

National Archives and Records Administration

Transmittal Memo

DATE: December 20, 2016

TO: All Staff

SUBJECT: NARA 273, ADMINISTRATIVE PROCEDURES FOR SECURITY CLEARANCES

Purpose: This directive provides policies and procedures by which National Archives and Records Administration (NARA) officials request, grant, terminate, suspend, and revoke clearances for access to classified national security information at the Confidential, Secret, and Top Secret levels. These policies and procedures are required and/or authorized by several Executive Orders, statutes, regulations, and other authorities, listed in paragraph 273.6.

Background: These revisions reflect changes to NARA's organization structure as well as a new directive style and format.

Available forms:

- NA Form 3016, Personnel Security Action Request and Certification.
- NA Form 6001A, NARA Security Official Credential - Part A.
- NA Form 6001B, NARA Security Official Credential - Part B.
- NA Form 6069, Request to Pass National Security Clearance for External Visit.
- SF 312, Classified Information Nondisclosure Agreement.

Cancelled forms: None.

Cancelled policy: NARA 273, Administrative Procedures for Security Clearances, dated June 21, 2013.

Related policy:

- NARA 202, NARA Classified Information Security Program.
- NARA 242, Insider Threat Program (ITP).

Effective date: This directive is effective upon date of signature.

National Archives and Records Administration

Contact information: For questions on this directive, please contact Paula Ayres (BX) in room 2300, AII; or by telephone at 301-837-1494.

DEBRA STEIDEL WALL
Deputy Archivist of the United States

Attachments

National Archives and Records Administration

NARA 273
December 20, 2016

SUBJECT: ADMINISTRATIVE PROCEDURES FOR SECURITY CLEARANCES

273.1 Policy.

- a. NARA will not grant access to classified information to any individual, unless that individual has a security clearance at the same (or higher) level as the information.
 - (1) This rule applies to all individuals who require access to classified information, including NARA employees, contractors, retired employees, and volunteers; employees, contractors, and volunteers of other Federal agencies; applicants for Federal employment; and former Presidential administration personnel.
 - (2) Supervisors may request a security clearance for, or “nominate”, only those individuals 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. Individuals nominated for a security clearance are referred to as “nominees.”
 - (3) All individuals holding security clearances (“cleared individuals”) must be re-investigated at least every five years. Supervisors must request a re-investigation. Cleared individuals nominated for a re-investigation are also referred to as “nominees”.
- b. NARA follows guidance under 5 CFR 732.101, issued by the United States Office of Personnel Management (OPM).
- c. Nominees are not eligible for a security clearance if they have been convicted as adults in any local, state, Federal, or foreign jurisdictions for any one of the below:
 - (1) Homicide,
 - (2) Sexual assault,
 - (3) Arson,
 - (4) Robbery,
 - (5) Burglary,
 - (6) Aggravated assault,
 - (7) Larceny where property loss exceeds \$1,000 per incident, or

(8) Fraud where property loss exceeds \$1,000 per incident.

d. Nominees are not eligible for a security clearance if they are not United States citizens. Individuals who claim dual citizenship as United States' citizens and another country may be eligible for a security clearance, based on a successful adjudication and freedom from conflicting allegiances.

e. 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) before they are granted access to classified information. Cleared individuals must complete training annually.

f. 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.

273.2 Coverage.

a. This directive covers all NARA officials that request, grant, terminate, suspend, and revoke clearances of nominees for access to classified national security information at the Confidential, Secret, and Top Secret levels, as well as the nominees and cleared individuals themselves.

b. This directive does *not* cover 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 a Special Access Program (or "SAP").

273.3 Responsibilities.

a. The Archivist of the United States (N):

- (1) Performs responsibilities specifically assigned to the position under Executive Order (E.O.) 12968, as amended;
- (2) Commits senior management and resources to the successful implementation of the NARA Personnel Security Program;
- (3) Ensures agency records systems are designed and maintained to safeguard personnel security records;
- (4) Delegates authority to the chief security officer to direct and administer the Personnel Security Program; and

- (5) Delegates authority through credentials (NA Form 6001B, NARA Security Official Credential - Part B) to conduct background investigations of nominees seeking collateral clearances.
- b. Executive Business Support Services serves as the Chief Security Officer (CSO), and:
 - (1) Oversees the NARA Personnel Security Program, as the senior agency official in accordance with E.O. 12968, section 6.1(a);
 - (2) Commits monetary and other resources necessary for the successful implementation of the NARA Personnel Security Program;
 - (3) Appoints, in writing, the NARA Personnel Security Officer (PSO) and further delegates to him or her, the authority to implement and manage the NARA Personnel Security Program on a full-time basis; and
 - (4) Serves as the “Senior Agency Official” as defined in E.O. 13526, section 5.4 (d).
- c. Director, Security Management Division (BX) serves as the Deputy Chief Security Officer (DCSO), and advises and assists the CSO with oversight and administration of the NARA Personnel Security Program.
- d. Information Security Officer (ISO) in BX directly oversees the NARA Personnel Security Program and staff to ensure integration with all other NARA security programs.
- e. The Personnel Security Officer (PSO), under the direction of the ISO --
 - (1) Develops and implements policies, procedures, standards, and requirements for determining the initial and continuing review of personnel for access to classified information, and manages the personnel security program;
 - (2) Assists the NARA Chief Security Officer and NARA Information Security Officer with inquiries into reported security incidents involving the actual or suspected loss, compromise, or unauthorized disclosure of classified information and recommends corrective actions to be taken;
 - (3) Coordinates with the Office of Human Capital, Talent Acquisition Division (HT) and Strategy, Analysis, & Automation Division (HS), as well as supervisors to ensure staff have the proper critical sensitivity requirement in position descriptions;
 - (4) Administers the personnel security program, gathers background information, monitors on-going investigations, evaluates investigative

findings to assess eligibility for a security clearance, and maintains and controls access to investigative case files;

- (5) Initiates review of an individual's security clearance eligibility when HTS indicates that an employee with a security clearance has sustained misconduct or has been placed on indefinite suspension, and advises the Office of Human Capital (H) of adverse determinations;
- (6) Provides the Insider Threat Program (ITP) with details concerning any change in personal information, such as a change in name or residence, foreign contacts, arrests, illegal drug involvement, financial delinquencies, mental health counseling, alcohol counseling, civil court actions, and subversive activities while holding a security clearance;
- (7) Notifies the ITP of all requests for new security clearances and any suspensions, revocations, or terminations of security clearances for NARA staff;
- (8) Provides the ITP with copies of all foreign travel documents and foreign contact reports;
- (9) Upon request, provides the ITP with access to personnel security files;
- (10) Acts as the NARA liaison and key official with other Federal agencies and departments to monitor changes in national policies, procedures, and developments in the personnel security programs;
- (11) Provides training, advice, and guidance to those individuals specifically involved in the personnel security program, including other BX personnel, information technology program managers, administrative officers, contracting officer representatives, and management at all levels, at NARA locations nationwide;
- (12) Prepares recurring and special reports on the NARA Personnel Security Program for internal or external release;
- (13) Periodically assesses the effectiveness of the NARA Personnel Security Program and makes policy and procedural adjustments and policy recommendations to the Strategy and Performance Division (MP) as necessary;
- (14) Ensures appropriate measures are taken to safeguard personnel security investigative records; and

- (15) Manages the accountability and issuance of NARA Security Official credentials (NA Form 6001B, NARA Security Official Credential - Part B).

f. Executives, Staff Directors, Office of the Inspector General (OIG), and supervisors

- (1) Oversee implementation of the NARA Personnel Security Program for facilities and activities under their authority by:
 - (a) Committing monetary and other resources necessary for compliance with NARA Personnel Security Program policies and procedures;
 - (b) Ensuring the accuracy of position descriptions reflecting the requirement for access to classified information for their subordinates;
 - (c) Ensuring that their information security program managers (ISPM) or other individuals approved by the PSO conduct security briefings and debriefings for nominees granted security clearances;
 - (d) Ensuring nominees in their organizations have the appropriate security clearances for access to the level of classified material likely to be encountered in the course of their work;
 - (e) Including briefings on NARA information security requirements and security awareness training required by NARA 202, NARA Classified Information Security Program;
 - (f) Coordinating with the PSO (before consideration of a current employee or applicant for assignment to a critical sensitive position requiring access to classified information) to conduct a preliminary financial history inquiry to determine if there are any financial issues that prevent the nominee from obtaining a security clearance;
 - (g) Submitting requests for security clearances (NA Form 3016, Personnel Security Action Request and Certification) to the personnel security staff, with the appropriate justification;
 - (h) Validating with HTS that position descriptions accurately reflect the level of access to classified information that is required for a nominee or cleared individual assigned to that position description;

- (i) Advising the PSO immediately of any change in a cleared individual's need for access to classified information, including reassignment to another unit or contract within NARA, changes in position duties, pending resignation, transfer to another agency or termination of employment and placement on leave without pay or administrative leave exceeding a continuous 30 days;
 - (j) Reporting to the PSO any personnel security issues or concerns that may have an impact on a cleared individual's ability to maintain a security clearance such as:
 - (i) Arrests by civilian authorities;
 - (ii) Failure or inability to live within one's means or meet financial obligations which may indicate a lack of judgment or unwillingness to follow rules and regulations;
 - (iii) Enrollment in a substance abuse program;
 - (iv) Failure of a random or directed urinalysis screening test;
 - (v) Problems in the individual's personal life with respect to medical or emotional difficulties that may impair judgment, reliability or trustworthiness (see paragraph 273.5 for a list of indicators or behaviors which supervisors should use in making a determination to report concerns to the PSO); or
 - (vi) Any reported allegations of workplace violence to include threats or intimidation; and
 - (viii) Any allegation of criminal activity by a cleared individual.
- g. BX personnel security staff:
- (1) Requests, investigates, and adjudicates investigations for security clearances;
 - (2) Denies, grants, administratively terminates, administratively reinstates, suspends, or revokes security clearances;
 - (3) Processes visit requests and clearance certifications for NARA employees to other NARA facilities and other Federal agencies;
 - (4) Receives visit requests, maintains, and safeguards records related to investigations and security clearances of NARA employees and contractors;

- (5) Advises H of the names of employees in critical sensitive positions with access to classified information that should be subject to the Drug Testing Program;
 - (6) Maintains and certifies security clearance information on employees of other agencies and organizations requiring access to classified information held by NARA; and
 - (7) Conducts financial history inquiry to determine if there are any financial issues that could negatively impact a nominee's eligibility for a security clearance.
 - (8) Verifies with HT the appropriate sensitivity level of the position.
- h. Staffing and Recruitment Branch (HTS):
- (1) Provides the personnel security staff with information on nominees selected for appointment, promotion, or reassignment to a critical sensitive position requiring access to classified information within 14 business days.
 - (2) Notifies the PSO in writing when an employee with a security clearance has sustained misconduct or has been placed on indefinite suspension.
- i. Insider Threat Program (ITP) creates and maintains a centralized analysis, reporting, and response capability to support continued evaluation of personnel security information.
- j. NARA nominees and cleared individuals:
- (1) Complete and provide to the personnel security staff in a timely manner all investigative forms, certificates of information security training completion or other documents and information required to request a security clearance;
 - (2) Report to the personnel security staff any changes in personal information, such as a change in name or residence, foreign contacts, arrests, illegal drug involvement, financial delinquencies, mental health counseling, alcohol counseling, civil court actions, and subversive activities while holding a security clearance;
 - (3) Complete mandatory briefings and training as described in section 8.4 of the NARA 202-H1, Classified Information Security Handbook, while holding a security clearance;
 - (4) Comply with all security regulations and requirements for the protection of classified information to which they have access; and

- (5) Are sensitive to, and report to the local Information Security Program Manager (ISPM) and the ITP, espionage indicators such as unusual amount of overtime related to working with classified material; unexplained reproduction of or access to classified material; unreported foreign travel by cleared individuals with specific clearances that should report the travel; or other suspicious activity that may have an impact on the protection of classified material. For further guidance, see paragraph 8.4 of the NARA 202-H1, Classified Information Security Handbook.

273.4 Procedures.

Procedures for requesting, granting, terminating, suspending, and revoking clearances for access to classified national security information at the Confidential, Secret, and Top Secret levels, and employees' rights, may be found in the attached supplement. Definitions of terms used in this policy and records management instructions are included in the supplement.

273.5 Behaviors indicating emotional difficulties in individuals

a. Supervisors should consider the following behaviors when determining whether problems in an individual's personal life may impact their ability to maintain a security clearance.

- (1) Depression/withdrawal.
- (2) Talk of severe financial problems.
- (3) Increased use of alcohol and/or illegal drugs.
- (4) Unexplained increase in absenteeism; vague physical complaints.
- (5) Noticeable decrease in attention to appearance and hygiene.
- (6) Resistance and overreaction to changes in policy and procedures.
- (7) Repeated violations of agency policies.
- (8) Increased severe mood swings.
- (9) Noticeably unstable, emotional responses.
- (10) Explosive outbursts of anger or rage without provocation.
- (11) Increasingly frequent mentions of problems at home.
- (12) Escalation of domestic problems into the workplace.

- b. The above list is not comprehensive. Supervisors should report concerns to the PSO as soon as possible if any behaviors or indicators lead them to believe that a person should not have access to classified information.

273.6 Authorities.

- a. 50 U.S.C. §§ 403, et seq, National Security Act of 1947, as amended;
- b. 42 U.S.C. 2011 Atomic Energy Act of 1954, as amended;
- c. E.O. 10450, as amended, Security Requirements for Government Employment (April 27, 1953);
- d. E.O. 12968, as amended, Access to Classified Information (August 2, 1995);
- e. E.O. 13526, Classified National Security Information (December 29, 2009);
- f.. E.O. 12829, as amended, National Industrial Security Program, (January 6, 1993);
- g. E.O. 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust (January 16, 2009);
- h. E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, June 30, 2008);
- i. E.O. 13587, Structural Reform To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011;
- j. Presidential Policy Directive/PPD-19, Protecting Whistleblowers with Access to Classified Information (“PPD-19”);
- k. 5 CFR Part 732, National Security Positions, revised (January 1, 2011);
- l. 32 CFR Part 2001, Classified National Security Information (June 25, 2010), and Part 2004, National Industrial Security Program Directive No. 1 (April 6, 2010, as amended);
- m. Department of Defense (DoD) Manual 5220.22-M, National Industrial Security Program Operating Manual (NISPOM) (February 28, 2006); and
- n. [OPM Adjudication Guidelines](#).

273.7 Public release.

Unlimited. This directive is approved for public release.