*A pedestrian change has been made to the directive and appears in blue. – 2/29/2011

FEDERAL DEPOSIT INSURANCE CORPORATION

DIRECTIVE SYSTEM

TYPE AND NUMBER	
Circular 1610.2	
CONTACT	TELEPHONE NUMBER
Tommie Barnes	703-562-2749
DATE	
January 28, 2010	
DATE OF CANCELLATION *(Bulletins Only)*	

TO: All Employees

FROM: Arleas Upton Kea, Director
Division of Administration

SUBJECT: Personnel Security Policy and Procedures for FDIC Contractors

1. Purpose

To revise FDIC personnel security policy and procedures for contractors.

2. Revision

FDIC Circular 1610.2, Security Policy and Procedures for FDIC Contractors and Subcontractors, dated August 1, 2003, is hereby revised and superseded.

3. Applicability

This circular applies to all Contracting Officers and all other Acquisition Services Branch (ASB) personnel, Oversight Managers (OMs), Technical Monitors (TMs), and other employees involved in the contracting process.

4. Background

The regulation 12 CFR Part 366 entitled “Minimum Standards of Integrity and Fitness for an FDIC Contractor,” sets forth requirements regarding conflicts of interest, ethical responsibilities, and use of “confidential information” as defined in 12 USC 1822, by contractors seeking to perform services on behalf of the FDIC. The regulation incorporates requirements to ensure that contractors performing services under FDIC contracts meet minimum standards of integrity and fitness.

5. Policy

The integrity and fitness requirements apply to all contractors seeking to perform services on behalf of the FDIC. In addition, all contractor personnel who will have long term access to FDIC facilities, sensitive information, or Information Technology Resources, must meet minimum security standards required by regulation. This policy shall not apply to intermittent vendors who access FDIC facilities on an infrequent, and generally

Policy (cont'd)

unscheduled basis, and do not require access to sensitive information (i.e. equipment repair, delivery personnel, etc.). These vendors should not be processed under this circular, but must be continuously and attentively escorted, kept under visual surveillance, and work only during normal business hours. Building maintenance, repair and custodial workers may require security checks consisting of fingerprint checks to allow unescorted access to FDIC space.

Provisions of this policy may be waived based on the operational needs of the FDIC and upon the request of an FDIC Division Director and the concurrence of the Associate Director, Corporate Services Branch.

6. Authorities

12 CFR Part 366 entitled "Minimum Standards of Integrity and Fitness for an FDIC Contractor"

Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS 210) entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors"

7. Definitions

Terms specific to this circular are defined below:

a. **Background Investigations (BI**). Pertains to various types of investigations conducted by the U.S. Office of Personnel Management (OPM) for the FDIC.

b. **Break in Employment**. A period of over 60-days in which contractor personnel have not been assigned to an FDIC task, such break may require additional security processing upon the individual's return to an FDIC task with the same or another contractor.

c. **Company Clearance**. A generic term that describes an investigatory process the Security and Emergency Preparedness Section (SEPS) completes on contractor companies to ensure they meet minimum Integrity and Fitness standards as set forth by the FDIC. These may include checks of various on-line databases such as Lexis/Nexis, Dun and Bradstreet, and the General Services Administration's Debarred and Suspended Bidders List.

d. **Contractor**. An individual, corporation, partnership, joint-venture, or other third party entity that enters into a contract with FDIC to provide goods or services.

Definitions (cont'd)

e. **Contracting Officer**. The FDIC representative with delegated authority to enter into and legally bind, administer and terminate contractual instruments on behalf of the FDIC.

f. **Contractor Personnel**. All employees of a Contractor who perform under an FDIC contract. These employees include key and non-key personnel.

g. **Key Personnel**. Contractor personnel that are deemed essential and critical to the performance of the contract and who are contractually required to perform by the Key Personnel contract clause.

h. **Long Term**. Having access to FDIC facilities, information technology systems, or sensitive information for more than six months.

i. **Oversight Manager (OM)**. An FDIC employee nominated by the Program Office, and appointed by the Contracting Officer, whose responsibility it is to monitor and evaluate contractor performance under an FDIC contract.

j. **Personally Identifiable Information (PII)**. Any information about an individual maintained by FDIC which can be used to distinguish or trace that individual's identity, such as their full name, home address, E-mail address (non-work), telephone numbers (non-work), Social Security Number (SSN), driver's license/state identification number, employee identification number, date and place of birth, mother's maiden name, photograph, biometric records (e.g., fingerprint, voice print), etc. This also includes, but is not limited to, education, financial information (e.g., account number, access or security code, password, personal identification number), medical information, investigation report or database, criminal or employment history or information, or any other personal information which is linked or linkable to an individual.

k. **Preliminary Approval**. A generic term that describes a process the SEPS completes on contractor personnel to ensure they meet minimum Integrity and Fitness standards as set forth by the FDIC. These may include checks of Federal Bureau of Investigation (FBI) fingerprint criminal records, review of personnel security questionnaires, credit reports provided by the three major credit reporting agencies, and other internal FDIC resources.

Definitions (cont'd)

l. **Risk Level**. An evaluative classification designation assigned to contracts or contract labor categories based on duties performed that have the potential for affecting the integrity, efficiency, and/or effectiveness of the Corporation's mission, and when misused, may diminish public confidence.

m. **Sensitive information**. Any information, the loss, misuse, or unauthorized access to or modification of which could adversely impact the interests of FDIC in carrying out its programs or the privacy to which individuals are entitled. It includes the following:

(1) Information that is exempt from disclosure under the Freedom of Information Act (FOIA) such as trade secrets and commercial or financial information, information compiled for law enforcement purposes, personnel and medical files, and information contained in bank examination reports (see FDIC Rules and Regulations, 12 C.F.R. Part 309, for further information);

(2) Information under the control of FDIC contained in a Privacy Act System of Record that is retrieved using an individual's name or by other criteria that identifies an individual (see FDIC Rules and Regulations, 12 C.F.R. Part 310, for further information);

(3) PII about individuals maintained by FDIC that if released for unauthorized use may result in financial or personal damage to the individual to whom such information relates.

(4) Information about insurance assessments, resolution and receivership activities, as well as enforcement, legal, and contracting activities.

n. **Subcontractor**. An individual, corporation, partnership, joint-venture, or other third party entity that has entered into a contract with an FDIC contractor to perform work on behalf of FDIC.

o. **Technical Monitor**. An FDIC employee nominated by the Program Office, and appointed by the Contracting Officer, whose responsibility it is to assist the OM in monitoring and evaluating contractor performance under an FDIC contract.

p. **Vendor**. Usually service sector personnel who access FDIC facilities on an infrequent and generally unscheduled basis (e.g., no more than three times weekly).

8. General Responsibilities

a. **Personnel Security Unit (PSU)**. The PSU is a group within SEPS that is responsible for establishing and implementing contractor personnel security policy, which includes conducting integrity and fitness evaluations, granting security approval, conducting company clearances, and ensuring appropriate background investigations are conducted on contractor personnel. The PSU is also responsible for processing potentially disqualifying information discovered during the SEPS integrity and fitness evaluation. Final determinations of contractor eligibility are coordinated by the PSU through the Contracting Law Unit, Legal Division.

b. **Office of Inspector General (OIG)**. Records of any improper activities detected should be maintained and be subject to OIG review at any time.

c. **Division of Information Technology (DIT**). Establishes Security and Access Control policies and procedures for FDIC Information Technology Resources (IT).

d. **Oversight Managers (OM) and Technical Monitors (TM):** are responsible for managing all aspects of contractor security as defined in this Circular, which includes requesting contractor access to FDIC facilities and IT resources. OMs and TMs must quality control all security requests to ensure accuracy, completeness, and legibility of the forms prior to submitting to PSU. **Note**: **All forms must be signed and dated within the previous 60 days**. In addition, the OM/TM must carefully review all forms before sending them to PSU for issues which may cause concern such as criminal history, financial difficulties, or issues from prior employment. The PSU should be consulted immediately if the OM review reveals derogatory or potentially disqualifying information such as criminal or dishonest conduct, intentional false statement, deception or fraud, alcohol abuse, Illegal use of controlled substances, or any regulatory bar or debarment which prevents the lawful assignment of the person to the contract in question (See 12 CFR 366).

e. **Contracting Officers**. Contracting Officers are responsible for ensuring all solicitations for services include all applicable Security documents and clauses required in this circular and under the APM. Further, Contracting Officers are required to obtain necessary security forms from the contractor and to request Company Clearance from the PSU on the successful contractor(s).

9. Pre-Award Security Procedures

a. **Contractor Risk Level Designation**. The Program Office representative responsible for the solicitation shall establish one of the following risk levels for contracts or contractor job categories as part of the planning phase for those contracts whose personnel will have **long term** access to FDIC facilities, sensitive information, or Information Technology Resources:

(1) **Low Risk (LR)** positions involve duties with limited relation to the Corporation's mission and have little effect on the efficiency of the Corporation's operations or programs.

(2) **Moderate Risk (MR)** positions involve duties of considerable importance to the Corporation or its program mission with significant program responsibilities and/or delivery of customer services to the public (e.g., assistants for policy development and implementation; mid-level management assignments; non-management positions with authority for independent or semi-independent action; or positions that demand public confidence or trust).

(3) **High Risk (HR)** positions involve duties that are critical to the Corporation or its program mission, with a broad scope of policy or program authority (e.g., policy development and implementation; higher level management assignments; independent spokesperson; or non-management positions with authority for independent action).

The Program Office representative responsible for the solicitation may use one of two methods to determine risk levels:

(1) By Labor Category. The Program Office can compare the description of the proposed contractor labor categories for the contract with the job responsibility examples contained in the risk level matrix *(See Attachment A)*. Background investigations will then be conducted accordingly. This is the recommended practice to ensure contractor personnel assigned to positions with varying levels of risk under one contract are subject to the appropriate investigation.

(2) By Contract. The Program Office representative may assign a risk level for an entire contract by comparing the work required in the contract with the job responsibility examples contained in the risk level matrix *(See Attachment A)*. All contractors assigned to the contract will have a background investigation conducted appropriate for that risk level. The risk level(s) will be established in the solicitation with all of the required security requirements for the prospective offerors to follow. This method should only be

Pre-Award Security Procedures (cont'd)

used when the Program Office Representative can verify that all personnel performing under the contract are assigned to positions with the same level of risk.

The Program Office representative will document the results of the pre-solicitation risk level determination by using the Contractor Risk Level Record (Attachment B) and coordinate those results with the appropriate Division Information Security Manager (ISM). Once the ISM concurs with the levels, the Program Office representative will provide the assigned level(s) to the Contracting Officer in the Requirements Package.

The Contracting Officer will ensure the assigned risk level(s) are included in the solicitation package. The Contracting Officer will provide a copy of the draft solicitation to the PSU.

b. **Company Clearances**. The Contracting Officer is responsible for ensuring all Solicitations (Requests for Proposals or Requests for Quotations) for services include the **form FDIC 1600/07**, Background Investigation Questionnaire for Contractors (See Attachment D.) Contracting Officers shall ensure that the required Company Clearance forms are included in solicitations and provided by offerors in their proposals. The Contracting Officer shall provide completed Company Clearance forms for the successful contractor to the PSU prior to award. Company Clearance must be granted before contract award. However, if an award is urgent, it may be made contingent upon the outcome of the Company Clearance. The OM shall closely monitor the contractor's performance if a contingent award is made and the Contracting Officer will ensure that the Company Clearance is completed as soon as possible following the award.

c. **Key Personnel Integrity and Fitness Checks** will be conducted on contractor personnel identified in the Key Personnel Clause who will not have direct operational duties under the task. Forms FDIC 1600/10 (Attachment E) and 1600/04 (Attachment C) must be submitted with the Company Clearance request. Key Personnel that are expected to perform operational tasks under the contract should be processed as outlined in subparagraph 10.a.(2).

10. Post-Award Security Procedures

a. **Post Award Preliminary Approval Requests**

(1) No later than five (5) calendar days after award, the contractor will provide the Oversight Manager with a list of all contractor and subcontractor personnel proposed on a new contract and identify any that have a current or otherwise valid background investigation conducted by the U.S Government.

(2) Each contractor and subcontractor employee proposed to work on the contract shall complete the following security forms and be fingerprinted, **regardless of whether they have an existing background investigation conducted by the U.S. Government**. (Unless they meet the exception outlined in subparagraph 10.a.(5).)

(a) **FDIC 1600/04**, Background Investigation Questionnaire for Contractors Personnel and Subcontractors

(b) **Form FDIC 1600/10,** Notice and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681, et. seq.

(c) **Standard Form 85P** Background Investigation Questionnaire (See Attachment G.)

(3) **Fingerprinting**

(a) Preferably, fingerprints should be taken at FDIC locations with the capability. They can either be manually rolled using an FDIC provided FBI Form **FD 258** Fingerprint Card with the special FDIC Overprint **USFDIC20Z** in the ORI Block, or electronically taken. Electronic fingerprints are only available at a limited number of FDIC Offices. The OM will make the necessary arrangements for the contractor to be fingerprinted.

(b) Alternatively, fingerprints may be taken at local law enforcement agencies or commercial vendors. The applicant should be provided with (two) FD 258 Fingerprint Cards to increase the likelihood of obtaining legible prints. Once the prints are taken, the contractor must submit both cards to the OM. The OM must review the cards to determine if they meet standards prior to submitting to SEPS. Failure to get legible prints may render them unclassifiable and may delay the security approval process.

Post-Award Security Procedures (cont'd)

(c) Commercial vendors and some local law enforcement agencies may perform fingerprinting services for a fee, any costs associated with such services must be borne by the contractor. **Electronic prints cannot be accepted from these sources**.

(4) **Preliminary Approval**

Once the security forms have been completed by the contractor personnel, they should be forwarded to the OM for review and quality control. The OM shall complete a **FDIC Form 1600/13 Personnel Security Action Request** (Attachment F) for each contractor personnel and identify any that have a current or otherwise valid background investigation conducted by the U.S. Government. The OM shall forward the entire package to the PSU:

The PSU will:

(a) Review forms for accuracy and completeness;

(b) Conduct the integrity and fitness checks to include criminal records and credit checks; and

(c) Based on a favorable result of the above checks, the PSU will provide the OM with written notification of the Preliminary Approval. At this point the contractor will be authorized to start work. The preliminary approval process should take approximately 3 to 5 business days to complete once all of the required information has been received by the PSU.

Individuals will not be permitted to begin work (to include access to FDIC facilities and IT systems) until the preliminary approval is granted by SEPS.

(5) **Contractor Personnel Transfers, Reactivations, and Departures**

The OM is responsible for obtaining the appropriate background investigation forms and submitting requests to the PSU for all Contractor Personnel transfers. In general, contractor personnel that have security approval for one contract should not have to submit all the original documentation if they are assigned to another contract. It is imperative that the OM/TM coordinate such transfer with the PSU prior to allowing contractor personnel to perform. Inter-contract transfers can be approved expeditiously if the following conditions are met: previous approval was granted within the last 24-months; and there was no break in employment in excess of 59-days. If these conditions are

Post-Award Security Procedures (cont'd)

met, the OM shall provide current and complete forms FDIC 1600/13 and 1600/04 to the PSU. The PSU will review the existing security file and provide the OM with a preliminary approval notification.

Reactivation is required when contractor personnel have a break in employment in excess of 60 days. The OM shall provide completed forms 1600/04 and 1600/13 to the PSU. The PSU will review the existing security file, conduct additional checks if necessary, and provide the OM with a preliminary approval notification. **If these conditions are not met, the OM should follow the procedures outlined in subparagraph 10.a.(2), unless an exception is requested and approved by SEPS.**

The OM/TM is also responsible for providing the PSU with the names of departing contractor personnel and ensuring the appropriate exit clearance is conducted.

b. **Background Investigation Process**

(1) All Contractor personnel with **long-term** access to FDIC facilities, IT systems, or sensitive information must undergo an OPM background investigation commensurate with the designated risk level associated with the duties of each position. At a minimum, a National Agency Check with Inquiry (NACI) will be required.

(2) The PSU will send the completed Background Investigation Forms to USOPM to conduct the appropriate background investigation.

(3) A new OPM background investigation may be unnecessary for contractor personnel who have a current or otherwise valid background investigation; that was favorably adjudicated by the U.S. Government; meets the requirement for the current risk level; was conducted within the previous 54-months; and the individual maintained a continuous federal affiliation in the previous 24-months.

c. **Reassignment for Cause**. When issues are discovered during the preliminary approval process or the OPM background investigation, that call into question the contractor personnel's integrity and fitness they will be given an opportunity to refute, explain or otherwise mitigate the issue. If the PSU determines the issue cannot be mitigated or refuted the contracting officer will be advised to have the individual reassigned from the task. In general, contractor personnel who either self-report or an investigation reveals prior duties as an officer or director of a Failed Financial Institution or of an affiliate of a Failed Financial

Post-Award Security Procedures (cont'd)

Institution who (1) participated in a material way in one or more transactions that caused a Substantial Loss to any such Failed Financial Institution; or (2) in connection with such Substantial Loss has been found by a court or administrative tribunal, or alleged in a judicial or administrative action brought by the FDIC or any federal or state governmental entity to have (i) violated any law, regulation or order issued by a Federal or State banking agency; (ii) breached a written agreement with a Federal or State banking agency or with a Failed Financial Institution; (iii) engaged in an unsafe or unsound practice in conducting the affairs of a Failed Financial Institution; or (iv) breached a fiduciary duty owed to a Failed Financial Institution, will render the contractor personnel unsuitable for performance on the contract. In these cases, the FDIC program office in consultation with the PSU and Legal Staff, will submit a request to the Contracting Officer to have the contractor reassign the contractor employee to another contract not associated with providing services to the FDIC. This is not considered a determination of suitability and therefore the contractor personnel does not have the right to challenge or provide additional information to mitigate the concern.

d. **Effect on Obligations Under Contract**. Nothing contained in this circular or on any form used in implementing the provisions of this circular shall be construed to waive any contractor obligation pursuant to a contract. This includes, without limitation, any obligation to supervise its agents, employees, and subcontractors used in connection with the contract with the FDIC, and any obligation to protect the property, information, and confidences of the FDIC from misappropriation by the contracting firm, its agents, employees, or subcontractors.

11. Forms

The forms listed below are available on the FDICnet under Policy, FILs, Directives, Standardized Forms.

a. Form FDIC 1600/04, Background Investigation Questionnaire for Contractor Personnel and Subcontractors;

b. Form FDIC1600/07, Background Investigation Questionnaire for Contractors;

c. Form FDIC 1600/10, Notice and Authorization Pertaining to Consumer Reports

d. Form FDIC 1600/13, Personnel Security Action Request;

Forms (cont'd)	The FD 258, Applicant Fingerprint Card with FDIC overprint is only available in hard copy. At FDIC HQ send requests to SEPS specifying the number of cards needed. At Regional and Temporary Satellite Offices send requests to the Regional DOA Security Representative.

12. Effective Date The provisions outlined in this circular are effective immediately.

Attachments:

Attachment A – Risk Level Matrix
Attachment B – Contractor Risk Level Record
Attachment C – Form FDIC 1600/04 Background Investigation Questionnaire for Contractor Personnel and Subcontractors
Attachment D – Form FDIC 1600/07 Background Investigation Questionnaire for Contractors
Attachment E – Form FDIC 1600/10, Notice and Authorization Pertaining to Consumer Reports
Attachment F – Form FDIC 1600/13 Personnel Security Action Request
Attachment G – SF 85P Questionnaire for Public Trust Positions

RISK LEVEL MATRIX

Risk Level	Risk Level Definition	Job Responsibility Examples
High Risk	Contract duties or responsibilities which are especially critical to the Corporation or particular program mission, system(s), or information. Access to highly sensitive/critical systems or information with the potential for causing exceptionally serious damage.	• Responsibility for the development, implementation, and/or administration of Corporate computer security programs. • Significant involvement in life-critical or mission critical systems or programs. • Responsibility for preparing or approving data for input into a system which does not necessarily involve personal access to the system, but which creates a high risk for effecting grave damage or realizing significant personal gain. • Responsibility for the planning, design, testing, maintenance, operation, monitoring or management of systems hardware or software. • Access to a system during the operation or maintenance in such a way to permit high risk for causing grave damage or realizing significant personal gain. • Work involving investigative, compliance, or senior level auditing type duties. • Access to sensitive financial information which could result in realizing significant personal gain. • Significant public health or public safety duties. • Access to or control of highly sensitive, but unclassified information/data. • Work involving fiduciary, public contact, or other duties involving the highest degree of public trust. • Work occurring after duty hours within FDIC buildings which is not supervised by an FDIC employee and where appropriate physical security measures are not in place to prevent unauthorized access to sensitive data or information. • Any other duties designated by the OM, Contracting Officer, or Program

Risk Level	Risk Level Definition	Job Responsibility Examples
		Manager which will have a high risk for effecting grave damage or realizing significant financial gain.
Moderate Risk	Contract duties or responsibilities which are of considerable importance to the Corporation or particular program mission, system(s), or information. Access to moderately sensitive/critical systems or information with the potential for causing moderate damage.	• Work involving similar duties as outlined above, but which has close technical review by a senior FDIC employee. • Work involving free access and movement within FDIC buildings during normal duty hours with little or no supervision by an FDIC employee. • Work occurring after duty hours within an area which houses sensitive information or equipment even though supervised by an FDIC employee. • Work requiring access to sensitive information such as that protected by the Privacy Act. • Any other duties as designated by the OM, Contracting Officer, or Program Manager.
Low Risk	Contract duties and responsibilities which have limited impact on the Corporation or particular program mission, system(s), or information. Access to systems or information with the potential for causing minimal damage.	• All other duties/responsibilities not falling into one of the above risk levels.
Note 1	If contract duties involve access to National Security Classified Information, contact the Assistant Director, Security Management Section.	

Federal Deposit Insurance Corporation

CONTRACTOR RISK LEVEL RECORD

DIVISION/OFFICE	PURCHASE REQUEST NUMBER

CONTRACT NUMBER

DESCRIPTION OF CONTRACT:

Click here to type text. If additional space is needed, use the TAB key to insert another row. Otherwise, move the cursor to the next field.

METHOD FOR DETERMINING RISK LEVEL *(Choose one).* If Labor Category *(Use extra sheets, if needed.)*

☐ LABOR CATEGORY

LABOR CATEGORY	RISK LEVEL	JUSTIFICATION

☐ CONTRACT

RISK LEVEL:

Click here to type text. If additional space is needed, use the TAB key to insert another row. Otherwise, move the curso next field.

JUSTIFICATION:

Click here to type text. If additional space is needed, use the TAB key to insert another row. Otherwise, move the curso next field.

PROGRAM MANAGER	INFORMATION SECURITY MANAGER

FDIC 1600/17 (2-10)