FDIC DIRECTIVE 1610.02

Personnel Security and Suitability Program for Contractors and Contractor Personnel

Approval Authority: Brandon Milhorn, Deputy to the Chairperson, Chief of Staff, and Chief Operating Officer

Originating Division/Office: Division of Administration

Approval Date: 01/15/2020 **Pedestrian Change Date**: 02/26/2021

PURPOSE

This revised Directive provides policy relating to contractors and contractor personnel security and fitness in accordance with federal directives and authorities.

SCOPE

The provisions of this Directive apply to all FDIC personnel involved in the on- and off-boarding (boarding) and continuous vetting of contractors and contractor personnel. This Directive does not apply to intermittent contractors and contractor personnel who access FDIC facilities on an infrequent and generally unscheduled basis, and do not require access to sensitive information (e.g., equipment repair, delivery personnel). These contractors and contractor personnel are required to be escorted.

AUTHORITIES

See Appendix A.

FORMS

See Appendix B.

SUMMARY OF CHANGES

This Directive supersedes 1610.2, Personnel Security and Suitability Program for Contractors and Contractor Personnel, dated January 28, 2010.

REVISION, dated January 15, 2020

This Directive had been revised to update personnel security authorities and responsibilities, incorporating previously published Interim Policy Memoranda. It also introduces FDIC's Enterprise Workforce Solution (eWORKS) as the tool which automates the boarding process for FDIC contractor personnel.

PEDESTRIAN CHANGE, dated February 26, 2021

This Directive had been revised to:

- Add responsibilities for Insider Threat and Counterintelligence Program Management Office (ITCIPMO) to align with FDIC Directive 1600.07, FDIC Insider Threat and Counterintelligence Program; and

- Upon approval, renumber Directive to 1610.02.

TABLE OF CONTENTS

PURPOSE 1
SCOPE 1
AUTHORITIES 1
FORMS 1
SUMMARY OF CHANGES 1
BACKGROUND 4
POLICY 5
A. Contractor and Contractor Personnel Risk Levels 5
B. Fingerprinting 6
C. Background Investigations 6
D. Integrity and Fitness Standards 7
E. Continuous Evaluation 7
RESPONSIBILITIES 8
A. DOA/SEPS Assistant Director 8
B. DOA/SEPS Chief, Security Operations 8
C. Legal Division 8
D. Division/Office Directors 9
E. Contracting Officer 9
F. Oversight Managers and Technical Monitors 9
G. Chief Information Officer Organization 10
H. Division/Office Information Security Managers 10
I. Insider Threat and Counterintelligence Program Management Office 10
APPENDIX A – AUTHORITIES 11
APPENDIX B – FORMS 12
GLOSSARY OF TERMS 13
GLOSSARY OF ACRONYMS 18

BACKGROUND

FDIC's Personnel Security and Suitability Program vets all contractors and contractor personnel performing any service for or on behalf of the FDIC by implementing the requirements and responsibilities found within the applicable authorities (see Appendix A), U.S. Office of Personnel Management (OPM) Federal Investigations Notices, FDIC Directives, and other guidance.

Specific to FDIC, 12 U.S.C. Section 1822(f) and 12 CFR Part 366, Minimum Standards of Integrity and Fitness for an FDIC Contractor, set forth "the minimum standards of integrity and fitness that contractors, subcontractors, and employees of subcontractors and subcontractors must meet if they perform any service or function on [FDIC's] behalf." The regulations identify conduct and behaviors that may prevent the contractors, subcontractors and their personnel from performing FDIC contracts.

In 2018, DOA initiated the use of eWORKS functioning as a tool to automate the end-to-end processes for boarding FDIC contractor personnel. Refer to the SEPS on FDICnet at DOA Home > Workplace Services > Security > Security & Emergency Preparedness Section > eWORKS.

eWORKS improves the boarding process which:

- Creates transparency in the background investigation process for Oversight Managers (OMs) in the form of a dashboard and status updates;
- Reduces the time it takes contractor personnel to complete and submit required personnel security forms; and
- Decreases the opportunity for errors.

POLICY

The integrity and fitness requirements[1] apply to all contractors and contractor personnel seeking to perform services on behalf of the FDIC. In addition, respective security eligibility and suitability requirements apply to all contractors and contractor personnel who have, or may have, access to FDIC facilities, information, information technology (IT) systems, and sensitive or classified information for longer than six months, and may be subjected to modified vetting if less than six months.

NOTE: This Directive does not apply to intermittent contractors and their personnel who access FDIC facilities on an infrequent and generally unscheduled basis, and do not require access to sensitive information (e.g., equipment repair, delivery personnel). These contractors and their personnel are required to be escorted.

A. Contractor and Contractor Personnel Risk Levels

In lieu of designation of a contract, Basic Ordering Agreement (BOA), Receivership BOA (RBOA), Blanket Purchase Agreement (BPA), or task order with an overall risk category of High, Moderate, or Low, each contract, BOA, RBOA, or BPA contains separately designated risk levels for each FDIC established labor category, or in the absence of labor categories, separately designated risk levels for each defined area of functional responsibility.

1. Labor Categories or Areas of Functional Responsibility

   Each contractor and contractor personnel is designated to one or more labor categories or one or more areas of functional responsibility generating one or more of the following risk levels:

   a. Low Risk (LR)

   b. Moderate Risk (MR)

   c. High Risk (HR)

   d. High Risk IT (HR-IT)

   NOTE: When a contractor or contractor personnel performs in more than one labor category or area of functional responsibility, and the assigned risk levels are not the same, the highest of the assigned risk levels applies to the contractor or contractor

[1] See 12 CFR Part 366, Minimum Standards of Integrity and Fitness for an FDIC Contractor, January 1, 2012, for integrity and fitness requirements.

personnel. Contracts, BOAs, RBOAs, BPAs, and task orders no longer receive an overall risk level designation.

2. Conditions and Exceptions

   a. Assignment to HR and HR-IT Positions:

      1) A contractor or contractor personnel assigned to provide services under labor categories or functional categories are designated as HR must be U.S. citizens.

      2) In the absence of qualified available U.S. citizens, non-U.S. citizens with lawful permanent resident (LPR) status may be considered, by exception, for an assignment to HR positions, provided those positions are time-limited.

      3) In the case of HR IT contract positions, approval of such exceptions by the Chief Information Officer Organization (CIOO) is required, along with concurrence by the Chief Financial Officer (CFO) and Chief Operating Officer (COO). For HR non-IT contract positions, such exceptions require the approval of the responsible Division or Office Director, along with concurrence by the CFO and COO.

   b. Assignment to positions at all risk levels:

      1) Non-US citizens with less than three years residing within the U.S. will have limited information available to conduct a thorough background investigation, thereby not meeting the required investigative standards.

      2) As such, the Chief of Security Operations is unable to preliminarily approve such individuals.

      3) In this case, approval of such exceptions is required by the respective Division, coordinated through the OM.

B. Fingerprinting

All contractor personnel are subject to digital fingerprints.

C. Background Investigations

1. Initial Requirements

   All contractors and contractor personnel are subject to background investigation commensurate with the risk level for the position held. For initial background

investigation guidance, please reference the authorities listed in Appendix A. This applies to contractors or contractor personnel who:

a. Work on-site and have unescorted access to FDIC offices or facilities;

b. Have access to FDIC networks/systems; or

c. Have access to sensitive information.

2. Periodic Reinvestigations

Contractors and contractor personnel, if applicable, are subject to periodic reinvestigation and continuous evaluation commensurate with the risk level for the position held. For periodic reinvestigation guidance, please reference the authorities listed in Appendix A.

3. Exemptions

Contractors and contractor personnel may be granted a background investigation exemption in certain circumstances. For guidance on exemption(s), please reference the authorities listed in Appendix A.

D. Integrity and Fitness Standards

All contractors and contractor personnel are subject to applicable laws and regulations governing integrity and fitness. A favorable integrity and fitness determination is required for access to FDIC facilities, IT systems, and sensitive information, and to enter into a contract or to perform a service or function on FDIC's behalf. 12 CFR Section 366.3.

All contractors and contractor personnel must maintain the applicable standards and comply with FDIC security eligibility and suitability policies.

E. Continuous Evaluation

In accordance with the Office of the Director of National Intelligence (ODNI) policy, as amended, all FDIC security clearance holders are subject to enrollment in the National Background Investigations Bureau's Continuous Evaluation services.

RESPONSIBILITIES

A. DOA/SEPS Assistant Director (SEPS Assistant Director):

The SEPS Assistant Director is responsible for the administration of FDIC's Personnel Security and Suitability Program.

B. DOA/SEPS Chief, Security Operations (Chief, Security Operations):

The Chief, Security Operations is responsible for the day-to-day management of FDIC's Personnel Security and Suitability Program including:

1. Establishes and implements FDIC's Personnel Security and Suitability Program;
2. Maintains the Procedural Guide;
3. Conducts integrity and fitness evaluations and processing potentially disqualifying information;
4. Grants adjudicative decision and confirms applicable subsequent action is taken: such as, but not limited to, approval, denial, revocation, and removal;
5. Concurs/not concurs with contractor and contractor personnel risk levels;
6. Records contractor personnel risk designations in internal systems;
7. Conducts contractor company clearances;
8. Ensures reciprocity is applied in accordance with federal regulations and OPM/ODNI guidance;
9. Initiates and updates appropriate background investigations corresponding to risk levels;
10. Reviews results of background investigations; and
11. Ensures fitness determinations are performed and reported in a timely manner and in accordance with federal regulations and OPM/ODNI guidance, including criteria pertaining to suitability guidelines. In addition, ensures certain security eligibility and suitability determinations are coordinated with Legal/Contracting & Risk Management Unit.

C. Legal Division:

The Contracting and Risk Management Unit of the Legal Division provides advice to SEPS regarding the applicability of certain aspects of 12 CFR Part 366 that may impact SEPS'

security eligibility and suitability determinations, including whether the contractor or contractor personnel demonstrate:

1. A pattern and practice of defalcation under 12 CFR Section 366.4; or

2. A substantial loss to the Deposit Insurance Fund under 12 CFR Section 366.5.

D. Division/Office Directors:

The Division/Office Directors are responsible for adhering to FDIC's Personnel Security and Suitability Program.

E. Contracting Officer:

1. Ensures all solicitations for services include all applicable personnel security forms and clauses required in this Directive and under the Acquisition Policy Manual and Acquisition Procedures, Guidance and Information;

2. Obtains necessary personnel security forms from the bidding company along with the bidding company's key personnel for pre-award fitness determination; and

3. Coordinates with the Oversight Manager (OM) and submits any additional required personnel security forms for any key personnel expected to perform operational tasks under the contract.

F. Oversight Managers (OMs) and Technical Monitors:

1. Initiate and review all forms for completeness in eWORKS before forwarding to SEPS/PSU; and

2. Manage all aspects of contractor personnel security as defined in this Directive, including:

    a. Contractor personnel access to FDIC facilities, IT systems, and sensitive information;

    b. Ensure quality control over all personnel security boarding requests to confirm completeness prior to submitting to SEPS/PSU through eWORKS; and

    c. Ensure Pre-Exit Clearance procedures are followed, which includes removal of contractor in accordance with Unfavorable Fitness/Integrity Removals of Contractor Personnel Procedures.

G. Chief Information Officer Organization (CIOO):

The CIOO establishes security and access control policies and procedures for FDIC IT resources, in accordance with data loss prevention procedures.

H. Division/Office Information Security Managers:

1. Promote Division/Office compliance with FDIC personnel security directives;
2. Implement business-specific security practices;
3. Serve as primary liaison between the Office of the Chief Information Security Officer and the specific Division/Office;
4. Collaborate with program and project managers in identifying existing and appropriate security features for applications;
5. Participate in risk analyses;
6. Coordinate the development of security plans; and
7. Ensure the Risk Level determination identified on FDIC Form 1600/17, Contractor Risk Level Record, accurately reflects the IT access assigned to the position and the OPM's Position Designation Tool was used to determine the accurate level.

I. Insider Threat and Counterintelligence Program Management Office (ITCIPMO):

1. Reviews cases referred by the Chief of Security Operations or Personnel Security and Suitability Program for possible insider threat and/or counterintelligence concerns;
2. Confirms timely, final completion of all pre-exit clearance procedures in removals related to unfavorable adjudicative decisions;
3. Works with CIOO on data loss prevention reviews to identify potential, historical unauthorized data/information disclosures, as necessary; and
4. Communicates to the Chief of Security Operations, any gaps or abnormalities pertaining to removals.

APPENDIX A – AUTHORITIES

- 5 CFR Section 731, Suitability
- 5 CFR Section 736, Personnel Investigations
- 12 CFR Part 366, Minimum Standards of Integrity and Fitness for an FDIC Contractor
- 12 U.S.C. Section 1822 (f), Corporation as Receiver. Conflict of Interest
- Executive Order 10450, Security Requirements for Government Employment, as amended
- Executive Order 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, as amended, and as modified by Executive Order 13869, Transferring Responsibility for Background Investigations to the Department of Defense
- Executive Order 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust, January 16, 2009, as amended
- Executive Order 13526, Classified National Security Information
- Executive Order 13764, Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters
- FDIC Directive 1600.03, Classified National Security Information Program
- Homeland Security Presidential Directive-12 (HSPD-12)
- Federal Information Processing Standard (FIPS) Publication 201-2 titled “Personal Identification Verification (PIV) for Federal Employees and Contractors”
- Joint Guidance issued by OPM and ODNI in June 2018 titled “Transforming Workforce Vetting: measures to Reduce the Federal Government’s Background Investigation Inventory in Fiscal Year 2018”
- Security Executive Agent Directive-7 (SEAD-7), Reciprocity of Background Investigations and National Security Adjudications

APPENDIX B – FORMS

Contracting with and Reinvestigations – Contractor Personnel

- FDIC Form 1600/04, Background Investigation Questionnaire for Contractor Personnel and Subcontractors
- FDIC Form 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.
- FDIC Form 1600/13, Personnel Security Action Request
- FDIC Form 1600/17, Contractor Risk Level Record
- FDIC Form 1620/01, Employee/Contractor Personnel Identification Card Request
- Optional Form 306, Declaration for Federal Employment
- Standard Form 85, Questionnaire for Non-Sensitive Positions
- Standard Form 85P, Questionnaire for Public Trust Positions
- Standard Form 86, Questionnaire for National Security Positions
- Standard Form 86C, Questionnaire for National Security Positions

NOTE: All, or a combination of, listed forms may be required based upon initial background investigation, background reinvestigation, and fitness determination.

GLOSSARY OF TERMS

12 CFR Part 366: This regulation establishes the minimum standards of integrity and fitness that contractors and employees of contractors must meet if they perform any service or function on FDIC's behalf. The regulation does the following:

- Defines the persons with whom the FDIC is prohibited from entering into a contract;
- Describes the prohibited conduct, including having a felony conviction; was removed from participating in the affairs of an insured depository institution as a result of a federal banking agency final enforcement action; has a pattern and practice of defalcation; or is responsible for a substantial loss to the Deposit Insurance Fund; and
- Establishes other conduct that may prevent the contractor from performing services on behalf of FDIC, such as, conflicts of interest, unethical conduct, failing to maintain confidential information; and failing to provide certain information defined in the regulation.

Background Investigation: A personnel security investigation conducted by written or telephone inquiries or through personal contacts to determine the suitability, eligibility, or qualifications of individuals for Federal employment, for work on Federal contracts, or for access to classified information or restricted areas.

Boarding: The action or process of integrating a person into or out of the Corporation, known as on-boarding and off-boarding.

Classified National Security Information: Official information or material that requires protection in the interest of national security and which is classified for that purpose under authority designated in E.O. 12958. The levels of Classified national security information are Top Secret, Secret, and Confidential.

Continuous Evaluation: A personnel security investigative process to review the background of individuals who have been determined to be eligible for access to classified national security information or to hold a sensitive position.

Contractor: A corporation, partnership, joint-venture, or other third party entity that enters into a contract with FDIC to provide goods or services, including Subcontractors.

Contractor Company Clearance: A generic term that describes an investigatory process the SEPS/PSU completes on contractors to ensure they meet minimum Integrity and Fitness standards as set forth by 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.

Contractor Personnel: All employees of a Contractor/Subcontractor who perform under an FDIC contract, including key and non-key personnel.

Defalcation: Misappropriation of funds by a person trusted with its charge; also, the act of misappropriation, or an instance thereof.

FDIC Facilities: A building, or any part thereof, including parking areas, owned or leased by the FDIC.

Fitness Determination: A decision by an agency that an individual has or does not have the required level of character and conduct necessary to perform work for or on behalf of a Federal agency as a contractor or contractor personnel.

High Risk: Level associated with positions that 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).

High Risk Information Technology: Level of risk associated with positions that involve duties in which the incumbent has:

- Responsibility for development or administration of IT security programs, including direction and control of risk analysis and/or threat assessments;
- Access to or processing of proprietary data, information requiring protection under the Privacy Act of 1974, sensitive information, Personally Identifiable Information (PII) and FDIC-developed privileged information; including user level access to the FDIC network and information systems, system security and network defense systems, or to system resources providing visual access or ability to input, delete or otherwise manipulate sensitive information without controls to identify and deny access to sensitive information;
- Responsibility for the preparation or approval of data for input into a system which does not necessarily involve personal access to the system, but with relatively high risk for effecting exceptionally serious damage or realizing significant personal gain;
- High risk assignments associated with or directly involving the accounting, disbursement or authorization for disbursement from systems of:
    - Dollar amounts of $10 million per year or greater; and
    - Lesser amounts if the activities of the individual are not subject to technical review by a higher authority to ensure the integrity of the system.

- Responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, or management of systems hardware or software; or

- Other responsibilities, designated by the CIO, which involve high risk for effecting exceptionally serious damage or realizing significant personal gain.

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

Lawful Permanent Resident: Any person not a citizen of the U.S. residing in the U.S. under legally recognized and lawfully recorded permanent residence as an immigrant, also known as a Permanent Resident Alien, Resident Alien Permit Holder, and Green Card Holder.

Low Risk: Level associated with positions that involve duties with limited relation to the Corporation's mission and have little effect on the efficiency of the Corporation's operations or programs.

Moderate Risk: Level associated with positions that involve duties of considerable importance to the Corporation or its program mission with significant program responsibilities 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).

National Security: Those activities which are directly concerned with the foreign relations of the United States, or protection of the Nation from internal subversion, foreign aggression, or terrorism.

Periodic Reinvestigation: A background investigation conducted at a specified interval to update a fitness determination.

Person: An individual, corporation, partnership, or other entity with a legally independent existence.[2]

Preliminary Approval: A generic term that describes a process the SEPS/PSU completes on contractors and 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 fingerprint criminal records, review of personnel security questionnaires, credit reports provided by the three major credit reporting agencies, and other internal FDIC resources.

[2] PART 366 — MINIMUM STANDARDS OF INTEGRITY AND FITNESS FOR AN FDIC CONTRACTOR Definitions at https://www.fdic.gov/regulations/laws/rules/2000-8800.html

Reciprocity: As it applies in background investigations, it is the practice of accepting background investigations, suitability decisions and security eligibility decisions conducted by other authorized agencies.

Risk Level: An evaluative classification designation assigned based on duties performed that have the potential for affecting the integrity, efficiency, or effectiveness of the Corporation's mission, and, when misused, may diminish public confidence.

Security Eligibility: The evaluation of an individual's loyalty, character, trustworthiness, and reliability to ensure that the individual is eligible for access to classified national security information.

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

- 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 CFR Part 309, for further information);

- 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 CFR Part 310, for further information);

- 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; and

- Information about insurance assessments, resolution and receivership activities, as well as enforcement, legal, and contracting activities.

Sensitive Position: Any position within a department or agency in which the occupant could cause, by virtue of the nature of the position, a material adverse effect on national security as defined in Section 3(b) in EO 10450.

Suitability: Identifiable character traits and past conduct sufficient to determine whether a given individual is or is not likely to be able to carry out the duties of a Federal job or Federal contract. Suitability is distinguishable from a person's ability to fulfill the qualification requirements of a job, as measured by experience, education, knowledge, skills, and abilities.

Vetting: The process by which covered individuals undergo investigation, evaluation, and adjudication of whether they are, and remain over time, suitable or fit for Federal employment,

eligible to occupy a sensitive position, eligible for access to classified information, eligible to serve as a non-appropriated fund employee or a contractor, eligible to serve in the military, or authorized to be issued a Federal credential.

GLOSSARY OF ACRONYMS

BOA: Basic Ordering Agreement

BPA: Blanket Purchase Agreement

CIO: Chief Information Officer

CO: Contracting Officer

eWORKS: Enterprise Workforce Solution

HR-IT: High Risk Information Technology

ISM: Information Security Manager

IT: Information Technology

OM: Oversight Manager

OPM: U.S. Office of Personnel Management

PSU: Personnel Security Unit

RBOA: Receivership Basic Ordering Agreement

SEPS: Security Emergency Preparedness Section