Approved On: April 23, 2013

DOJ POLICY STATEMENT

CONTRACTOR SECURITY REQUIREMENTS

PURPOSE: This Policy Statement establishes security requirements and policies, including minimum investigative requirements, for all contract personnel who require access to Department of Justice (DOJ) information, information technology (IT) systems, and/or DOJ facilities or space. This Policy Statement further sets forth the responsibilities of the component Security Programs Managers (SPM) and Justice Management Division (JMD) Staff Directors regarding contractor security.

SCOPE: This Policy Statement applies to all DOJ components, and all DOJ contractors requiring access to information, IT systems, and/or DOJ facilities or space, except for the following:

a. Contractors who work in foreign countries in U.S. embassies that only have access to the facility and do not have access to DOJ information or IT systems (facility access requirements are implemented by the Department of State's Regional Security Officer at each U.S. embassy);

b. Experts and consultants who are hired into DOJ appointments covered by DOJ Order 1200.1. (Such individuals should be processed under the requirements set forth in DOJ Order 2610.2B); and

c. Classified contractors processed through the National Industrial Security Program.

Visitors who do not work under a contract or provide services but require access only to DOJ space are outside the scope of this Policy Statement.

ORIGINATOR: Justice Management Division (JMD), Security and Emergency Planning Staff (SEPS)

CATEGORY: (I) Administrative, (II) Security and Emergency Preparedness

AUTHORITY: 5 C.F.R. Part 731; Executive Orders 13467 and 13488; Homeland Security Presidential Directive-12; DOJ Orders 2600.2D and 2640.2F

CANCELLATION: Employment Eligibility Verification (I-9 Form) Contractors Policy Amendment Memorandum, dated April 30, 1998; Contractor Personnel Security Guidance, dated September 15, 1998; Background Checks for Contractor Access to DOJ Facilities Policy Memorandum, dated January 29, 2001; Department of Justice Residency Requirement-Amendment Policy Memorandum, dated December 10, 2002; Contractor Escorted Access to Department of Justice Facilities Policy Memorandum, dated August 11, 2004; the Contractor Escorted Access to Department of Justice Facilities Policy Memorandum, dated August 8, 2005; and Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification Card Interim Policy Memorandum, dated August 14, 2009.

DISTRIBUTION: This Policy Statement is distributed electronically to all components listed in the Scope Section of this Policy Statement as well as posted to the DOJ Directives electronic repository (SharePoint).

APPROVED BY: James L. Dunlap
James L. Dunlap
Department Security Officer

ACTION LOG

All DOJ directives are reviewed, at minimum, every five years and revisions are made as necessary. The action log records dates of approval, recertification, and cancellation, as well as major and minor revisions to this directive. A brief summary of all revisions will be noted. In the event this directive is cancelled, superseded, or supersedes another directive, that will also be noted in the action log.

Action	Authorized by	Date	Summary
Initial Approval	Department Security Officer	**April 23, 2013**	This Policy Statement reflects updated security requirements and policies for contract personnel and conforms with the format of guidance issued under DOJ's Directives Management Program.

TABLE OF CONTENTS

GLOSSARY OF TERMS

DEFINITIONS

Term	Definition
Contract Employee	May also be referred to as "contractor." A non-federal employee who works on a DOJ contract/contractual instrument or provides a service of any kind for the DOJ (e.g., Justice Federal Credit Union, Justice Occupational Health Organization, Federal Express, United Parcel Service, and Airborne Express personnel). Task Force Officers who require access to DOJ information, IT systems and/or unescorted access to DOJ facilities or space are included under this definition and must comply with this Policy Statement.
DOJ Information	DOJ Information is information owned by, produced by or for, or under the control of the DOJ, both electronic and hard copy, and may be sensitive or non-sensitive. Sensitive information, also referred to within the DOJ as Limited Official Use (LOU) information, is information of a sensitive, proprietary, or personal nature, which must be protected against release to unauthorized individuals (to include the public) and requires safeguarding controls. Examples of LOU information include informant and witness information, Grand Jury information, and component proprietary information. Non-Sensitive DOJ information is any other DOJ information, an unauthorized release of which may have limited potential for adversely affecting the Department's mission. For purposes of this Policy Statement, DOJ information does not include information that is publicly available, such as certain annual reports, publications, and press releases made public by the Department.
DOJ Space	All DOJ facilities or office space, including building lobbies or hallways, as well as unoccupied areas such as renovation/construction space, stairwells, and elevators.
Fitness Determination	A determination of fitness based on character and conduct for work for or on behalf of the Government as a contract employee.
Five-Year Scope Background Investigation (BI)	An investigation consisting of a National Agency Check (NAC), personal interviews of subject and sources, written inquiries, and record searches covering specific areas of the subject's background during the most recent five years, and a credit search covering seven years.

Intermittent Contractors	Contract employees having access to DOJ information, IT systems, and/or DOJ facilities or space for a maximum of one day per week, regardless of the duration of the required intermittent access.
JSTARS	The Justice Security Tracking and Adjudication Record System (JSTARS) is an automated tracking system used by DOJ components to process and track personnel security activities and information. JSTARS enables DOJ components to manage their personnel security programs and enables the Department-level personnel security office to conduct oversight in order to ensure compliance with the various government-wide regulations, policies, and mandates.
Long-term Contractors	Contract employees having access to DOJ information, IT systems, and/or DOJ facilities or space for six months or more.
Moderate Risk Background Investigation (MBI)	An investigation which consists of a NAC, a personal subject interview, written inquiries (five year coverage for employment, education and law enforcement, and three year coverage for residence), and a credit search covering seven years.
National Agency Check (NAC)	A required component in all background investigations consisting of searches of the OPM Suitability/Security Investigations Index, Federal Bureau of Investigation (FBI) Criminal History Records, FBI Headquarters investigation files, Defense Clearance and Investigations Index (DCII), and other sources as necessary to cover specific areas of a subject's background.
National Agency Check and Inquiries (NACI)	An investigation consisting of a NAC, written inquiries and record searches covering specific areas of an individual's background during the past five years.
National Agency Check with Law and Credit (NACLC)	An investigation consisting of a NAC, law enforcement checks for the past five years (inquiry or records), and a credit search for the past seven years.
National Security Information (NSI)	Information requiring protection against unauthorized disclosure (marked Confidential, Secret, or Top Secret when in documentary form, to indicate its classified status), pursuant to Executive Orders 12958 and 12968. Also known as classified information.
Periodic Reinvestigation (PRI)	Type of reinvestigation required for high risk public trust positions consisting of a NAC and subject interview.
Public Trust Position	A position where action or inaction by the person occupying the position could affect the integrity, efficiency and effectiveness of the service. Public Trust positions consist of three risk level designations:

	High Risk, Moderate Risk, and Low Risk. See Appendix A for risk designation criteria.
Reinvestigation (RI)	An update investigation based on position risk and/or position sensitivity level to determine continued employment and/or NSI access eligibility.
Short-term Contractors	Contract employees having access to DOJ information, IT systems and/or DOJ facilities or space for fewer than six consecutive months.
Security Programs Manager (SPM)	An individual, regardless of title, with the delegated responsibility for the management and coordination of all security programs within a DOJ component.

ACRONYMS

Acronym	Meaning
AAG/A	Assistant Attorney General for Administration
BI	Background Investigation
CFR	Code of Federal Regulations
DOJ	Department of Justice
DSO	Department Security Officer
JMD	Justice Management Division
OPM	Office of Personnel Management
PIV	Personal Identity Verification
SEPS	Security and Emergency Planning Staff

I. Delegated Authority

Security Programs Managers (SPMs) have delegated authority to maintain their component contractor security programs. The duties and functions set forth in this Policy Statement may be re-delegated within the component. However, the SPM is accountable for compliance with the DOJ's established security requirements for component contractor security programs. In addition, the fact that a delegation has been granted does not waive the Department Security Officer's (DSO) authority to make any determinations that have been delegated.

II. Responsibilities of SPMs and JMD Staff Directors

For the purposes of this paragraph, JMD Staff Directors have the same responsibilities with respect to their offices as component SPMs, with the exception of paragraph II.F. However, the DSO is the official SPM for JMD and retains security approval authority and overall responsibility for the JMD Contractor Program.

A. **Establishment of Access Procedures.** The SPMs are responsible for establishing procedures within their components to ensure that no contractor is allowed access to DOJ information, IT systems, and/or unescorted access to DOJ facilities or space until the appropriate background investigation or pre-appointment background investigation waiver, meeting the requirements set forth in this Policy Statement, has been conducted and favorably adjudicated.

B. **Security Requirements for Contracts.** After the SPM has made the risk designation, the SPM is responsible for providing the Contracting Officer with the appropriate contractor personnel security screening requirements (including waiver requirements, if appropriate) and investigative requirements to be included in any contractual instrument used for obtaining services. The contractor personnel security screening requirements must be based on the risk designation of the task(s).

C. **Certification of Security Requirements.** The SPM is responsible for providing the Contracting Officer with written certification that the personnel security requirements of the contract are adequate to ensure the security of Departmental operations, information and personnel. The SPM is also responsible for ensuring that this written certification is provided to the Contracting Officer prior to release of the Request for Proposal (RFP) or other similar solicitation.

D. **Monitoring.** The SPM is responsible for monitoring and ensuring that the contractor personnel security requirements are adhered to throughout the life of the contract. This

must be accomplished through periodic review of the contractor files to ensure the appropriate checks/investigations (including waiver requirements) required by each contract are being completed and properly documented.

E. **Contractor Roster.** The SPM is responsible for maintaining up-to-date information on active contract employees. The information must be correctly recorded and reviewed for accuracy on a monthly basis.

F. **Contract Expirations and Transfers.** The SPM is responsible for proper handling of a contractor's security record upon expiration of a contract and the record must reflect the separation date. If the contractor transfers to another DOJ contract/contractual instrument, the gaining office/component must immediately notify the appropriate personnel security office and provide any new or updated paperwork that is required as a result of the transfer. An example of updated paperwork is a new OBD-232 form, Access Card/Credential Request form.

G. **Safeguarding Requirements.** The SPM must safeguard the contractor background investigation files pursuant to the Privacy Act, including any applicable requirements contained in DOJ system of records notices for personnel security investigations and clearance records.

H. **Reinvestigations.** The SPM is responsible for ensuring that contract employees whose investigations are five years or older undergo the appropriate reinvestigation. The SPM is also responsible for ensuring that contract employees working on renewed contracts whose investigations are five years or older are reinvestigated. Reinvestigation requirements are set forth in this document.

I. **JSTARS.** The SPM is responsible for ensuring that all contract employees' personnel security actions are properly processed and documented using JSTARS.

III. Reciprocity

The SPM must accept any previous federal government background investigation if 1) it is current (investigations are considered current if completed within the last five years) and favorably adjudicated, 2) it meets or exceeds the level of investigation required for the DOJ contractual instrument, and 3) there has been no continuous (not cumulative) break in federal contract/service employment of more than two years.

The SPM must obtain a written certification of the reciprocated background investigation information, to include the date of favorable adjudication and/or fitness determination, from the adjudicative agency/DOJ component or OPM's Central Verification System (CVS).

A component may not establish additional investigative or adjudicative requirements. Specifically, no duplicative forms, including completion of a new or updated security questionnaire form, or investigative checks that were completed as part of the investigation, shall be required. The only exception is for unique suitability/fitness considerations based on a component's mission that may require additional, not duplicative, forms or processes such as the Drug Enforcement Administration's drug use statement. Any request for exception must be submitted to the DSO for initial consideration and who will, if applicable, forward the request for exception approval to the Suitability Executive Agent, a member of the Suitability and Security Clearance Performance Accountability Council established by E.O. 13467 of June 30, 2008.

A. **Granting Reciprocal Recognition of Prior Determinations.** SPMs making fitness determinations must grant reciprocal recognition to a prior favorable fitness determination or adjudication when:

   1. the gaining agency uses criteria for making fitness determinations equivalent to suitability standards established by OPM;

   2. the prior favorable fitness determination or adjudication was based on criteria equivalent to suitability standards established by the OPM; and

   3. the individual has had no continuous (not cumulative) break in federal contract/service employment of more than two years since the favorable determination was made.

B. **Denying Reciprocal Recognition of Prior Determinations.** SPMs making fitness determinations may deny reciprocal recognition of a prior favorable fitness determination or adjudication when:

   1. the new position requires a higher level of investigation than previously conducted for that individual;

   2. during the course of the security approval process, an SPM obtains new information as a result of gathering routine information (such as responses to questions raised during interviews or information obtained during reference checks) that calls into question the individual's fitness based on character or conduct; or

3. the individual's investigative record shows conduct that is incompatible with the core duties of the new contract position. A "core duty" is a continuing responsibility that is of particular importance to the relevant covered position or the achievement of an agency's mission. Core duties will vary from agency to agency and from position to position, and the identification of core duties is the responsibility of each DOJ Component.

C. **Breaks in Federal Contract Employment Service.** If the contractor has a current background investigation (investigations are considered current if completed within the last five years) that meets or exceeds the level of investigation required for the DOJ contract but has had a continuous (not cumulative) break in federal contract employment of more than two years, he/she must complete an updated e-Application and undergo the investigation required by the relevant risk level/position designation. A review of the e-Application, credit check (required for all risk level position determinations above level 1), and an FBI fingerprint check are required prior to working on a DOJ contract.

IV. Contractor Access to NSI

Refer to the Security Program Operating Manual (SPOM), or its successor, for additional guidance regarding classified contracts/contractors.

A. **Required Coordination through the Security and Emergency Planning Staff (SEPS).** Contracts requiring access to NSI must be coordinated through the SEPS, Office of Information Safeguards and Security Oversight, in accordance with National Industrial Security Program guidelines.

B. **Verification of Background Investigations**. Background investigations conducted for the Defense Industrial Security Clearance Office (DISCO) and DISCO's adjudicative decisions must be verified through the appropriate personnel security system (i.e. CVS, Joint Personnel Adjudication System (JPAS) or their successors) and copies of clearance verifications must be kept in contractors' JSTARS security records. In addition, if database checks are unclear as to eligibility or type of clearance, then a written certification should be requested from the contract company's Facility Security Officer.

C. **Special Conditions for Interim or Temporary Clearance.** The principles of reciprocity do not require acceptance of an interim or temporary clearance. In order for the DOJ gaining component to accept an interim or temporary clearance, the gaining component must complete and document the following:

1. Review the existing (current) security questionnaire form that was submitted for the interim or temporary clearance; and,

2. Conduct a new FBI fingerprint check and, if warranted, a credit check.

3. If questionable or derogatory information surfaces as a result of the security questionnaire review or fingerprint and credit checks, the component must discontinue review of the proposed contractor and wait for DISCO to complete its investigation and/or adjudication and grant the final clearance.

V. Escorted Access to DOJ Space (No Access to DOJ Information)

A. Escorting Visitors While in DOJ Facilities and/or Space.

1. A DOJ contractor with a valid DOJ HSPD-12 Personal Identification Verification Card (PIV Card) or approved AEGIS "green" badge and who is authorized to be in DOJ facilities and/or space is not required to be escorted. An individual who does not have a valid PIV Card or approved AEGIS card must be escorted in DOJ facilities and/or space.

2. A contract employee may serve as an escort provided they 1) have a valid DOJ HSPD-12 PIV Card, and 2) have a current background investigation.

3. Escorting means ensuring that the escorted individual is continuously accompanied and monitored while within DOJ facilities and/or space in a manner sufficient to maintain awareness of the escorted individual's activities at all times.

4. The contractor assuming escort responsibility is responsible for the escorted individual until responsibility is either turned over to another approved escort, or the escorted person departs the DOJ facility and/or space.

5. In the event the escorted individual departs from the escort, exhibits any suspicious behavior, and/or fails to comply with the escort procedures, the escort shall:

    a. Attempt to gain compliance via verbal request; if this fails, the escort must immediately notify their facility security provider of the location of the incident, direction of travel, and description of the situation.

6. Contractor escorts may be subject to appropriate sanctions including revocation of escort privileges, or other sanctions in accordance with applicable law and Department regulations for any knowing, willful, or negligent act that results in the individual being escorted obtaining unauthorized access to DOJ information, IT systems, and/or unescorted access to DOJ facilities or space.

B. Screening Requirements for Contractors Being Escorted.

1. Contractors cleared for escorted access are not authorized to access any DOJ information or IT system.

2. For escorted contractors in Level V high risk buildings (as defined in the Physical Security Criteria for Federal Facilities (PSC), An Interagency Security Committee (ISC) Standard, dated April 12, 2010, and the Facility Security Level Determinations for Federal Facilities (FSL), An ISC Standard, dated February 21, 2008), such as the Robert F. Kennedy Main Justice Building (RFK Building), a National Crime Information Center (NCIC)[1] check must be conducted. The NCIC check will be effective for 90 days. Sponsors should reassess the need for facility access after 90 days to determine whether to request continued escorted access for another 90 days, clear the contractor for unescorted access, or terminate the contractor's facility access altogether. Absent an extension or some other action by the sponsor, the escorted access approval will be automatically deactivated after 90 days.

3. Where the capability exists, an NCIC check will be conducted for all escorted contractors accessing DOJ space during the non-duty hours of 6:00 p.m. to 6:00 a.m., to include weekends and holidays. The NCIC check will be effective for 90 days at which time a reassessment must be made using determination criteria stated in paragraph V.B.2. above.

4. The contractor may be subject to additional personal screening, such as a magnetometer and search of personal belongings, upon each entry to DOJ space based on the security recommendations contained in the PSC and FSL.

[1] NCIC is a nationwide computerized information index of documented criminal justice information concerning crime and criminals of nationwide interest and a locator-type file for missing persons. An unfavorable NCIC check does not mean that the contract employee should be terminated from the Company or that the contractor will not be eligible to work on a DOJ contract in the future. It simply means that access to any DOJ facility or space cannot be granted without making a favorable final determination based on the results of a FBI Fingerprint Check. Therefore, it is the Component's responsibility to initiate the FBI Fingerprint Check in these instances.

C. **Restriction.** Contractor escorted access cannot be used to circumvent the approval process described in paragraph VI. For example, a contractor who has not undergone the approval process described in paragraph VI cannot attend a meeting as a visitor if DOJ information is being discussed at the meeting. A contractor who needs ongoing access cannot be escorted daily instead of submitting paperwork to undergo the personnel security approval process.

VI. Minimum Requirements for Contractor Access to DOJ Information, IT Systems, and/or Unescorted Access to DOJ Facilities or Space

For a quick information reference, see Appendix B

A. **Position Risk Designations.** Components are in the best position to analyze and determine the risk level designations and the corresponding level of background investigations required in their contracts beyond the minimum standards. The decision is based primarily on the contract services to be performed, including the risk level of information to be accessed, and the level of government supervision that will be available. Therefore, the SPM is responsible for determining the risk level for each contractor position within the component. (See Appendix A for risk designation criteria and minimum background investigations.) The risk level must be based on an overall assessment of the damage that an untrustworthy contractor could cause to the efficiency or the integrity of Departmental operations. In making the decision, component SPMs should consider:

1. Whether the contractor will have access to a DOJ IT system;

2. Location where the contractor will be performing his/her duties (for example, work performed in the Attorney General's conference room is potentially more sensitive than work done in the Great Hall); and

3. The contractor's duties, responsibilities and access in relation to Department employees in similar positions.

B. **Conditions for Approval.** All contractor applicants being processed and approved for unescorted access to DOJ space and/or access to DOJ information or IT systems must meet the following DOJ requirements:

1. **Residency Requirement.** The Residency Requirement ensures an adequate background investigation can be completed. This requirement applies to both U.S. citizens and non-U.S. citizens.

   a. Immediately prior to gaining unescorted access to DOJ space or access to DOJ information, contractors must have:

      1) Resided in the U.S. for three out of the last five years (not necessarily consecutive years); or

      2) Worked for the U.S. in a foreign country as either an employee or contractor in a federal or military capacity for three out of the last five years; or

      3) Been a dependent of a federal or military employee or contractor in a foreign country for three out of the last five years.

   b. Waiver of Residency Requirement. Only the DSO, or designee, can approve Residency Requirement waivers. The approval must be obtained prior to the proposed contractor beginning work or providing any service to the DOJ. The Head of the Component, or designee, must submit a written request to the DSO and provide the completed BI for review and adjudication by the DSO's staff. The BI must provide sufficient coverage to determine the subject's activities in the foreign country. Approval is based on the completed and favorably adjudicated BI. Each waiver determination is made on a case-by-case basis.

2. **Citizenship.**

   a. All contractors who are U.S. citizens must provide proof of citizenship prior to working on a DOJ contract.

   b. Any non-U.S. citizen working in the U.S. and assigned to a DOJ contract must have been admitted legally to the U.S. Acceptable Department of Homeland Security Credentials to prove immigrant status or employment authorization are listed in Form I-9, Employment Eligibility Verification.

   c. Non-U.S. citizen contract employees may be considered for unescorted access to DOJ space and/or access to DOJ information if they are citizens of a country on the Allied Nations list.[2]

[2] The Allied Nations list is included in the Treasury and General Government Appropriations

d. Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems, unless a waiver has been granted by the Head of the Component, as required in DOJ Order 2640.2F. Prior to the Head of the Component's approval/disapproval of the request, components shall submit all waiver requests for concurrence by the DSO and the DOJ Chief Information Officer (CIO). All questions regarding DOJ Order 2640.2F, including those regarding waivers, should be directed to the DOJ CIO.

e. The requisite investigation, based on position risk designation, must be conducted on all non-U.S. citizen contractors who will have either short-term or long-term unescorted access to DOJ space and/or access to DOJ information.

f. Components must adjudicate a non-U.S. citizen's background investigation according to the standards found in title 5 CFR part 731 and to OPM-issued supplemental guidance.

g. Dual Citizenship. DOJ components may use U.S. citizen contractors who hold dual citizenship with a foreign country; however, how the contractor has obtained or exercised his or her dual citizenship status will be considered by the SPM in making a security approval.

3. **Homeland Security Presidential Directive 12 (HSPD-12) and Federal Information Processing Standard 201 Revision 1 (FIPS 201-1) Pre-employment Requirements.**[3] All contractors will be subject to the identity proofing, registration,

---

Act. Updated copies of this list can be obtained by referencing that Act. The Department of State also publishes allied countries information by treaty on its U.S. Collective Defense Arrangements website (http://www.state.gov/s/l/treaty/collectivedefense/).

[3] Homeland Security Presidential Directive-12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors," establishes a common standard for identification badges issued by federal departments and agencies to employees and contractors who need physical access to federally controlled facilities and/or logical access to federally controlled information systems. Federal Information Processing Standard Publication 201 Revision 1 (FIPS 201-1) entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors," implements HSPD-12.

and issuance requirements outlined in FIPS 201-1 and the pre-employment requirements outlined below.

a. Contractors must present two forms of identification in original form prior to commencement of work on a DOJ contract and badge issuance (acceptable documents are listed in Form I-9, Employment Eligibility Verification, and at least one document must be a valid State or Federal government-issued picture ID);

b. Contractors must appear in person at least once before a DOJ official or an official of a trusted contract company (i.e., has a facility security clearance) who is responsible for checking the identification documents. This identity proofing must be completed any time prior to commencement of work under this contract and badge issuance, and must be documented by the DOJ or contractor official; and

c. In order to reduce identity fraud, the identity proofing, registration, and badge issuance process must adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a badge without the cooperation of another authorized person.

d. Long-term Contractors. In addition to those requirements in paragraph VI.B.3.(a-c) above, contractors in this category must undergo the requisite background investigation, the minimum of which shall be an OPM NACI investigation.

    1) Long-term Contractor Background Investigation Pre-Employment Waiver Requirements for all Position Risk Levels. The pre-employment background investigation waiver requirements for contractors in this category are the initiation of the appropriate investigation, a favorable review of the security questionnaire, favorable FBI fingerprint results, a DOJ-555 form if an SF 85P security questionnaire is completed and a favorable credit report, if required,[4] a waiver request memorandum from the Head of the Component or designee that includes 1) name of Component, 2) company name, 3) position title (optional), 4) position risk level, 5) type of investigation initiated, 6) investigation schedule date and case number, and 7) a request for an HSPD-12

[4] For contractors in position risk levels above level 1, a favorable credit check is required as part of the pre-employment waiver package. If a component determines a credit check is necessary for its position risk level 1 contractors and an SF 85 security questionnaire is completed, then a DOJ-555 form is required.

PIV Card, or equivalent ID badge, if required. The contractor must have met the DOJ Residency Requirement as described in paragraph VI.B.1. A PIV Card/ID badge, which allows unescorted access to DOJ facilities or space and access to DOJ information and IT systems, may be issued following approval of the above waiver requirements.

2) PIV Card/ID badge validation will occur once the investigation is completed and favorably adjudicated. If the investigation results so justify, ID badges issued under the pre-employment waiver will be suspended or revoked.

e. Short-term Contractors. Contract employees in this category are subject to those requirements in paragraph VI.B.3.(a-c) above. The requisite investigation does not need to be initiated except in the case of non-U.S. citizen contract employees. See paragraph VI.B.2.e.

1) Pre-Employment Waiver Requirements for Short-Term Contractors. The pre-employment background investigation waiver requirements for contractors in this category are a favorable review of the security questionnaire form, favorable FBI fingerprint results, a DOJ-555 and favorable credit report, if required,[5] a waiver request memorandum from the Head of the Component or designee that includes 1) name of Component, 2) company name, 3) position title (optional), 4) position risk level, 5) the duration of the appointment, and 6) the component's acceptance of risk for the contractor's access to DOJ facilities or space and information and IT systems. The contractor must have met the DOJ Residency Requirement as described in paragraph VI.B.1. A request for a temporary ID badge, if required, must be submitted with the pre-employment waiver package.

2) An ID badge, which allows unescorted access to DOJ facilities or space, and access to DOJ information, may be issued following approval of the above waiver requirements. The ID badge will expire six months from the date of issuance.

3) The short-term security approval process can only be used once for a short-term contractor in a twelve-month period. This will ensure that consecutive short-term contractors are not used to circumvent the full identity proofing process. For example, if a contractor requires daily access for a three or four-week period, this contractor would be cleared according to the above short-

[5] See footnote 4.

term requirements. However, if a second request is submitted for the same contractor within a twelve-month period for the purpose of extending the initial contract/contractual instrument or service regardless of the length of extension, or for employment under a totally different DOJ contract/contractual instrument or service, this contractor would now be considered long-term and must be cleared according to the long-term requirements as stated in this Policy Statement.

f. Intermittent Contractors. Intermittent contractors are an exception to the short-term requirements stated in VI.B.3.e. Contract employees needing access to DOJ information, IT systems, and/or DOJ facilities or space for a maximum of one day per week, regardless of the duration of the required intermittent access must be escorted. (See paragraph V. for escort procedures.) An example of an intermittent contractor would be a water delivery contractor who delivers water one time each week.

1) If a component requests unescorted access to DOJ facilities or space, or any access to DOJ information or IT systems for an intermittent contractor, the pre-employment background investigation waiver requirements that apply to short-term contractors are required. See paragraph VI.B.3.e.

2) If an intermittent contractor is approved for unescorted access, the contractor will be issued a daily badge. The daily badge will be issued upon entrance into a DOJ facility or space and must be returned upon exiting the same facility or space.

3) If an intermittent contractor is approved for unescorted access, the approval will not exceed one year. The contractor will need to be re-approved each year. Re-approval consists of a minimum of an NCIC check.

VII. Access to DOJ Information

A contract employee who will only need access to DOJ information and will not be required to access DOJ facilities or IT systems, must meet the requirements listed in paragraph VI, however an ID badge will not be issued.

VIII. Adjudication

A. **For Access to DOJ Information or IT Systems.** Background investigations conducted on contract employees that require access to DOJ information or IT systems must be adjudicated according to the OPM's suitability criteria published at 5 CFR Part 731.202 and to OPM-issued supplemental guidance.

B. **For Unescorted Access to DOJ Facilities or Space.** Background investigations conducted on contract employees that only require unescorted access to DOJ facilities or space, and no access to DOJ information or IT systems, must be adjudicated using the basic fitness determination criteria stated in OPM's memorandum to the Heads of Departments and Agencies entitled "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12, dated July 31, 2008."

C. **Reporting Final Adjudication.** The SPM or a designee must report the final adjudication determination of each background investigation to OPM within 90 days of the date of the completed investigation as required by E.O. 10450.

D. **Nondiscrimination in Adjudication.** The DOJ does not discriminate on the basis of race, color, religion, national origin, sex, gender identity, age, disability, genetic information status as a parent, sexual orientation, marital status, or political affiliation in granting DOJ access security approvals for contract employees.

IX. Waiver Approval Authority

Only the DSO may waive any contractor security requirement.

APPENDIX A

Risk Designations and Minimum Background Investigations

The following criteria should be used as additional guidance in determining the appropriate risk levels:

High Risk:

1. Those sensitive positions that have the potential for exceptionally serious impact on the integrity and efficiency of the DOJ and involve duties especially critical to the DOJ or a program mission with broad scope of policy or program authority, such as:
   a. Attorney positions;
   b. Law enforcement personnel;
   c. Policy development or implementation;
   d. Higher level management assignments;
   e. Independent spokespersons or non-management positions with authority for independent action; and/or
   f. Positions that include the planning, direction, and implementation of a computer security program; the direction, planning, and design of a computer system, including the hardware and software; privileged users, including database, system, and application administrators; or, access to a system during its operation or maintenance that invokes a high risk of grave damage or the potential of significant personal gain.
2. The minimum background investigation required for High Risk positions is a five year scope Background Investigation (BI) and the five year reinvestigation required is a Periodic Reinvestigation (PRI). The Standard Form (SF) 85P, Questionnaire for Public Trust Positions, is required.

Moderate Risk:

1. Those sensitive positions that have the potential for moderate to serious impact on the integrity and efficiency of the DOJ. Duties involved are very important to the DOJ or program mission with significant program responsibility or delivery of services, such as:
   a. Assistance with policy development and implementation;
   b. Mid-level management duties/assignments;
   c. Position with authority for independent or semi-independent action;
   d. Delivery or service positions that demand public confidence or trust;
   e. IT positions of a lesser degree of risk than that required for High Risk positions;
   f. Freedom of Information/Privacy Act duties; and/or
   g. Positions that require access to Grand Jury information.

2. The minimum background investigation required for Moderate Risk positions is a Moderate Background Investigation (MBI) and the five year reinvestigation required is a National Agency Check with Law and Credit (NACLC). The SF-85P, Questionnaire for Public Trust Positions, is required.

Low Risk (Non-sensitive):

1. Low Risk (Non-sensitive) positions are those which have limited potential for adversely affecting the DOJ's mission, such as:
   a. Positions that are not in direct support of the above positions; and
   b. IT positions not falling into one of the above positions.
   These positions do not have access to sensitive information.
2. The minimum background investigation required for Low Risk positions is a National Agency Check and Written Inquiries (NACI) and the required five year reinvestigation is also a NACI. The SF-85, Questionnaire for Non-Sensitive Positions, is required.

APPENDIX B

Contractor Security Requirements Matrix
Risk Designation Level – Requisite Investigations

PUBLIC TRUST POSITIONS						
RISK LEVEL DESIGNATION	RISK LEVEL	SF FORM REQUIRED			INITIAL BACKGROUND INVESTIGATION (BI) REQUIRED	REINVESTIGATION (RI) REQUIRED*
		85	85P	85PS		
High Risk	6		X	X**	BI***	PRI
Moderate Risk	5		X	X**	MBI	NACLC
Low Risk****	1	X			NACI	NACI

* All Reinvestigations will be conducted every five years.

** Applies to positions previously approved by the Office of Personnel Management (OPM).

*** Five-year scope BI.

**** When initiating an investigation for a Low Risk (Risk Level 1) position, the OPM requires that an Optional Form 306, Declaration for Federal Employment, be submitted with the paperwork.

Note: A Foreign National Relatives or Associates Statement must be included in all investigation packages where a non-U.S. citizen is listed on the security questionnaire form.

APPENDIX C

Additional Resources

- Federal Information Processing Standard Publication 201-1
- Department of Homeland Security, U.S. Citizenship and Immigration Services, Form I-9 (Rev. 08/07/09 or any future revision), Employment Eligibility Verification
- Office of Personnel Management memorandum entitled Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12, dated July 31, 2008
- Physical Security Criteria for Federal Facilities, An Interagency Security Committee (ISC) Standard, dated April 12, 2010
- Facility Security Level Determinations for Federal Facilities, An ISC Standard, dated February 21, 2008.