Transportation Security Administration

TSA MANAGEMENT DIRECTIVE No. 2800.71
PRE-EMPLOYMENT INVESTIGATIVE STANDARDS FOR TSA NON-SCREENER EMPLOYEES AND CONTRACTORS

1. **PURPOSE:** This directive establishes the Transportation Security Administration (TSA) pre-employment investigative standards for non-screener employees and contractors who will have access to TSA facilities, sensitive information or information technology resources.

2. **SCOPE:** This order applies to all TSA non-screener employees, contractors, subcontractors, vendors, and others who have access to TSA facilities, sensitive information or information technology resources.

3. **AUTHORITIES:**

   A. Public Law 107-071, The Aviation and Transportation Security Act.

   B. Department of Homeland Security (DHS) Management Directive No. 11020.1, Issuance of Photo Control Media.

   C. DHS Management Directive No. 11030.1, Physical Protection of Facilities and Real Property.

   D. DHS Management Directive 11042, Safeguarding Sensitive But Unclassified (For Official Use Only) Information.

   E. Executive Order 10450, Security Requirements for Government Employment, as amended, dated April 27, 1953.

   F. Executive Order 13958, as amended, Classified National Security Program, dated March 28, 2003.

   G. Executive Order 12829, National Industrial Security Program, dated January 6, 1993.

   H. Title 5, Chapter 73 of the U.S. Code, relating to suitability, security and conduct.

   I. 49 Code of Federal Regulations Part 1520, Protection of Sensitive Security Information.

   J. 5 Code of Federal Regulations, Part 736, Personnel Investigations.

4. **DEFINITIONS:**

   A. Access: The ability to enter and/or pass through an area or a facility; or the ability or authority to obtain information, monetary or material resources. In relation to classified information, the ability, authority, and/or opportunity to obtain knowledge of such information.

   B. Access National Agency Check and Inquiry (ANACI): Consists of a National Agency Check (NAC); employment/self-employment/unemployment coverage (five-year inquiry); education

(five-year highest degree inquiry); residence (three-year inquiry); reference contacts (inquiry); law enforcement checks and/or record (five-year inquiry), and credit check.

C. Classified Information: Official information or material that requires protection in the interest of National Security and is classified for such purpose by appropriate classification authority in accordance with the provisions of Executive Order 12958, Classified National Security Information, as amended, or any successor authority.

D. Contract: A mutually binding legal relationship obligating the seller to furnish supplies or services (including construction) and the buyer to pay for them. It includes all types of commitments that obligate the Government to expenditure of appropriated funds and that, except as otherwise authorized, are in writing. In addition to bilateral instruments, contracts include, but are not limited to, awards and notices of awards; job orders or task letters issued under basic ordering agreements; letter contracts; orders, such as purchase orders, under which the contract becomes effective by written acceptance or performance; and bilateral contract modifications. This includes reimbursable agreements and interagency agreements.

E. Contracting Officer (CO): A person with the authority to enter into, administer, and/or terminate contracts, and make related determinations and findings. The term includes certain authorized representatives of the CO acting within the limits of their authority as delegated by the CO. The CO maintains a strong relationship with the COTR.

F. Contracting Officer's Technical Representative (COTR): A person who supports the CO in managing a contract and/or business arrangement. The COTR provides technical direction within the confines of the agreement, monitoring performance, ensuring requirements are met within the terms of the contract, and maintains a strong relationship with the CO. The CO and COTR work together to ensure that contract requirements are clearly communicated to the contractor.

G. Consultant/Contractor: An expert or consultant to a Government 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 persons who act for or on behalf of an agency, as determined by the appropriate agency head, based on a defined, properly executed business agreement.

H. For Official Use Only (FOUO) and Sensitive But Unclassified (SBU) Information: Unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the National interest. Information impacting the National Security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958, "Classified National Security Information," as amended, or its predecessor or successor orders, is not to be considered FOUO or SBU. FOUO and SBU information is not to be considered classified information.

I. Information Technology Resources: Computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software,

computer software, and software programs.

J. National Agency Check (NAC): Consists of records searches of the Office of Personnel Management (OPM) Security/Suitability Investigations Index (SII); Federal Bureau of Investigation (FBI) Identification Division/Headquarters investigation files; FBI National Criminal History Fingerprint Check; Defense Clearance and Investigations Index (DCII); and other sources, as necessary, to cover specific areas of a subject's background.

K. National Agency Check and Inquiries and Credit (NACIC): Consists of a NAC; employment/self-employment/unemployment coverage (five-year inquiry); education (five-year highest degree inquiry); residence (three-year inquiry); reference contacts (inquiry); law enforcement checks (five-year inquiry); and credit check.

L. National Crime Information Center (NCIC) Record Check: The NCIC is a computerized index of criminal justice information (i.e., criminal record history information, fugitives, stolen properties, and missing persons). It is available to Federal, state, and local law enforcement and other criminal justice agencies and is operational 24-hours a day, 365 days a year.

M. National Industrial Security Program (NISP): A single, integrated, cohesive security program established by Executive Order 12829 to protect classified National Security information provided to or developed by contractors and applicable to all Executive Branch departments and agencies.

N. Sensitive Security Information (SSI): Information as defined in 49 Code of Federal Regulations Part 1520.5.

O. Staff-like Access: Unescorted access to TSA-owned or controlled facilities, information systems, security systems or products containing SSI or SBU information.

P. TSA Non-Screener Employee: Persons employed directly by TSA in any non-screener position.

5. RESPONSIBILITIES:

A. The Office of Transportation Vetting and Credentialing (TVC) shall:

(1) Receive and process forms to initiate required investigations on TSA non-screener employees and contractor employees.

(2) Adjudicate the results of personnel security investigations to determine suitability and advise the CO, COTR, Office of Security, and other offices on a need-to-know basis of the adjudication.

(3) Conduct or arrange for additional investigation, when necessary, to resolve suitability issues.

(4) Provide non-screener TSA employees an opportunity to respond to information developed during an investigation prior to taking any unfavorable action based on that information.

(5) Notify the Office of Security and the employing office in writing about any employee or the CO and COTR about any contractor employee found unsuitable for access to TSA facilities, sensitive information or information technology resources.

(6) Maintain records on personnel security investigations and maintain personnel security files on TSA employees and, as necessary, on contractor employees.

B. The Office of Security shall:

(1) Determine, in consultation with COs and COTRs, which contracts require personnel security investigation of the contractor and/or contractor employees.

(2) Assist the Office of Acquisition in developing appropriate language for inclusion in solicitations, contracts, and agreements.

(3) Notify the employing office or the CO and COTR, as appropriate, in writing to deny access to those employees and contractor employees who are found unsuitable for access to TSA facilities, sensitive information or information technology resources.

(4) Coordinate, as appropriate, with the Office of Human Resources (OHR), the employing office and TVC, or, if a contractor employee, CO/COTR-appropriate action to take whenever reasonably creditable information is received that appears to raise a question about a TSA employee or contractor employee's suitability.

(5) Provide the CO and COTR with all DHS and TSA security directives that the contractor needs to fulfill security responsibilities under the contract.

C. TSA CO shall:

(1) In consultation with the COTR and program office, ensure that all proposed solicitations and contracts are reviewed to determine whether contractors or contractor employees will have access to TSA facilities, sensitive information or information technology resources.

(2) Ensure that whenever a solicitation, contract, or agreement requires investigation of any contractor employees, the document contains language sufficient to achieve this objective in an orderly and expeditious manner. The document shall also contain language allowing TSA to deny a contractor employee access to TSA facilities, sensitive information, or information technology resources if the Office of Security or TVC determines that the person is unsuitable.

(3) Ensure that the Office of Security and the COTR are notified whenever there is a change in the status (e.g., replaced, extended, defaulted, terminated) of an existing contract where contractor employees are subject to investigation.

(4) Ensure that the Office of Security, the TVC and COTR are notified of any reasonably credible information received that may raise a question about the suitability of a contractor employee.

(5) Ensure that the Physical Security Division, Office of Security, is advised if a contract in which there will be access to TSA facilities, sensitive information or information technology resources, will be completed in 90 days or less.

D. TSA COTR:

(1) Prior to the CO issuance of the solicitation prospective, COTRs shall ensure coordination with the Office of Security and TVC to determine any applicable personnel security investigative requirements. These requirements also apply to any proposed agreements with outside parties, other than contractors, that would result in non-TSA personnel having such access.

(2) Ensure that contractors submit for their employees (including prospective subcontractor employees), to the TVC, completed forms and information for each person subject to investigation, as required by the applicable contract.

(3) Ensure that the Office of Security is notified whenever a contractor employee has completed work under the contract or leaves his or her position with the contractor.

(4) Ensure that required, completed forms for investigation of contractor employees are submitted to TVC prior to the contractors or subcontractor personnel receiving access to the facilities, sensitive information or information technology resources that make them subject to investigation. The office for which the contracted work is being done shall assist the COTR as necessary.

(5) Ensure that any appropriate action directed by the Office of Security or TVC is taken whenever a question has arisen regarding the suitability of a contractor employee. Appropriate action may include, but is not limited to, temporarily denying the contractor employee access to TSA facilities, sensitive information or information technology resources pending resolution of the issue(s) raising a question of suitability.

(6) Upon direction of the Office of Security, ensure that appropriate action is taken when the Office of Security or TVC determines that a contractor employee is unsuitable for access to TSA facilities, sensitive information or information technology resources. Appropriate action may include excluding the contractor employee from working on any aspect of the TSA contract.

E. The OHR shall:

(1) Ensure that all TSA vacancy announcements state that employment is contingent upon a favorably adjudicated personnel security investigation enabling the granting of a security clearance.

(2) Ensure that required personnel security investigations have been initiated or completed in accordance with this directive prior to making any commitment to hire.

(3) Instruct applicants who are tentatively offered a non-screener TSA position provide a completed Standard Form 86 (SF86), *Questionnaire for National Security Positions*, two Standard Form 87 (SF87) fingerprint cards completed by the applicant and signed by the person taking the fingerprints, an Optional Form 306 (OF306), *Declaration for Federal Employment*, and TSA Form 2201, *Fair Credit Reporting Act Form* to their recruitment officer/personnel specialist.

6. POLICIES & PROCEDURES:

A. Non-Screener TSA Employees:

(1) The ANACI is the minimum investigative standard for TSA non-screener employees.

(2) Prospective TSA non-screener employees new to the Government must have a favorably adjudicated fingerprint-based criminal history record check and credit check prior to a hiring commitment being made. These record checks may be conducted prior to or concurrently with the ANACI investigation.

(3) TSA non-screener employees entering on duty whose prior employer was a U.S. Government agency and who have no break in service may be granted access to TSA facilities, sensitive information or information technology resources upon verification by their prior agency that a NAC-equivalent or higher investigation had been performed within the last three years. If a NAC-equivalent investigation is unavailable, they must meet the standard defined in section 6A(2).

B. TSA Screener Employees Moving From a Public Trust Position to a National Security Position:

(1) A TSA employee moving from a public trust to a National Security position shall complete a SF86, *Questionnaire for National Security Positions*, two SF87 fingerprint cards completed by the applicant and signed by the person taking the fingerprints, an OF306, *Declaration for Federal Employment*, and TSA Form 2201, *Fair Credit Reporting Act Form* and submit the documents to their recruitment officer. If the employee has received the required investigation for the National Security position, no reinvestigation is required unless the time elapsed since the previous investigation necessitates updating, or unless information disclosed on the newly completed SF86 or other special circumstances justify additional investigation.

C. Contractors, Subcontractors, Vendors and Others:

(1) The NACIC is the minimum investigative standard for TSA contractor employees requiring staff-like access to TSA facilities on a recurring basis (i.e., more than 14 days per year). Prior to being given access to TSA facilities, sensitive information or information technology resources, contractors must have a favorably adjudicated fingerprint-based,

criminal history record check and credit check. These record checks may be conducted prior to or concurrently with a NACIC investigation.

(2) Contractors, subcontractors, vendors and others who require temporary unescorted facility access, but who do not require access to TSA information technology resources or sensitive information, require a fingerprint-based criminal history record check in lieu of a NACIC. Disqualifying offenses for unescorted access under this provision are listed in 49 U.S.C. Section 44936(b)(1)(B).

(3) A company that participates in the NISP may, through their CO, certify in writing that its employees have met the standard defined in sections 6C(1) or 6C(2) of this directive.

(4) Forms required to complete a NACIC include: SF86, *Questionnaire for National Security Positions*, two FD 258 fingerprint cards completed by the applicant and signed by the person taking the fingerprints, and TSA Form 2201, *Fair Credit Reporting Act*.

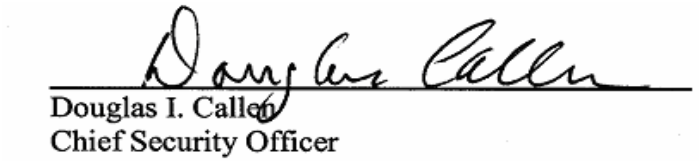
D. Waivers and Exceptions:

(1) Operational, physical, or unforeseen circumstances may prevent or preclude the implementation in a timely manner of some of the requirements of this directive. In such cases a waiver or exception to the stated requirements may be requested. The waiver or exception request must be in writing and addressed to the Chief Security Officer and identify a compelling reason for issuance of a waiver or exception. Access will not be granted under the waiver/exception process until the waiver/exception is approved by the Chief Security Officer.

7. EFFECTIVE DATE & IMPLEMENTATION:

This policy is effective immediately upon signature.

APPROVAL



Douglas I. Callen
Chief Security Officer

12/20/04
Date

Filing Instructions:	File with Office of Security Management Directives
Effective Date:	December 20, 2004
Review Date:	December 20, 2005
Distribution:	TSA Assistant Administrators, Office Directors
Point Of Contact:	Daniel Boyce, 571-227-2487