National Archives and Records Administration

NARA 273, S1
December 20, 2016

Supplement to NARA 273, Administrative Procedures Related to Security Clearances and Applicant and Employee Rights

PART 1 - REQUESTING AND GRANTING SECURITY CLEARANCES

1. Establishing the need for a security clearance.

a. When a nominee requires access to a particular level of classified information in order to perform his or her job, he or she has a need for a security clearance.

b. Supervisors may request a security clearance only for those nominees who require access to classified information due to required work assignments, and can only request a clearance for the level appropriate to the work assignments.

c. Executive Order (E.O.) 12968 expressly directs agencies to keep the number of employees with eligibility for access to classified information to the minimum required to conduct agency functions and expressly prohibits requesting eligibility in excess of actual requirements.

(1) Only those staff members who require access to classified information on a regular and recurring basis should have a security clearance.

(2) No individual is entitled to a security clearance solely because of title, position, or previous position that required a security clearance.

(3) A security clearance is not appropriate to only permit entry to, or ease movement within, controlled areas.

2. First steps when proposing to hire, appoint, promote, or reassign a nominee to a critical sensitive position.

a. Before making a final commitment and establishing an effective date for placing a nominee in a critical sensitive position, the Office of Human Capital, Staffing and Recruitment Branch (HTS) must provide notification to the Personnel Security Officer (PSO) as outlined below:

(1) When a nominee is not a NARA employee, HTS will provide the following information:

(a) Full name;

(b) Social security number;

(c) Date of birth (DOB);

(d) Place of birth (POB) - city and state if born in the United States or City and Country if born outside the United States;

(e) Email address;

(f) Proposed and current position title, series, and grade;

(g) Organization code of the gaining unit;

(h) Sensitivity level;

(i) Copy of the nominee's resume or application;

(j) Copy of the Optional Form (OF)-306, Declaration for Federal Employment; and

(k) Copy of the position description being hired into.

(2) When the nominee is a current NARA employee, HTS will provide the following information:

(a) Copy of the nominees current Standard Form (SF) 50;

(b) Copy of the position description the nominee is being recommended for; and

(c) Organization code of the gaining unit.

b. Upon receipt of this information, the Security Management Division (BX) determines whether the nominee has had the necessary investigation for placement in the position and has been previously granted a clearance. BX also requires the nominee to sign a release under the Fair Credit Reporting Act of 1970 as amended and conducts a credit check;

c. BX notifies the staffing specialist in HTS as soon as the nominee has been cleared for appointment or hire to a critical sensitive position requiring access to classified information. HTS must not make a final commitment to the nominee until the initial screening has been approved by the PSO; and

d. HTS determines if the position is subject to drug testing and if so, initiates a screening test.

3. Eligibility determination process.

BX personnel security specialists grant security clearances upon completion and favorable decision of an appropriate background investigation, or through a reciprocal exchange with another Federal agency that has already conducted an investigation on that nominee.

4. Investigation standards that NARA follows.

NARA follows guidance under 5 CFR 732.101 issued by the United States Office of Personnel Management (OPM). The minimum standards and the investigative levels are:

a. For initial access to Confidential, Secret and Top Secret information, NARA requires a successfully adjudicated security investigation at the required level determined by the PSO and current OPM, National Background Investigations Bureau policy for all nominees.

b. All Confidential, Secret and Top Secret clearances require recertification for nominees whose initial investigation either did not meet the required standard or whose investigation was not within the five-year time frame specified in paragraph 10 of this Supplement.

5. Requesting security clearances when no appropriate pre-existing clearance is identified or if a re-investigation is required.

a. NARA officials requesting clearances must send a completed NA Form 3016, Personnel Security Action Request and Certification, to BX indicating which type of clearance is being requested - Confidential, Secret, or Top Secret. They also must provide the appropriate cost account information in Part B of the NA Form 3016 and submit the completed form to BX.

b. Upon receipt of the NA Form 3016, the personnel security staff notifies the nominee to complete forms in e-QIP. The nominee must complete the security forms and have an approved initial record screening, before he or she is assigned to the critical sensitive position or brought on duty. The personnel security staff notifies the requesting office when the security forms have been reviewed and approval of the prescreening requirement, so the effective date of the personnel action can be determined without delay.

6. Maintaining collateral clearances for retired NARA employees who return as volunteers on classified projects.

The office head submits a written request to the PSO to allow the retired employee to maintain his or her clearance on classified projects. If the investigation is within the allowable valid time frame and issues of suitability are not noted, then the PSO may allow the retired employee to maintain the clearance for the time necessary to complete the project. If the date of the investigation is outside the allowable valid time frame for the project, the office head will have to fund a periodic re-investigation so that the retired employee can continue to hold the clearance.

7. Implementing reciprocity.

Employees who previously held a security clearance granted by another Federal agency may be approved for access at NARA if their last investigation was completed within the past five years, and they have not retired or otherwise been separated from the Government for more than two years. The employing NARA office completes and forwards to the personnel security staff NA Form 3016. There is no charge for the investigation; enter "no cost" in Part B, Item 2.

8. Requesting access to information classified under the Atomic Energy Act (also known as Restricted Data and Formerly Restricted Data (or "RD/FRD"), Sensitive Compartmented Information (or "SCI"), or Special Access Program (or "SAP").

Procedures for access to these types of classified information are not outlined in this directive. Contact the NARA PSO for guidance.

9. Temporary security clearances.

If the PSO determines that a nominee is eligible for access to classified information based on an approved investigation, the PSO may grant the nominee temporary access to material classified at a higher level than the clearance level the nominee already has, if such access is necessary to meet a one-time deadline or other emergency situation. The access must not exceed 180 days.

10. Re-investigations.

All individuals holding security clearances are subject to re-investigation every five years. The PSO notifies supervisors of re-investigations that are due for employees working in their areas. The supervisors follow procedures outlined in paragraph 5. After the re-investigation has been completed the supervisor or ISPM must inform the nominee of the results of the re-investigation.

11. Clearance verification.

a. **Certification within NARA.** BX maintains the official records of all security clearances granted to NARA nominees. Supervisors must confirm security clearances with the personnel security staff and should not grant access to classified material to any individual whose clearance status is unknown.

b. **Reassignments within NARA.** When an individual is about to be permanently reassigned from one unit within NARA to another, the supervisor of the gaining office must submit NA Form 3016 to the personnel security staff if the individual will need a security clearance for the new position. Before submitting the form, the supervisor of the unit may verify with the personnel security staff the current level of clearance and whether any cost for reinvestigation will be necessary. A personnel security specialist certifies the clearance on the form and returns a copy to the requesting unit, either immediately or when the reinvestigation has been completed.

c. **Visits by other NARA employees.** Offices receiving visits from NARA cleared individuals outside their own organization must telephone the personnel security staff to

confirm the visitor's clearance. BX provides written verification of clearances upon request.

(1) NARA cleared individuals who require access to classified material at another NARA facility may request personnel security staff to forward their security clearance verification to the director of that NARA facility prior to their visit.

(2) NARA cleared individuals who require access to classified material at another federal agency must submit NARA (NA) Form 6069 (Request to Pass National Security Clearance for External Visit) to BX (Personnel Security) at least two weeks before the planned visit.

d. **Visits by researchers and other cleared individuals from outside NARA.** BX handles, in accordance with procedures in paragraph 3.3 of NARA 202-H1, Classified Information Security Handbook, verification of security clearances for researchers and other cleared individuals from outside NARA who require access to classified information within NARA's control.

12. Required security briefing prior to granting access to classified information.

Nominees must complete Module 1 "Safeguarding Classified Information" in the NARA Learning Management System (LMS) and the NARA Briefing Slides under (Security Management on NARA@Work). After completion of the Module 1 training and the briefing slides:

a. The nominee signs the SF 312, "Classified Information Nondisclosure Agreement," and the ISPM or the supervisor signs as witness;

b. The ISPM or the supervisor then forwards the signed SF 312 and the Module 1 training certificate to the PSO for filing;

c. If a nominee refuses to sign the SF 312 he or she is not granted access to classified information and;

(1) The briefer reports the nominee's refusal to the PSO; and

(2) The PSO is responsible for notifying the nominee's supervisor that the nominee refused to sign.

PART 2 - TERMINATING, SUSPENDING AND REVOKING SECURITY CLEARANCES AND EMPLOYEE RIGHTS

13. Administratively terminating a cleared individual's access to classified information.

Cleared individual's access to classified information shall be administratively terminated if that person:

a. Is reassigned to a non-sensitive position that does not require access to classified information or the work of their current position no longer requires them to have access to classified information;

b. Will be on an unexcused absence from NARA for 30 calendar days or more; or

c. Leaves NARA employment.

14. Reinstating administratively terminated clearances.

Nominees who previously held a security clearance within NARA and whose access was administratively terminated because it was no longer needed may have their clearances reinstated without further investigation, if they have remained employed by NARA and their last investigation was completed within the previous five years. The NARA office that requests the clearance reinstatement completes and forwards NA Form 3016 to the personnel security staff with the words "no cost" entered in Part B, Item 2.

15. Debriefing a cleared individual when their clearance is administratively terminated, suspended or revoked.

Whenever a cleared individual's access to classified information is no longer authorized, that person must attend a security debriefing and must sign a debriefing statement. The debriefing is intended to remind the individual of his or her continuing responsibilities for the protection of classified information.

16. Other reasons for terminating a security clearance.

When NARA officials have an information security concern regarding a cleared individual, they must notify the PSO. The PSO evaluates all the information available and determines whether it is serious enough to warrant a recommendation of suspension or revocation of the clearance. If the PSO determines, and the Deputy Chief Security Officer (DCSO) concurs, the access should be suspended or revoked, the PSO notifies the cleared individual's appropriate first line supervisor and arranges for the cleared individual to be debriefed.

17. Rights of a cleared individual when a security clearance is suspended.

There are no specific appeal rights for suspension of a security clearance. The suspension is a temporary administrative action to immediately prevent an individual's further access to classified information while there is an inquiry into his or her conduct or actions. During the suspension period, a decision will be made to reinstate the clearance or to proceed with the revocation of the clearance, depending on the results of the inquiry. Suspensions normally last approximately 30 working days, but can be extended by the DCSO as appropriate.

18. Ability of the OIG to delay reporting allegations to PSO against a NARA cleared individual that include security clearance implications.

The OIG may delay notification while it investigates the allegations. The PSO should be notified as soon as possible once there is no risk of jeopardizing the investigation, or once the investigation is closed.

19. NARA employee or applicant for federal employment rights when a security clearance is revoked or denied.

NARA employees and applicants are entitled to the process established in section 5.2 of E.O. 12968. A NARA employee or applicant who does not meet the standards for access to classified information is entitled to the following as summarized below:

a. A written explanation of the basis for the conclusion consistent with the national security interests of the United States and other applicable laws;

b. Any documents, records, and reports upon which a denial or revocation is based, upon request and to the extent the documents would be provided if requested under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act (3 U.S.C. 552a), as applicable. These documents must be provided to the employee within 30 days of the date of request. To request these documents and the entire investigative file, the employee must submit:

(1) A letter to the personnel security staff, requesting the address and other information necessary to obtain the OPM investigative file;

(2) A Privacy Act request sent to the NARA Privacy Officer in the Office of the General Counsel (NGC) to obtain NARA files;

c. Information concerning the employee's right to be represented by counsel or other representative at the employee's own expense;

d. The opportunity to reply in writing to the Chief Security Officer (CSO) and to request a review of the determination, within two weeks of receiving notification of the denial or revocation of the security clearance; and

e. Written notice of and reasons for the results of the review if he or she has requested one, the identity of the deciding authority, and written notice of the right to appeal.

20. NARA employee or applicant for federal employment appeal rights if he or she is not satisfied with the results of the procedures outlined in paragraph 19.

a. A NARA employee or applicant may appeal in writing to the Archivist, who appoints a high level *ad hoc* panel.

(1) The panel consists of at least three NARA employees, who hold the same clearance as the clearance that has been denied or revoked, two of whom must be selected from outside the security field and one from BX who does not work in the personnel security office. If necessary, to avoid a conflict of interest or the appearance of a conflict of interest, the Archivist may appoint non-NARA employees to the *ad hoc* panel.

(2) At the discretion of the Archivist, the *ad hoc* panel will issue a final decision on the appeal. The Archivist may personally issue the written decision, based upon recommendations from the *ad hoc* panel. The decision issued must be in writing and is final.

(3) If the appeal is filed by an employee of the Office of Inspector General, the Archivist will consult with the Inspector General in the establishment of the *ad hoc* panel, which may include non-NARA employees. The Archivist's final decision on an appeal by an OIG employee will be made in consultation and agreement with the Inspector General.

b. Any appeal must be submitted within two weeks of any decision under subparagraph 19(e) of this supplement to the CSO who will transmit the appeal to the Archivist; and

c. A NARA employee or applicant who appeals the denial or revocation of a clearance will be provided an opportunity to appear personally and to present relevant documents, materials, and information to the *ad hoc* panel. A written summary or recording of such appearance will be made part of the employee's security file.

d. When the Archivist personally certifies that the appeal process cannot be made available in a particular case without damaging the national security interests of the United States by revealing classified information, the appeal may not proceed, and the Archivist makes the final decision regarding the denial or revocation.

e. The Archivist's power and responsibility under any law or other E.O. to deny or terminate access to classified information in the interests of national security are not limited or affected by any of the procedures in this directive. However, the power and responsibility to deny or terminate access to classified information under any law, or other E.O. without providing the appeals process described above, may be exercised only when the Archivist determines that the ad hoc panel described in subparagraph 20(a) of this supplement cannot be convened in a manner that is consistent with national security as described in subparagraph 20(d) of this supplement. The Archivist's determination is final.

21. Rights of an employee if they believe that their security clearance was revoked or denied in reprisal for making a protected disclosure as defined in the Supplement to NARA 273, Administrative Procedures for Security Clearances.

a. An employee who believes that his or her security clearance was revoked or denied in reprisal for making a protected disclosure may raise this allegation as part of the written reply provided for in paragraph 19(d) of this supplement.

b. If an employee raises an allegation of reprisal for making a protected disclosure in his or her written reply, the CSO will refer the matter to the Inspector General, who will conduct a review to determine whether the revocation or denial of the security clearance was in reprisal for making a protected disclosure. The Inspector General will expeditiously conduct this review and make a recommendation to the Archivist.

c. The Inspector General may recommend that the Archivist reconsider the determination to revoke or deny the employee's eligibility for access to classified information consistent with the national security and with Executive Order 12968 and recommend that the Archivist take other corrective action to return the employee, as nearly as practicable and reasonable, to the position the employee would have held had the reprisal not occurred.

d. The Archivist shall carefully consider the findings and recommendation of the Inspector General. The Archivist will issue a written decision.

e. To the extent authorized by law (including the Back Pay Act), corrective action may include, but is not limited to, reinstatement, reassignment, reasonable attorney's fees, other reasonable costs, back pay and related benefits, travel expenses, and compensatory damages.

f. An employee alleging reprisal for making a protected disclosure who has exhausted the review processes detailed in (a) through (e) may request an external review by a three-member Inspector General panel chaired by the Inspector General of the Intelligence Community. If such a request is made, the Inspector General of the Intelligence Community shall decide, in his or her discretion, whether to convene the External Review Panel, and if so, shall designate two other panel members from the Inspectors General of the following agencies: Departments of State, the Treasury, Defense, Justice, Energy, and Homeland Security and the Central Intelligence Agency. The Inspector General from the agency that completed the initial review shall not be a member of the External Review Panel. The External Review Panel shall complete a review of the claim, which may consist of a file review, as appropriate, within 180 days.

g. If the External Review Panel determines that the individual was the subject of reprisal for making a protected disclosure, the panel may recommend that the Archivist take corrective action to return the employee, as nearly as practicable and reasonable, to the position the employee would have held had the reprisal not occurred and that the Archivist reconsider the employee's eligibility for access to classified information consistent with the national security and with Executive Order 12968.

h. The Archivist shall carefully consider the recommendation of the External Review Panel and inform the Panel and the Director of National Intelligence (DNI) of

what action he or she has taken within 90 days. If the Archivist fails to inform the DNI, the DNI shall notify the President.

PART 3 – DEFINITIONS

22. Definitions. The following terms are used in NARA 273, Administrative Procedures for Security Clearances, and this Supplement:

a. **Access**. The ability or opportunity to obtain knowledge of classified information. Permissible access to classified information requires both a security clearance (matching or above the level of the information sought) and a need to know.

b. **Access with National Agency Check with (Written) Inquiries (ANACI)**. An ANACI is the required initial investigation for nominees who need access to classified information at the Confidential or Secret level.

c. **Administrative terminations**. Terminations of access to classified information effected because the individuals no longer require such access to perform their duties. The determination is final. An administrative termination in no way reflects adversely on the employee whose clearance has been terminated.

d. **Applicant.** As defined in E.O. 12968, "applicant" means a person other than an employee who has received an authorized conditional offer of employment for a position that requires access to classified information. (See Section 1.1(b) of E.O. 12968.)

e. **Classified information.** Information that has been determined pursuant to E.O. 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. See NARA 202 and its Handbook for a description of classified markings.

f. **Collateral security clearance**. Security clearance granted by the NARA Personnel Security Officer (PSO) to nominees for access to classified information at the confidential, secret, or top secret levels.

g. **Electronic Questionnaires for Investigations Processing (e-QIP).** A secure web site that is designed to house all personnel investigations forms. The United States Office of Personnel Management (OPM) requires the use of this data collection tool that allows a user to complete his or her investigative form on-line instead of using a paper form.

h. **Employee.** As defined in E.O. 12968, "employee" means a person, other than the President or Vice president, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts

for or on behalf of an agency as determined by the appropriate agency head. (See Section 1.1(e) of E.O. 12968.)

i. **Information Security Program Manager (ISPM).** An individual and alternate(s) appointed by the head of each NARA component maintaining classified information to act on behalf of the Information Security Officer (ISO) in providing assistance, advice and training to component personnel and to implement the NARA Classified Information Security Program at their location.

j. **National Agency Check with Local Agency Check and Credit (NACLC)**. The NACLC is designed as the initial investigation for contractors at the Confidential and Secret levels. The NACLC also is used to meet the reinvestigation requirement for all individuals (including contractors) who have Confidential or Secret clearances.

k. **Nominee.** Individuals nominated for a security clearance are referred to as "nominees". This includes applicants for Federal employment (defined as "applicants by EO 12968); and all other persons nominated for a security clearance (defined as "employees" by EO 12968).

l. **Protected Disclosure**. A Protected Disclosure is:

(1) A disclosure of information by an employee to a supervisor in the employee's direct chain of command up to and including the head of the employing agency, to the Inspector General of the employing agency or Intelligence Community Element, to the Director of National Intelligence, to the Inspector General of the Intelligence Community, or to an employee designated by any of the above officials for the purpose of receiving such disclosures, that the employee reasonably believes evidences (i) a violation of any law, rule, or regulation; or (ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety;

(2) Any communication described by and that complies with subsection (a)(1), (d), or (h) of section 8H of the Inspector General Act of 1978 (5 U.S.C. App.); subsection (d)(5)(A) of section 17 of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403q); or subsection (k)(5)(A), (D), or (G), of section 103H of the National Security Act of 1947 (50 U.S.C. 403-3h);

(3) The exercise of any appeal, complaint, or grievance with regard to the violation of Section A or B of PPD-19;

(4) Lawfully participating in an investigation or proceeding regarding a violation of Section A or B of PPD-19; or

(5) Cooperating with or disclosing information to an Inspector General, in accordance with applicable provisions of law in connection with an audit,

inspection, or investigation conducted by the Inspector General, if the actions described under subparagraphs (3) through (5) do not result in the employee disclosing classified information or other information contrary to law.

m. **Reciprocity or Reciprocal Exchange**. Employees who previously held a security clearance granted by another Federal agency may be approved for access at NARA if their last investigation was completed within the past five years and they have not retired or otherwise been separated from the Government for more than two years.

n. **Critical sensitive position**. Any position that the occupant of which could bring about by virtue of the nature of the position, a material adverse effect on the national security. For the purposes of this Directive, all positions requiring access to classified information are critical sensitive positions.

PART 4 – RECORDS MANAGEMENT

23. Records Management.

a. BX maintains records as follows:

(1) File no. 312-1 for investigative case files; file no. 312-2 for investigative reports and related documents furnished to NARA by investigative organizations for use in making security determinations; and Records Schedule DAA-0064-2011-0003 for the Security Clearance Tracking System (SCTS). See Privacy Act System Notice, "NARA 24: Personnel Security Files," for additional requirements.

(2) File no. 315, "Classified Information Non-Disclosure Agreements," for nominees' original SF 312s (security briefings and debriefings) and Module 1 training certificates.

(3) File no. 303-2 for copies of position descriptions **not** filed in nominees' investigative case files (i.e, position descriptions for vacant positions).

(4) File no. 314, "Security Violations Files," for inquiries into reported security incidents involving loss, compromise, or unauthorized disclosure of classified information and resulting recommendations for corrective actions.

(5) File no. 258, "Classified Documents Access Request Files," for visit requests and clearance certifications for:

(a) NARA employees and contractors (includes NA Form 6069s); and

(b) Employees of other agencies and organizations who require access to classified information held by NARA.

(6) File no. 649-1, "Credentials Files," for BX credentials (NA Form 6001B).

b. The Learning and Organizational Development Division (HL) is the system owner of the NARA LMS which is the repository for Module 1 of the online "Safeguarding Classified Information" course. All data in the LMS are currently unscheduled and must **not** be deleted until the Archivist of the United States approves disposition authorities.

c. ITP – All records maintained by the ITP Manager are currently unscheduled and must **not** be destroyed until the Archivist of the United States approves disposition authorities. See NARA 242, Insider Threat Program, for further information.

d. OIG – Maintain "Investigative Case Files" (file nos. 1208-1 or 1208-2) as warranted. Follow disposition instructions under file no. 1208-3 for the IG Case Management and Tracking System. See Privacy Act System Notice, "NARA 23: Office of Inspector General Investigative Case Files," for additional requirements.

e. Supervisors – In unofficial personnel files, keep your copies of the SF 52, NA Form 3016, NA Form 6069, and any other records relating to the individual's performance and conduct as a security clearance holder, but **not** any copies of investigative forms. See Privacy Act System Notice, "NARA 22: Employee-Related Files," for additional requirements. Use the file number applicable to your location:

(1) All Federal Records Centers (including Washington National Records Center), National Personnel Records Center, all Field Support Offices (including Washington National Records Center), and all Archival Facilities – File no. 269-1.

(2) All other organizations in DC area and Presidential libraries – File no. 303-1.

f. Volunteer coordinators – In individual volunteer files, keep your copies of requests and related records for a retired NARA employee's continued retention of a security clearance. However, do **not** keep any copies of investigative forms. See Privacy Act System Notice, "NARA 26: Volunteer and Unpaid Student Intern Files," for additional requirements. Use the file number applicable to your location:

(1) All Federal Records Centers (including Washington National Records Center), National Personnel Records Center, all Field Support Offices (including Washington National Records Center), and all Archival Facilities – File no. 1618.

(2) All other organizations in DC area and Presidential libraries – File no. 1605-3.