, send the request to the J2 PERSEC office for processing.
- d. Soldiers eligible for continued access are ineligible for interim access.

Chapter 7 – Requesting an Expedited Investigation or Adjudication

7.1 – Overview

- a. Expedited investigations or adjudications often time become a requirement when a deployment or training attendance is fast approaching. Keep in mind that although the process may be expedited, it is not an overnight process. Ensure to always leave adequate time, if able to, to make sure all investigations and adjudications are completed prior to the required reporting date.
- b. In most cases, expedite requests are filed in conjunction with interim requests.
- c. Soldiers eligible for continued access are ineligible for expedite requests.

d. All correspondence to the DoD CAF, including memorandums for record, reconsideration packets, requests for expedited investigation or adjudication and appeals, should be addressed to: Commander, Department of Defense Consolidated Adjudications Facility, Army Division, Building 600, 10th Street Suite 200, Fort George G. Meade, Maryland 20755-5250.

7.2 – Administrative Requirements for an Expedite Request

a. Investigation

1. T3

(a). A T3 investigation type must be officially opened. This is verifiable within JPAS.

(b). A request for expedited investigation must be sent to the J2 PERSEC office in memorandum format, signed by the first O5 in the Soldier's chain of command. Delegated signature authority is not authorized and only digital signatures will be accepted.

(c). Attach the expedite request to an e-mail, complete with the Soldier's personal identifiers, and send it to the J2 PERSEC office for processing.

2. T5

(a). A T5 investigation type must be officially opened. This is verifiable within JPAS.

(b). A request for expedited investigation must be sent to the J2 PERSEC office in memorandum format, signed by the first O5 in the Soldier's chain of command. Delegated signature authority is not authorized and only digital signatures will be accepted.

(c). Attach the expedite request to an e-mail, complete with the Soldier's personal identifiers, and send it to the G1 PERSEC office for processing.

b. Adjudication

1. Secret

(a). The commensurate investigation type must be closed. This is verifiable in JPAS.

(b). A request for expedited adjudication must be sent to the J2 PERSEC office in memorandum format, signed by the first O5 in the Soldier's chain of command. Delegated signature authority is not authorized and only digital signatures will be accepted.

(c). Attach the expedite request to an e-mail, complete with the Soldier's personal identifiers, and send it to the J2 PERSEC office for processing.

2. TS/SCI

(a). The commensurate investigation type must be closed. This is verifiable in JPAS.

(b). A request for expedited adjudication must be sent to the J2 PERSEC office in memorandum format, signed by the first O5 in the Soldier's chain of command. Delegated signature authority is not authorized and only digital signatures will be accepted.

(c). Attach the expedite request to an e-mail, complete with the Soldier's personal identifiers, and send the packet to the J2 PERSEC office for processing.

Chapter 8 – Indoctrinating and Debriefing Access

8.1 – Overview

a. As previously stated, there is a drastic difference between being investigated, a determination that a subject is eligible for a security clearance and finally being granted access to maintain classified information.

b. Once a subject is investigated and deemed eligible for a clearance, it is up to the unit to determine access requirements. Access requirements can range anywhere from having software application access to being able to enter a TOC or secured area.

8.2 – Access Types

a. U.S. Access

1. U.S. access is utilized for access to United States government systems, locations, facilities and briefings.

2. U.S. access, once indoctrinated, does not expire until either debriefed or the subject's current investigation expires.

3. The levels of U.S. access are as follows:

- (a). Confidential
- (b). Secret
- (c). Top Secret
- (d). SCI (SCI and additional caveats are managed by SSO)

b. NATO Access

1. NATO access is utilized for access to NATO systems, locations, facilities and briefings. NATO access is most common during mobilization and general & staff officers that frequently visit our ally countries for training exercises.

2. NATO access expires upon completion of NATO duty or when the subject's current investigation expires, whichever is less.

3. The levels of NATO access are as follows:

- (a). NATO Confidential
- (b). NATO Secret
- (c). NATO Cosmic Top Secret
- (d). Atomal Confidential
- (e). Atomal Secret
- (f). Atomal Top Secret

c. Additional access types such as NC2-ESI and Nuclear data are NOT managed by the J2 PERSEC office. Should these or other SCI caveats be required, contact the J2 SSO.

8.3 – Indoctrinating Access

a. Once all access prerequisites are met, a subject is eligible to be granted access. Keep in mind that although a subject may be eligible for access at the top secret level, that does not necessarily mean that their need-to-know is beyond the secret level. Their type of work, place of work, commander's intent, etc will determine the access level.

b. U.S. access should be granted using the following procedures:

1. Present the subject with an SF 312.

2. Once the document is read in its entirety, the subject requiring access should fill out all blocks in section 11.

3. A witness to the reading, preferably the security manager or readiness NCO, should fill out all blocks and sign as the WITNESS and ACCEPTOR (must be 2 different signatures). Unit will iPERM the document into the subjects record.

4. Once complete, forward the document to the J2 PERSEC office with an e-mail stating the request. The PERSEC section will grant the subject commensurate U.S. access in JPAS.

c. NATO access (up to NATO Secret) should be granted using the following procedures:

1. Subject completes an SF 312.

2. Once the document is read in its entirety, the subject requiring access should fill out all blocks in section 11.

3. A witness to the reading, preferably the security manager or readiness NCO, should fill out all blocks and sign as the WITNESS and ACCEPTOR (must be 2 different signatures). Unit will iPERM the document into the subjects record.

4. Present the subject with the NATO Briefing, NATO Security Brief and Introduction to NATO Powerpoint presentation for thorough review and understanding.

5. Once complete, forward the SF 312 to the J2 PERSEC office with an e-mail stating the request. The PERSEC section will grant the subject commensurate NATO access in JPAS.

6. For NATO access beyond NATO secret, contact the J2 SSO for instruction and guidance.

8.4 – Debriefing Access

a. Access should always be debriefed or rescinded upon completion of access-requiring duty, termination of need-to-know, loss of security clearance eligibility or forfeiture of membership in the NYARNG due to retirement, ETS or administrative separation.

b. Debriefing procedures are as follows:

1. Present the subject with their original SF 312 that was used to grant them access.

2. Have the subject thoroughly read and review the SECURITY DEBRIEFING ACKNOWLEDGEMENT portion of the SF 312.

3. The subject must sign and date the document.

4. A witness, preferably the unit security manager or readiness NCO, must sign and print below the subject's signature.

5. Return the document, once again, to the J2 PERSEC office for debriefing with an e-mail stating the request. The completed document must also be made a part of the subject's iPerms record.

c. If the original SF 312 is not available, present the subject with a new SF 312 and follow the above stated procedures.

Chapter 9 – Security Clearance Verification

9.1 – Overview

a. It is often necessary to provide security clearance verification for Soldiers who are mobilizing, attending training, attending conferences, etc. Although their eligibility information is listed in JPAS, not every section of every component at every site has access to view those records.

b. IAW Defense Manpower Data Center (DMDC) policy, JPAS printouts, screenshots and snippets are NOT AUTHORIZED. Such stated should never be provided to any person or entity for any reason, even quick reference.

9.2 – Verification Process

a. The recommended method of clearance verification is a security clearance verification statement.

PERSEC office, passed down from the National Guard Bureau (NGB).

b. The security clearance verification statement must include the subject's rank (if applicable), full name to include middle initial, the last 4 of their social security number or full EDI/P-ID, the date their current investigation closed, the date they were granted eligibility and the level in which they were granted eligibility.

1. Also recommended to be included in the verification statement is verification of the presence of NATO access and the type & date of any investigation that is currently open.

2. Do not use one statement for multiple individuals.

3. If an investigation is expired and the subject does not have a current reinvestigation open, manually downgrade the clearance eligibility on the statement. For instance, if the subject had an SSBI close 12 November 2009 giving them TS/SCI eligibility and the current date is 9 December 2015 with no current reinvestigation open, their statement should read that they have secret eligibility given on 11 November 2014.

c. Only adjudication information contain in the Personnel Summary section of the subject's JPAS record may be used for clearance verification. If their JPAS record lacks adjudication information in this section but there is investigation information, the subject DOES NOT currently have clearance eligibility. Refer to Chapter 14 of this SOP for steps to request recertification of the subject's investigation to grant them eligibility.

d. Security managers at all echelons are authorized to compile security clearance verification statements.

Chapter 10 – DoD Consolidated Adjudications Facility (DoD CAF) Correspondence

10.1 – Correspondence Overview

a. Typically, the Office of Personnel Management (OPM) is the investigating authority for uniformed personnel in any component of the Army. During the investigation, OPM may contact the subject of the investigation for clarification, and clarification purposes only, of information present in their SF 86. However, once the investigation is complete and forwarded to the DoD CAF for adjudication, if derogatory information (with a few exceptions) is discovered from the investigative files, the DoD CAF will contact the subject and their chain of command for more information.

b. All correspondence from the DoD CAF will be generated in memorandum format and will have suspenses attached to them.

1. Suspenses should be taken very literally and will be strictly adhered to.

2. If suspenses cannot be met, inform the J2 PERSEC office as soon as that information is known so that an extension may be formally requested.

3. If correspondence is ignored or suspenses are missed without appropriate communication, eligibility will ultimately be denied or revoked as a result of due process.

4. All correspondence to the DoD CAF, including memorandums for record, reconsideration packets and appeals, should be addressed to: Commander, Department of Defense Consolidated Adjudications Facility, Army Division, Building 600, 10th Street Suite 200, Fort George G. Meade, Maryland 20755-5250. Ensure all correspondence is sent through the J2 PERSEC office.

10.2 – Correspondence Types

a. Request for Information (RFI)

1. RFI's are typically generated because the DoD CAF has discovered information that may not solely preclude the individual from clearance eligibility but without clarification could greatly diminish the subject's impression on the adjudicators and their all-around "whole-person concept."

2. This correspondence type can range anywhere from minor delinquent accounts to prior criminal complaints or arrests. RFI's are used to rectify any inadequate information in the subject's personnel file.

b. Statement of Reasons (SOR)

1. SOR's deal with situations that are, for lack of better terms, more serious than those that are dealt with via RFI's. The information present in an SOR could prevent the subject from obtaining security clearance eligibility without further clarification and justification surrounding the incidents that are outlined.

2. This type of correspondence can range anywhere from detrimentally delinquent accounts to prior or present felony convictions or arrests. With a proper, complete response along with adequate rehabilitation, if required, a subject can reasonably expect the SOR to be mitigated and the adjudication to continue.

c. Letter of Intent (LOI)

1. An LOI is used, essentially, as a warning to the subject that the DoD CAF is on a path to denying or revoking their eligibility if certain criteria is not met. This could be due to the subject not responding to an SOR or RFI, or the DoD CAF may have uncovered severely derogatory information in the investigative files.

2. LOI's must be responded to by the subject. Failure to respond will result in due process and the DoD CAF moving forward with their original intent.

d. Letter of Determination (LOD)

1. LOD's are issued typically after any suspense listed in the LOI is missed or due process has taken place. An LOD will only be delivered if the determination is unfavorable or if the determination was previously unfavorable and the subject was submitted for reconsideration and the determination was overturned.

2. LOD's do not require a response, however, they do contain instructions for the subject to appeal the decision.

e. Warning Letter

1. Warnings are given when substantial derogatory information was found in the subject's investigative files however, they took proper steps to rehabilitate themselves or correct the delinquencies. The adjudicators will take that information into account, favorably adjudicate (pending the discovery of any other derogatory information) and issue a letter of warning stating that any repeat offenses will be grounds for immediate revocation or suspension of eligibility.

2. Warning letters do not require a response. There is, however, pertinent information in the letter such as instructions for things that the unit commander should pay close attention to or instances that require periodic reporting to the DoD CAF.

f. Letter of Suspension of Investigation – Deployment

1. If a Soldier is input for investigation prior to mobilization and it is not completed before their mobilization date, OPM, in most cases, will suspend the investigation and issue such a letter. This stems from instances such as a T5 being requested but OPM is unable to perform the personal interviews due to the Soldier being OCONUS. Ultimately, the investigation is suspended because mobilization removed key pieces of the investigation.

2. Letters of suspension do not require a response, however, it should be retained as there are specific instructions contained in the letter pertaining to reopening the investigation upon return from overseas.

10.3 – Response Procedures

a. Careful attention is critical when correspondence is being forwarded, as each type has different requirements and different timelines. The below guidance is general and should not be assumed for all documents of these types. Refer to the correspondence itself for specifics.

b. RFI

1. Within 10 days of receipt of the RFI, the subject must sign and return the RFI acknowledgement document to the J2 PERSEC office. This will give the DoD CAF indication that the subject received the documentation.

2. Within 30 days of receipt of the RFI, the subject must respond in full to the RFI.

When responding, ensure the subject includes the following:

(a). A letter from the subject, preferably in memorandum format, addressing every issue within the RFI. It is recommended that the letter address the issues in a bullet or numbering format as to ensure that the response hits all of the points. If the response lacks discussion of any of the issues, it will initiate due process for failure to respond completely.

(b). Supporting documentation. For example: if the RFI asks about a reported unpaid local tax bill from 2007, attach the receipt from the local taxing authority showing proof of payment. This is regardless of any dollar amount or situation; **SUPPORTING DOCUMENTATION IS A MUST**. Supporting documentation even applies to delinquent accounts that currently have a payment plan established. The subject should attach documentation from the creditor that outlines the payment plan. Keep in mind that there can never be too much supporting documentation.

3. If additional time is required to gather supporting documentation or formulate a response, contact the J2 PERSEC office immediately to request an extension to the suspense.

c. SOR

1. Within 10 days of receipt of the SOR, the subject must sign and return the SOR acknowledgement document from the SOR to the J2 PERSEC office. This will give the DoD CAF indication that the subject received the documentation.

2. Within 30 days of receipt of the SOR, the subject must respond in full to the SOR.

When responding, ensure the subject includes the following:

(a). A letter from the subject, preferably in memorandum format, addressing every issue within the SOR. It is recommended that the letter address the issues in a bullet or numbering format as to ensure that the response hits all of the points. If the response lacks discussion of any of the issues, it will initiate due process for failure to respond completely.

(b). Supporting documentation. It will often times be necessary to locate and include dated court documentation, certificates of rehabilitation completion, payment receipts or evaluation completion certificates. For referenced delinquent accounts, it will benefit the subject to provide documentation proving that payment plans have been established (normally a letter from the creditor), proof of bankruptcy, etc. No matter the case, supporting documentation is a must and the LOI response will not be reviewed by the DoD CAF without it.

3. If additional time is required to gather supporting documentation or formulate a response, contact the J2 PERSEC office immediately to request an extension to the suspense.

d. LOI

1. Within 10 days of receipt of the LOI, the subject must sign and return the LOI acknowledgement document from the LOI to the J2 PERSEC office. This will give the DoD CAF indication that the subject received the documentation.

2. Within 30 days of receipt of the LOI, the subject must respond to, in full, the LOI. When responding, ensure the subject includes the following:

(a). A letter from the subject, preferably in memorandum format, addressing every issue within the LOI. It is recommended that the letter address the issues in a bullet or numbering format as to ensure that the response hits all of the points. If the response lacks discussion of any of the issues, it will initiate the DoD CAF proceeding with their intent.

(b). Supporting documentation. It will often times be necessary to locate and include dated court documentation, certificates of rehabilitation completion, payment receipts or evaluation completion certificates. For referenced delinquent accounts, it will benefit the subject to provide documentation proving that payment plans have been established (normally a letter from the creditor), proof of bankruptcy, etc. No matter the case, supporting documentation is a must and the SOR response will not be reviewed by the DoD CAF without it.

3. If additional time is required to gather supporting documentation or formulate a response, contact the J2 PERSEC office immediately to request an extension to the suspense.

4. Note that an LOI is normally accompanied by an SOR.

e. LOD

1. No response is required.

2. Maintain the correspondence as it contains specific appeal instructions.

f. Warning Letter

1. No response is required.

2. Maintain the correspondence as it contains specific instructions for the commander and reporting procedures, if applicable.

g. Notice of Investigation Suspension – Deployment

1. No response is required.

2. Maintain the correspondence as it contains specific instructions for reopening the investigation upon return from OCONUS.

10.4 – Soldiers Pending ETS/Separation

a. Even Soldiers that are pending ETS/separation or have already been processed for such are required to respond to DoD CAF correspondence.

b. If the subject cannot be reached due to this circumstance, a memorandum for record must accompany the correspondence back to the DoD CAF from the unit stating why the Soldier was unable to be reached.

c. Also included should be any formal separation documentation.

d. Without such a response, the DoD CAF will assume that the chain of command refuses to present the correspondence to the subject and will take appropriate action.

10.5 – Appeal Process

a. In any situation pertaining to security, the subject is always granted due process and the right to appeal; even if an appeal is denied, they are even further granted the right to have the determination reconsidered. See Chapter 11 of this SOP for the reconsideration process. Only after the appeal process is complete is the determination considered final.

b. If given the chance to appeal and the subject does respond, then their right is forfeited and, at which time, the determination is considered final. The subject must wait 1 year for submission of reconsideration.

c. In order to appeal the determination, the subject must follow the appeals process:

1. When issued their Letter of Determination, the subject must return the acknowledgement portion stating that they wish to appeal, either in person or not in person, within 10 days of receipt. NO OTHER METHOD OF INDICATING THE WISH TO APPEAL IS AUTHORIZED. If the subject fails to return the wish to appeal statement, the DoD CAF will make their determination final and the subject will need to follow the reconsideration process outline.

(a). Appeal in person.

(1). The subject will be called upon to appear before the Personnel Security Appeals Board (PSAB). The subject retains the right to have a lawyer present although this is not a legal matter but a matter of suitability. Appearing before an appeals board will be at no cost to the Government.

(2). Once the subject elects to appeal in person, the DoD CAF will no longer communicate with the subject through the J2 PERSEC office. Instead, the Defense Office of Hearings and Appeals (DOHA) will communicate directly with the subject via the phone number and mailing address that the subject provided on the appeal election. The DOHA is responsible for contacting the subject to inform them of the date, time and location of the personal appearance.

(b). Appeal without a personal appearance.

(1). The subject will be required to submit any and all documentation, to include newly founded information and justification to support their case, through the mail to the PSAB. They will also need to write a statement regarding their case, detailing the circumstances surrounding the incident(s) that led to the determination. This requirement is due within 40 days of receipt of the Letter of Determination.

(2). Once the subject elects to appeal without a personal appearance, the DoD CAF will no longer communicate with the subject through the J2 PERSEC office. Instead, the Defense Office of Hearings and Appeals (DOHA) will communicate directly with the subject via the phone number and mailing address that the subject provided on the appeal election.

d. When the appeal process is complete, the PSAB will again review any information that was submitted to them. They will issue yet another determination stating either a denied appeal or approved (overturned determination) appeal in writing through the J2 PERSEC office to the subject. This determination is considered final and cannot be refuted until the reconsideration process.

e. The J2 PERSEC office cannot obtain any information regarding the case. Once the appeal process is started, all information is reserved between the PSAB and the subject. The J2 PERSEC office nor the DoD CAF can contact the PSAB or DOHA to inquire about a status of the case.

Chapter 11 – Reconsideration Process

11.1 – Overview

a. Once a determination is issued, the subject may appeal. Once an appeal determination is issued, it is considered final. However, the subject may attempt to have the determination reconsidered once per year, every year, starting 12 months after receiving the appeal determination letter.

b. The reconsideration process should not be assumed to be a quick turnaround process. Once the request is submitted, the DoD CAF must first re-order the subject's investigation files from the investigating agency then assign the case to an adjudicator. Depending on the gravity of the situation surrounding the denial/revocation, the reconsideration adjudication can take anywhere from a few weeks to a few months, even a year.

c. All correspondence to the DoD CAF, including memorandums for record, reconsideration packets and appeals, should be addressed to: Commander, Department of Defense Consolidated Adjudications Facility, Army Division, Building 600, 10th Street Suite 200, Fort George G. Meade, Maryland 20755-5250.

11.2 – Reconsideration Procedure

a. Elements of a reconsideration packet

1. A thorough response to the original SOR/LOD. Ensure the response is detailed and presents any information that may have previously been left out of the original response. The more detailed the response, the more efficient the process.

2. Any and all supporting documentation/updated information. Included should be all previously submitted documentation and anything new that may have surfaced since the original incident.

3. A letter from the subject stating why they believe their determination should be reconsidered. It is recommended that the subject make a compelling case including their need for security clearance eligibility.

4. Letter(s) of recommendation from the subject's commander. This letter should attest to the subject's character and their ability to maintain security clearance eligibility and adhere to standards. Multiple letters from commanders all of the way through the subject's chain of command would be welcomed and favored.

b. All elements of the reconsideration packet should be submitted to the J2 PERSEC office for forwarding to the DoD CAF. While the subject is going through the reconsideration process, it should not be assumed that they will be granted eligibility and therefore they should not be scheduled for clearance-requiring training attendance nor should they be slotted in a DPOS that requires a clearance.

c. Once submitted, there will be no updates of the reconsideration until the process is complete. If the determination is overturned, security clearance eligibility will be granted in JPAS with an effective date of the day adjudication completed. Note that this may be a date AFTER the adjudicated investigation has expired. In this case, the subject will simply need to be reinvestigated.

d. Denied or revoked out-of-scope investigations must first be over-turned prior to reinvestigation.

Chapter 12 – Incident Reporting

12.1 – Overview

a. It is the responsibility of everyone from a subject and their peers all of the way to the J2 PERSEC office to report, or inquire about, derogatory information if they hear about it or see it (see AR 380- 67, Chapters 2 & 8). Derogatory information should be reported as soon as possible. For instance; the moment the subject is arrested (criminal cases), when they are verified to be abusing drugs or alcohol or when it is assumed they are no longer trustworthy or capable of handling classified information.

b. Regardless of the subject's security clearance eligibility, they are required to report derogatory information. Even if their eligibility is currently suspended and they embark on an additional infraction, it must be reported.

c. Not all cases of derogatory information reporting warrant the suspension of an individual's eligibility. Using the whole-person concept and the adjudicative guidelines, the commander should make such recommendation to maintain or suspend eligibility. When the information is forwarded to the DoD CAF, they too will use the adjudicative guidelines, the nature of the situation, any supporting documentation and the commander's recommendation in order to make their determination.

12.2 – Incident Reporting Process

a. When derogatory information is discovered that coincides with the adjudicative guidelines, it should immediately be reported to the J2 PERSEC office via a DA Form 5248-R. Attached to the form should be any and all supporting documentation surrounding the incident. Supporting documentation may include (not all-inclusive):

1. Court docket sheets.
2. Serious Incident Reports (SIR).
3. Counseling statements.
4. Urinalysis reports from NYARNG Counterdrug.
5. ARD discharge certificates.
6. Sworn statements.

b. The more supporting documentation that is submitted with the incident report, the better. This will enable the DoD CAF to make a more suitable determination as well as streamline the process for when the commander wishes to reinstate the subject's security clearance eligibility, if they so choose.

12.3 – Incident Reporting Requirements

a. Once the original incident report is submitted with supporting documentation, a follow-up incident report is then required every 90 days until conclusion and final adjudication. Follow-up incident reports are not required to have supporting documentation attached however, if new information surfaces, it would benefit all parties involved to include such items. These reports must be submitted on a DA 5248-R.

b. When the situation concludes, for instance criminal charges are withdrawn in court or a subject completes their ARD program, a final incident report must be submitted with supporting documentation detailing the conclusion of the incident. This report must be submitted on a DA 5248-R.

1. If the subject's eligibility was suspended due to the original incident report and the commander now wishes to reinstate, such action must be annotated on the DA 5248-R.

2. If the subject's eligibility was suspended due to the original incident report and the commander wishes to have their eligibility revoked, such action must be annotated on the DA 5248-R.

3. If the subject's eligibility was not previously suspended but due to the circumstances surrounding the conviction or conclusion the commander now wishes to suspend or revoke the subject's eligibility, such action must now be annotated on the DA 5248-R. If suspension is sought after, the incident should be considered to remain open and follow-up incident reports must continue to be submitted (every 90 days).

c. The final incident report will be sent to the DoD CAF for appropriate adjudication. Every attempt will be made to follow the commander's recommendation however, adjudication is ultimately the call of the DoD CAF adjudicators utilizing the whole-person concept and the adjudicative guidelines.

d. Incident reports MUST be signed by the unit commander or AO if the commander is not available.

12.4 – ETS and Separation

a. Personnel who ETS or are separated from the NYARNG and currently have their eligibility suspended must still be reported to the J2 PERSEC office via a DA 5248-R.

b. Security managers should submit the final DA 5248-R with the commander's recommendation to the J2 PERSEC office and attach the Soldier's discharge or separation documentation.

c. Incident reports must be closed out, favorably or unfavorably, in the event that the Soldier makes an attempt to transfer services, reenlist or seeks other federal employment.

Chapter 13 – Continuous Evaluation (CE)

13.1 – Overview

a. As a corroboration, CE was developed by the DoD and OPM as a way of capturing unreported derogatory information. The process utilizes dozens of federal, state and local databases to query for the presence of derogatory information pertaining to investigated personnel.

b. Information that CE searches for includes types such as felonies, non-traffic misdemeanors, drug or alcohol violations, severely delinquent credit and foreign travel. CE will only discover information fitting this criteria that was not previously reported to the DoD CAF. In most situations, CE will only search for discoverable information that came about since the subject last filed an SF 86. However, there are certain types of information that are searched for without a time constraint.

c. All personnel that have current investigations or personnel that will be investigated in the future are susceptible to CE.

13.2 – CE Processing

a. The CE report is generated by OPM and sent to the DoD CAF. The DoD CAF then forwards the CE report to the appropriate State UIC. Once the report is retrieved by the State security manager, it is distributed to BN/BDE security managers in an effort to gather more information.

b. Unit security managers will not always receive the actual CE report, instead they may just get an excerpt of the information that was discovered.

c. If a unit security manager receives a CE inquiry, the following steps should be followed:
1. Identify the actual unit that the Soldier belongs to or is attached to. Contact the unit of assignment to acquire information surrounding the incident.

2. Report the incident back to the J2 PERSEC office via a DA 5248-R. Supporting documentation still remains a requirement. See Chapter 12 regarding incident reporting.

3. If the Soldier is pending separation and cannot be contacted for information, the unit commander must supply a memorandum for record stating as such. Include any separation documentation.

d. Once the CE report is sent to the unit security manager, they will have **5 days to respond to the report in full**. This includes the DA 5248-R either recommending suspension or maintenance of their clearance eligibility and supporting documentation. Failure to respond to the request within the 5 day window will result in the DoD CAF contacting NGB and NGB contacting State leadership noting the failure to comply.

Chapter 14 – Requests for Action (RFA)

14.1 – RFA Overview

All personnel security actions not covered by the MN 1998-E or addressed by other documentation such as DoD CAF correspondence needs to be relayed and tracked by e-mail and supporting documentation.

14.2 – RFA Types

a. Upgrade

1. If a Soldier's current eligibility is No Determination Made, an e-mail should be used to request adjudication of a current investigation.

2. The e-mail needs to contain the Soldier's identifiers, investigation information and updated signature pages if the investigation is outside of the 5 year window. See Chapter 5.2d for more information on No Determinations Made.

b. Investigation Information Update

1. The e-mail should be utilized to inquire about the standing of a subject's investigation in the event that the information in JPAS appears to be inadequate.

2. BN/BDE security managers are discouraged from requesting investigation updates within an unreasonable amount of time. Typically, investigations may take anywhere from 1 to 12 months to complete.

c. Reconsideration

1. An e-mail should always accompany a request to have a subject's revoked or denied eligibility reconsidered.

2. See Chapter 11 for more information on the reconsideration process.

d. Reciprocity

1. In many cases, personnel are investigated by other agencies before coming to the NYARNG. For example, they may have been investigated by the Defense Intelligence Agency (DIA) as a result of government employment. As a result, upon accessioning into the NYARNG, their previous, in-scope investigation may not have translated in JPAS.

2. IAW AR 380-67, all federal investigations, regardless of the investigating agency, will be recognized throughout. An e-mail should be utilized to request reciprocal adjudication. The subject's investigation information should be contained in the RFA with justification for adjudication.

3. It should first be confirmed that the subject did not have a greater than two year break in federal service since the conclusion of their investigation.

e. Recertification

1. Recertification RFA's can be used when personnel have eligibility of Loss of Jurisdiction, Eligibility Administratively Withdrawn or no eligibility at all when there is an in-scope investigation present.

2. First, it must be verified that the subject did not have a greater than two year break in federal service since the conclusion of the investigation.

3. Once it is confirmed that an applicable break in service does not exist, submit an e-mail containing the subject's administrative identifiers and investigation information.

4. See Chapter 5 for more information regarding the above stated adjudication types.

f. Incident Reports

1. Occasionally, Soldiers are accessed into the NYARNG with pending incident reports on file in JPAS and with the DoD CAF. This will be annotated in JPAS on their personnel summary screen. Because the NYARNG did not submit these reports, they are not readily available and must either be requested through the DoD CAF or from the agency that originally submitted the incident. This is necessary to verify the Soldier's suitability and to track repeat offenses.

2. Submit a request for information in an e-mail identifying the need for the incident report. Every effort will be made to grant the request.

g. Original SOR/LOI/LOD Apprehension

1. Because of the frequent cycling of personnel through units and reassignment of security managers, it is fairly common for a security manager to not retain original documentation pertaining to the denial or revocation of a Soldier's clearance. This is also the case when the Soldier was previously denied eligibility in a different branch, component or State of service. It will be necessary to obtain the original documentation in order to have the Soldier reconsidered for security clearance eligibility.

2. In the e-mail, include the subject's administrative identifiers, investigation information from the investigation that lead to denial/revocation and finally any other information that the Soldier may be able to present from when the original eligibility was issued. See Chapter 11 for the reconsideration process.

3. Once the e-mail is received by the J2 PERSEC office, the information/documentation will be submitted to the DoD CAF for re-presentation of the original documentation. However, the J2 PERSEC office will not be authorized to present the physical documents as the Soldier previously had their opportunity at due process. Instead, the office will summarize the key points and make recommendations towards the steps to rectify the situation.

Chapter 15 – Foreign Travel

15.1 – Overview

a. Recently, foreign travel has become a hot topic as well as foreign relationships and ties to foreign governments. Foreign travel is not looked at as derogatory until it is failed to be reported.

b. This chapter applies to all personnel working in the auspices of the NYARNG, regardless of rank or duty status, no matter their clearance eligibility, investigation status or standing within the organization.

15.2 – Foreign Travel Policy

a. Formal foreign travel policy has been developed by the J2 Directorate.

b. Keep in mind that every effort must be made to report foreign travel prior to the actual act. Reportable foreign travel is applicable to both business and personal travel with the only exception of mobilization.

c. Personnel traveling for personal reasons are subject to a briefing and several other requirements contained within the foreign travel policy.

d. Personnel traveling for business reasons are subject to a briefing and several other requirements contained within the foreign travel policy.

e. Personnel that travel abroad regularly for business reasons, such as State Partnership liaisons, are subject to the same requirements outlined in the foreign travel policy but only at a rate of every 6 months.

f. Unreported foreign travel is discoverable information in the CE process (see Chapter 13 for more information on CE). Unreported foreign travel is considered derogatory and will be administratively actioned to the fullest extent.

g. Personnel with SCI eligibility are subject to additional foreign travel reporting requirements contained in the foreign travel policy. Contact the NYARNG J2 for more information.

15.3 – Foreign Travel Reporting Process

a. Once foreign travel plans are confirmed, the processes within the foreign travel policy should be reviewed and adhered to.

b. Upon the subject's return from their travels, the processes within the foreign travel policy should be reviewed and adhered to.

c. Travel to OCONUS sites that are still United States territories need not to be reported. A solid reference is that if the subject's passport is going to be stamped, they must report the travel.

Chapter 16 – Maintaining a Security Clearance Access Roster (SCAR)

16.1 – Overview

a. To reiterate; there is a vast difference between being investigated, being granted security clearance eligibility and finally being granted commensurate access.

b. Once a subject is granted access, it is appropriately annotated in JPAS and the subject is now "cleared" for access to classified information and areas of operation.

c. The SCAR is, essentially, a quick reference list of all personnel that a particular echelon is responsible for that are cleared at such a level.

16.2 – SCAR Maintenance

a. Once all personnel are properly owned or serviced in JPAS, an initial SCAR can be built directly from the system. See Chapter 3 of this SOP for more information pertaining to inprocessing and out-processing personnel.

1. In JPAS, in the gray tab section, choose Reports.

2. Choose Personnel.

3. Select the appropriate configuration. Run the report.

4. Back in JPAS, choose Report Pickup under Reports. Save your report. Your initial SCAR is built.

b. You are now able to modify and manipulate the report in any way you choose. This report contains all personnel in your hierarchy, their investigation information, their eligibility information and the access level in which they were indoctrinated at, if applicable.

c. After this initial SCAR is built, it is now the security manager's choice whether to maintain this document, updating it as actions are complete, or run the report from JPAS whenever needed and adjust as necessary as local SOP dictates.

Chapter 17 – Systems and Authorities

17.1 – Systems within PERSEC

- a. Personnel Security Investigation Portal (PSIP)
 1. PSIP is maintained by PSI-CoE and is the central system for all Army component personnel security investigation requests.
 2. PSIP initiates all investigation openings through OPM and e-QIP.
 3. Contact information for PSI-CoE is as follows:
 - (a). Phone – (410) 278-4194
 - (b). Fax – (410) 306-0413
 - (c). Mail – Department of the Army PSI Center of Excellence, 3240 Raritan Ave., Aberdeen Proving Ground, MD 21005
- b. Joint Personnel Adjudications System (JPAS)
 1. JPAS is the system of record for all personnel security investigations and eligibility determinations throughout the DoD.
 2. Army entities are not authorized to perform any actions within JPAS with the exception of access granting. As a result, JPAS should be considered by field units to be a read only system.
- c. Defense Information System, for Security (DISS) Portal
 1. The DISS portal is the system used for communication between DoD adjudicators and State headquarter-echelon security managers, such as the J2 PERSEC office.
 2. All CAF correspondence and requests for action are processed through this system.
 3. All foreign travel is reported through JPAS and DISS portal.
- d. Electronic Questionnaires for Investigations Processing (e-QIP)
 1. e-QIP took the place of the original paper copy SF 85 & SF 86 submission. Subjects being investigated now login to the e-QIP website, administered by OPM, and complete their questionnaires digitally.
 2. All technical and administrative issues, such as login or specific questions regarding the questionnaire, should be addressed directly to PSI-CoE using the contact information provided above or in the emails received by the applicant from PSI-CoE.

17.2 – Authorities

- a. OPM is the oversight of all personnel security investigations for DoD entities. They physically execute investigations and maintain investigation files.
- b. DoD CAF is responsible for adjudication of personnel security investigations. They also remain the final approval authority for derogatory information reporting and unfavorable administrative action in terms of security clearance eligibility.
- c. PSI-CoE acts as a liaison between the Army and OPM. Their responsibilities include compiling a triaged list of investigation requests and determining need for investigation.
- d. NGB-G2 remains the policy maker and distributor regarding personnel security investigations within the ARNG. They also act as the J2 PERSEC office's higher headquarters.
- e. NYARNG J2 directorate maintain personnel security responsibility throughout the NYARNG. All personnel security issues, questions and inquiries from unit security managers will be directed here.

Chapter 18 – Requesting JPAS Access

18.1 – Steps for Requesting Access

- a. Request access through the J2 PERSEC office with an e-mail containing the IA certificate, PII certificate, JPAS Introduction certificate and a completed DD 2962 signed by a O-4 or higher as the nominating official.
- b. Although every attempt will be made to action and consider all requests, generally internal policy is to keep JPAS users at a maximum of 2 per battalion, 2 per brigade, 2 per division and 2 per TDA unit. At least 1 of the security managers at each echelon must be AGR.
 1. Special exceptions can be made to this preference in times of drastic need such as warfighter exercises or mobilization.
 2. Any personnel requesting JPAS access must have at least secret eligibility. This requirement cannot be waived.
- c. Upon reassignment of JPAS account holders, the J2 PERSEC office must be notified so that JPAS accounts may be adjusted.
- d. All unit security managers are eligible for level 7 access.

18.2 – JPAS Rules

- a. A user will never attempt to view their own record.
- b. JPAS accounts are frequently audited but need not to be renewed except in the instance of reassignment.
- c. Never print a JPAS personnel summary.
- d. JPAS is fed by several other HR systems that are subject to human error. If something doesn't look right, say something so that it may be corrected.
- e. Pay attention to the citizenship status in JPAS. If it annotates that a subject is a foreign national, they are ineligible for a clearance. If it annotates they are a U.S. citizen but foreign born, other systems may consider them still as foreign nationals. It would be safe to submit investigation requests for these subjects accompanied by naturalization paperwork.
- f. You must login to JPAS at least once every 30 days or risk your account being deleted.
- g. Never click the red "x" to exit JPAS; always log out or your account risks being locked.
- h. JPAS times out approximately every 5 minutes. If you are inactive in the system, log out.

Chapter 19 – Personnel Security Requirements for Soldier Readiness Process (SRP)

19.1 – Overview

- a. As a prerequisite to mobilize, personnel are required to have a favorable investigation and security clearance eligibility as required by their MOS or deployment manning document (DMD). Failure to meet this requirement will result as a NO GO for security.
- b. If a Soldier does not require security clearance eligibility due to their MOS or DPOS and they have no investigation present in JPAS, a requirement remains to at least be fingerprinted and have a favorable T3 completed prior to mobilization.
- c. The above stated requirements are the only security requirements for mobilization. If the theatre commander instills any additional requirements of security clearance eligibility and the Soldier does not meet them but do hold eligibility commensurate with their MOS & DPOS, they will remain a GO for security.

19.2 – J2 PERSEC Responsibilities for SRP

- a. The J2 PERSEC office will provide every individual with a personnel security clearance verification statement in their mobilization documents regardless of their eligibility standing.
- b. All personnel identified as NO GO's will need to have all items rectified prior to Soldier Readiness Check (SRC) to ensure being cleared.

Chapter 20 – Visit Requests

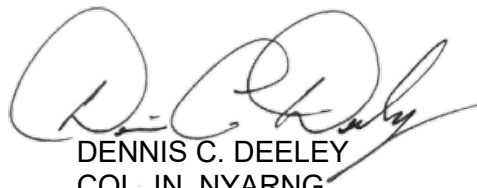
20.1 – Overview

- a. Visit requests grant entities outside of the NYARNG hierarchy permission to view security clearance eligibility in JPAS for personnel belonging to the NYARNG. This can be for instances such as VTC's or SVTC's, physical site visits, unit attachments, mobilization attachments, training attendance or conference attendance, among other things.
- b. JPAS visit requests can only be performed by the J2 PERSEC office.

20.2 – Visit Request Process

- a. Once it is identified that a visit request is required, the following information must be obtained:
 1. Security Management Office (SMO) code of the entity requiring access to particular NYARNG personnel's clearances.
 2. A point of contact for the SMO or visit.
 3. Phone number for the point of contact.
 4. The date range for which the SMO requires access. This could be the length of mobilization, length of conference, etc. A good rule of thumb is to add 1 day to the beginning and 1 day to the end as a buffer.
 5. The names and SSN's of the personnel that the SMO requires access to.
 6. If applicable, the classification level of the conference, training, visit, VTC, etc.
 7. Any additional information such as the reason for visit.
- b. Upon compilation of the items above, send the visit request to the J2 PERSEC office for input via e-mail to the J2 PERSEC office. Notification will be sent once the visit request is input.
- c. In the event that anything in the request needs to be modified after input, once again gather all of the required information, annotate what needs to change and resend to the J2 PERSEC office for action.

Revision suggestions or questions regarding this SOP should be directed to the PERSEC Office through SFC Ruth DeRenzo at ruth.j.derenzo@mail.mil or SSG Paul Croteau at paul.l.croteau.mil@mail.mil.



DENNIS C. DEELEY
COL, IN, NYARNG
Director, J2

This page intentionally left blank

APPENDIX A – References

AR 380-67 – DoA Personnel Security Program
AR 600-8-19 – Enlisted Promotions and Reductions
DA PAM 611-21 – MOS Smartbook
DCID 6/4 – Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)
Homeland Security Policy Directive-12 (HSPD-12)
ICD 704 – Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)
NGR 600-100 – Commissioned Officers; Federal Recognition and Related Personnel Actions
NGR 600-200 – Enlisted Personnel Management
PSIP Requester’s Continuity Handbook
SIDPERS Data Reference Manual (SDRM)
Submission of Tier 5 (T5) Investigation Requests

APPENDIX B – Terms and Acronyms

Access – The ability and opportunity to obtain knowledge of classified information.

Adjudication – Review of investigative files for the purpose of determining security clearance suitability.

ANACI – Advanced National Agency Check with Inquiries

AOC – Area of Concentration

ASI – Additional Skill Identifier

Atomal Confidential – U.S. restricted data level of access.

Atomal Secret – U.S. restricted data level of access.

Atomal Top Secret – U.S. restricted data level of access.

BI – Background Investigation

Caveat – Special access programs associated with personnel security.

CE – Continuous Evaluation

Commander’s Corner – G1 centric systems software application.

COMSEC – Communications security

Confidential – Level of adjudication.

Continued Access – The period in between when a subject’s previous investigation expired and their reinvestigation closed. Access is continued, without lapse, with the assumption their reinvestigation will close favorably.

CONUS – Continental United States

Debrief – To remove specified levels of access.

Denied – The refusal to grant a security clearance or to grant a higher level of clearance to a person who possesses a clearance of a lower degree.

DMDC – Defense Manpower Data Center

DoD – Department of Defense

DoD CAF – Department of Defense Consolidate Adjudications Facility

DoD Civilian – Civilians employed by the Department of Defense.

DOHA – Defense Office of Hearings and Appeals

DPOS – Duty position

Due Process – An in-place system with the purpose of granting subjects adequate time to refute any potentially unfavorable situation with regard to personnel security.

Eligibility Administratively Withdrawn – An administrative removal of one’s adjudication, most often times due to transfer of components.

e-QIP -

eSAAR – Electronic System Access Authorization Request

ETS – Expiration of Time in Service

Indoctrinate – To grant access.

Interim Clearance – A security clearance based on the completion of minimum investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirement

iPerms – Interactive Personnel Electronic Records Management System

JPAS – Joint Personnel Adjudications System

Letter of Suspension of Investigation; Deployment – a document issued by the DoD CAF with the purpose of suspending a subject’s investigation for reason of mobilization.

LOD – Letter of Determination

LOI – Letter of Intent

Loss of Jurisdiction – An administrative removal of one’s adjudication, most often times due to transfer of branches of service.

MOS – Military occupational specialty

MRD – Mandatory Retirement Date

NAC – National Agency Check
NACI – National Agency Check with Inquiries
NACLC – National Agency Check with Law and Credit
NATO Confidential – NATO level of access.
NATO Cosmic Top Secret – NATO level of access.
NATO Secret – NATO level of access.
NC2-ESI – Special access program classified as Extremely Sensitive Information.
NDA – Non-disclosure Agreement
NDS – Non-disclosure Statement
NDM – No Determination Made
NGB – National Guard Bureau
Nuclear Data – also known as a “Q” clearance; a Department of Energy level of access.
NYARNG – New York Army National Guard
OCONUS – Outside of Continental United States
OPM – Office of Personnel Management
PD – Position Description
PERSEC – Personnel security.
Personnel security – The application of standards and criteria to determine whether or not an individual is eligible for access to classified information, qualified for assignment to or retention in sensitive duties, and suitable for acceptance and retention in the total Army consistent with national security interests.
Personnel Security Investigation – Any investigation required for the purpose of determining the eligibility of DoD military and civilian personnel or contractors for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties requiring such investigation.
PSAB – Personnel Security Appeals Board
PSI-CoE – Personnel Security Investigations Center of Excellence
PSIP – Personnel Security Investigation Portal
PSIR – Personnel Security Investigation Request
QRB – Qualitative Retention Board
RCAS – Reserve Component Automation System
Read-on – Special process required to indoctrinate personnel into special access programs.
Revoked – The cancellation of a person’s eligibility for access to classified information.
RFI – Request for Information
SAC – Special Agreement Check
SCAR – Security Clearance Access Report
SCI – Sensitive Compartmented Information
Secret – Level of adjudication.
Security Clearance – A determination that a person is eligible under the standards of DoD regulatory guidance for access to classified information.
SIDPERS – Standard Installation and Division Personnel Reporting System
SIPRNET – Secret Internet Protocol Router Network
SMO – Security management office/security management officer
SOP – Standard Operating Procedure
SOR – Statement of Reasons
SQI – Skill Qualification Identifier
SRB – Selective Retention Board
SRC – Soldier Readiness Check
SRP – Soldier Readiness Process
SSBI – Single Scope Background Investigation
SSO – Special Security Office

SVTC – Secured video-teleconference
T1 – Tier 1 investigation
T2 – Tier 2 investigation
T3 – Tier 3 investigation
T4 – Tier 4 investigation
T5 – Tier 5 investigation
TDA – Table of Distribution and Allowances
TOC – Tactical Operations Center
TS – Top Secret
TS/SCI – Top Secret with Sensitive Compartmented Information
UJS – Unified Justice System
UMR – Unit Manning Report
Visit Request – To allow outside personnel to view internal security clearance information in JPAS.
VTC – Video teleconference
Warning Letter – Document issued by the DoD CAF to warn a subject of potentially harmful (to their clearance eligibility) information or actions.