FDIC DIRECTIVE 1610.02

Personnel Security and Suitability Program for Contractors and Contractor Personnel

Approval Authority: Daniel Bendler, Deputy to the Chairperson and Chief Operating Officer

Originating Division/Office: Division of Administration

Approval Date: 09/06/2024

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 onboarding, off-boarding, and transferring of contractors and contractor personnel who:

1. Work on-site at and have unescorted access to FDIC offices or facilities;
2. Have access to FDIC networks/systems; or
3. Have access to sensitive information in accordance with FDIC Directive 1360.09, Protecting Information.

This Directive does not apply to contractors and contractor personnel who access FDIC facilities on an infrequent and generally unscheduled basis (e.g., equipment repair or delivery personnel), and do not require access to FDIC systems/networks or sensitive information in accordance with FDIC Directive 1360.09, Protecting Information. These contractors and contractor personnel are required to be escorted.

AUTHORITIES

See Appendix A.

FORMS

See Appendix B.

SUMMARY OF CHANGES

This Directive supersedes FDIC Circular 1610.2, Personnel Security and Suitability Program for Contractors and Contractor Personnel, dated January 15, 2020, with a Pedestrian Change dated February 26, 2021.

REVISION, dated September 6, 2024

This Directive has been revised to:

- Update authorities reference for Federal Personnel Vetting Guidelines;
- Include responsibilities for the Chief, Personnel Security Unit;
- Add responsibilities for the Intelligence Threat Sharing Unit (ITSU), formerly referred as the Insider Threat and Counterintelligence Program Management Office (ITCIPMO);
- Update Unit/Section name changes;
- Include the ability for non-U.S. citizens without lawful permanent residency status to work on FDIC contracts under certain circumstances (as defined in Policy Section A.2.b); and
- Update the Glossary of Terms.

TABLE OF CONTENTS

BACKGROUND

The 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 applicable authorities, including Defense Counterintelligence and Security Agency Federal Investigations Notices, Executive Orders, FDIC Directives, and other guidance (see Appendix A).

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

The FDIC uses Enterprise Workforce Solution (eWORKS) to automate the end-to-end processes for onboarding and off-boarding FDIC contractor personnel. The eWORKS webpage describes the eWORKS automated tool, which:

- Digitizes the personnel security vetting process, discontinuing the need for most paper-based background investigation (BI) forms;
- Reduces the time it takes contractor personnel to complete and submit required personnel security forms;
- Decreases the opportunity for errors by enforcing data alignment and consistency; and
- Creates transparency in the personnel security vetting process by enabling Oversight Managers (OMs) and Contracting Officers (COs) (collectively referred to as "Service Requesters") to track initiated cases through the system.

POLICY

Integrity and fitness requirements[1] apply to all contractors, contractor personnel, and subcontractor personnel seeking to perform services on behalf of the FDIC. In addition, respective security eligibility and contractor fitness requirements[2] apply to all contractors and contractor personnel who have, or may have, access to FDIC facilities, FDIC networks/systems, and sensitive information.[3] Contractor personnel are subject to modified vetting if access is for less than six months.

A. Contractor and Contractor Personnel Risk Levels

At a minimum, a risk level designation (high, moderate, low, high risk-IT) must be designated for labor categories or areas of functional responsibility on each award.

1. Labor Categories or Areas of Functional Responsibility

   Each contractor and contractor personnel is designated to one labor category or one area of functional responsibility generating one or more of the following risk levels as required on FDIC Form 1600/17, Contractor Risk Level Record,[4] in accordance with Acquisition Procedures & Guidance Manual (APGM) 5.203(a), Pre-Solicitation Requirements:

   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

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

[2] For security eligibility and contractor fitness requirements, use equivalent criteria to 5 CFR 731, Suitability; Executive Order (EO) 12968, Access to Classified Information; and Security Executive Agent Directive 4 (SEAD-4), National Security Adjudicative Guidelines.

[3] Definition of "Sensitive Information" is in accordance with FDIC Directive 1360.09, Protecting Information.

[4] FDIC Form 1600/17, Contractor Risk Level Record, is completed by the Program Manager (PM)/Contract Oversight Manager (OM). An Information Security Manager (ISM) will review FDIC Form 1600/17, with final concurrence by a designated Personnel Security Specialist within the Personnel Security Unit.

same, the highest of the assigned risk levels applies to the contractor or contractor personnel.

2. Conditions and Exceptions

   a. Assignment to High Risk (HR) and High Risk-Information Technology (HR-IT) Positions:

      1) A contractor or contractor personnel assigned to provide services under labor categories or functional areas of responsibility designated as HR must be a U.S. citizen.

      2) In the absence of qualified and available U.S. citizens, non-U.S. citizens with lawful permanent resident (LPR) status may be considered, by exception, for an assignment to HR labor categories or areas of functional responsibility, provided they are time-limited to less than 180 days.

         a) In the case of HR-IT labor categories or areas of functional responsibility, approval of such exceptions by the Chief Information Officer is required, along with concurrence by the Chief Financial Officer (CFO) and Chief Operating Officer (COO).

         b) For HR non-IT labor categories or areas of functional responsibility, such exceptions require the approval of the responsible Division/Office Director, along with concurrence by the Chief Financial Officer and Chief Operating Officer.

         c) Exceptions to the 180-day limit will be addressed on a case-by-case basis, approved by the respective Division/Office Head as well as the CFO and COO. Exceptions beyond the 180-day limit require a full background investigation.

   b. Assignment to Moderate or Low Risk Labor Categories or Areas of functional responsibility:

      1) A contractor or contractor personnel assigned to provide services under labor categories or functional areas of responsibility designated as moderate risk or low risk do not need to be a U.S. citizen or a LPR of the United States.

2) Non-U.S. citizens without LPR status are permitted to work on a FDIC contract with labor categories designated as moderate risk or low risk provided that the contractor personnel meets the requirements of being legally admitted to the United States, and holds a valid authorization to work in the United States.

c. Assignment to labor categories or areas of functional responsibility at all risk levels:

1) Contractor personnel with less than three years out of the past five years residing within the U.S. do not meet the required background investigative standards, as there will be limited information available to conduct a thorough background investigation.

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

d. During a receivership activity, an acceptance of risk can be made by the respective Division/Office Head if the Division/Office has a necessary requirement to use non-U.S. citizens or legal permanent U.S. residents located in the respective foreign country to specifically conduct bank-related activities (e.g., tax filing). A written justification will be provided to the Division/Office Head for approval.

B. Fingerprinting

Contractor personnel are subject to digital fingerprinting for the background investigation process, and for identity verification for credentialing.

Homeland Security Presidential Directive-12 (HSPD-12) established a mandatory government-wide standard for secure and reliable personal identification (credentialing) for all federal employees and contractors. In turn, all departments and federal agencies are directed to issue their federal employees and contractors a Personnel Identity Verification (PIV) card for physical access to federal facilities and logical access to government-owned information systems. PIV Credentials are governed by Federal Information Processing Standard (FIPS) 201-3.

Additionally, in order to work for or on behalf of the federal government as a contractor, one must undergo a background investigation per Executive Order (EO) 13467, as amended.

C. Background Investigations

1. Initial Requirements

Contractors and contractor personnel are subject to a background investigation commensurate with the risk level for the labor category or functional responsibility.

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.

All individuals must meet the requirements for the requisite background investigation, complete the background investigation process, and be favorably adjudicated in order to perform work for or on behalf of the FDIC.

2. Periodic Reinvestigations

Contractors and contractor personnel, if applicable, are subject to periodic reinvestigation commensurate with the risk level for the labor category or area of functional responsibility held. For periodic reinvestigation guidance, please reference the authorities listed in Appendix A.

With the full implementation of Trusted Workforce 2.0,[5] periodic reinvestigation will be replaced by continuous vetting.

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 (see 5 CFR 731 Part 104.b.3(c)).

D. Integrity and Fitness Standards

Contractors and contractor personnel are subject to applicable laws and regulations governing integrity and fitness in accordance with 12 CFR Part 366. A favorable preliminary vetting and a favorable integrity and fitness determination are required for access to FDIC facilities, FDIC networks/systems, and sensitive information, and to enter into a contract or to perform a service or function on the FDIC's behalf (see 12 CFR Part 366.3).

Contractors and contractor personnel must continue to maintain integrity and fitness standards based on the applicable laws and regulations while working for the FDIC.

[5] Information regarding Trusted Workforce 2.0 can be found at https://www.performance.gov/trusted-workforce/.

E. Continuous Vetting

Executive Order 13764 defines continuous vetting (CV) which is applicable to all individuals affiliated with the federal government. Designed to replace the traditional periodic reinvestigations, it involves automated data checks to continuously monitor an individual's suitability or fitness to work for or on behalf of the federal government, or eligibility to maintain a security clearance.

In 2021, the national security sensitive population was enrolled into CV, and enrollment into CV for the non-sensitive public trust population will begin in Calendar Year (CY) 2024 and continue into 2025. All contractor personnel will be enrolled into CV. Individuals occupying labor categories or areas of functional responsibility designated as low risk will be enrolled into CV at a later date when mandated by the Suitability Executive Agent (SuitEA).

Additionally, all contractors and contractor personnel are subject to enrollment in the Federal Bureau of Investigation (FBI)'s Rap Back[6] program.

[6] The Rap Back program provides the FDIC with ongoing status notifications of any criminal history reported to the FBI.

RESPONSIBILITIES

A. Assistant Director, Security Enterprise Programs Section (SEPS), Division of Administration:

Oversees the FDIC's Personnel Security and Suitability Program.

B. Chief, Personnel Security Unit (PSU), SEPS:

Manages the day-to-day operations of the FDIC's Personnel Security and Suitability Program, by:

1. Establishing and implementing policies governing the FDIC's Personnel Security and Suitability Program;
2. Maintaining procedural guidance;
3. Conducting integrity and fitness evaluations while processing potentially disqualifying background investigation information;
4. Making adjudicative determinations and confirming applicable subsequent action is taken, such as (but not limited to) approval, denial, revocation, and removal;
5. Concurring or not concurring with risk level designations, gaining concurrence through collaboration with the respective program owner, oversight manager, contracting officer, and information security manager;
6. Conducting risk designations using the Position Designation System (PDS) and associated Position Designation Tool (PDT) to designate risk and sensitivity levels for all positions (e.g., military, federal, or civilian employees and contractor personnel);
7. Recording risk level designations in internal systems to include CHRIS and eWORKS;
8. Conducting contractor company screenings;
9. Ensuring reciprocity and transfer of trust is applied in accordance with federal regulations issued by the Security and Suitability Executive Agents;
10. Initiating and updating appropriate background investigations corresponding to risk levels;
11. Reviewing results of background investigations and Continuous Vetting and Rap Back alerts; and

12. Ensuring fitness determinations are made and reported in a timely manner in accordance with applicable federal and FDIC regulations, and in coordination with the Contracts & Risk Management Unit, Legal Division (as needed).

C. Intelligence and Threat Sharing Unit (ITSU), SEPS:

1. Reviews contractor cases referred by the Chief, PSU 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 fitness determinations;

3. Works with the CIOO to prevent and analyze data loss incidents to avert harm to the FDIC and banking industry; and

4. Communicates to the Chief, PSU any gaps or abnormalities pertaining to removals which may impact security determinations in accordance with SEAD-4, suitability/fitness determinations in accordance with 5 CFR Part 731, and integrity/fitness decisions in accordance with 12 CFR Part 366.

D. Contracts and Risk Management Unit, Legal Division:

Provides advice to the PSU regarding the applicability of certain aspects of 12 CFR Part 366 that may impact the fitness determination, including whether the contractor or contractor personnel has:

1. A criminal conviction as the final disposition of a criminal case under 12 CFR Part 366.3;

2. A pattern and practice of defalcation under 12 CFR Part 366.4; or

3. A substantial loss to the Deposit Insurance Fund under 12 CFR Part 366.5.

E. Division/Office Directors:

Ensure contractors adhere to the FDIC's Personnel Security and Suitability Program and suitability, integrity, and fitness standards.

F. Contracting Officer:

1. Ensures all solicitations and awards for services include all applicable clauses required in this Directive and under the Acquisition Procedures & Guidance Manual;

2. Initiates eWORKS for contractor company screenings, which contains necessary personnel security forms for the prospective contractor company along with the prospective key personnel for pre-award screening; and

3. Coordinates with the Contract OM to submit required personnel security forms for any key personnel expected to perform tasks under the contract in the automated eWORKS platform.

G. Oversight Managers (OMs) and Technical Monitors (TMs):

1. Ensure vendors validate/certify only individuals who meet the citizenship or lawful permanent resident requirement for High Risk positons (where applicable) are submitted to the PSU for vetting;

2. Ensure vendors validate/certify that all non-U.S. citizens assigned to work on a FDIC contract were legally admitted to the United States and have a valid authorization to work, before submission of a vetting request to the PSU;

3. Initiate and review all digital forms to ensure they are filled out correctly and completely in eWORKS before forwarding to the PSU for processing;

4. Provide FDIC Form 1600/17, Contractor Risk Level Record, and any supporting documentation for Position Risk and Sensitivity determination; and

5. Manage the following aspects of contractor personnel security as defined in this Directive, including:

    a. In coordination with CIOO stakeholders, PSU, and other responsible parties, managing contractor personnel access to FDIC facilities, FDIC networks/systems, and sensitive information;

    b. Ensuring contractor personnel that require transfer actions only are submitted to the PSU with FDIC Forms 3700/25, Pre-Exit Clearance/Transfer Record for Contractor Personnel, and 1600/13, Personnel Security Action Request. If the contractor personnel is transferring to a new labor category, areas of functional responsibility, or contract that needs an upgraded background investigation, then the OM will initiate a new eWORKS request identified as “transfer with upgrade;” and

    c. Ensuring Pre-Exit Clearance procedures are followed for contractor personnel who were subject to a background investigation, which includes removal of contractor personnel in accordance with APGM 5.203(c)(2), Adverse Findings.

H. Chief Information Officer Organization (CIOO):

Establishes security and access control policies and procedures for FDIC IT resources commensurate with the sensitivity of information processed, stored, or transmitted.

I. Division/Office Information Security Managers:

1. Promote Division/Office compliance with FDIC personnel security directives;

2. Implement business-specific security practices;

3. Review and provide security risk guidance to OMs/TMs on respective accesses assigned to FDIC networks/systems and sensitive information;

4. Coordinate the development of security plans; and

5. Ensure the risk level determination identified on FDIC Form 1600/17, Contractor Risk Level, accurately reflects the access assigned to FDIC network/systems, sensitive information, and unescorted access to facilities.

APPENDIX A – AUTHORITIES

- Title 12, United States Code (U.S.C.), Section 1822 (f), Corporation as Receiver, Conflict of Interest
- Title 5, Code of Federal Regulations (CFR), Part 731, Suitability
- Title 5, CFR, Part 736, Personnel Investigations
- Title 12, CFR, Part 366, Minimum Standards of Integrity and Fitness for an FDIC Contractor
- Executive Order (EO) 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, dated June 30, 2008, as amended
- EO 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust, dated January 16, 2009, as amended
- EO 13526, Classified National Security Information
- EO 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 1360.09, Protecting Information
- FDIC Directive 1600.03, Classified National Security Information Program
- FDIC Directive 1600.07, Insider Threat and Counterintelligence Program
- FDIC Directive 1600.09, Intelligence and Counterintelligence Programs
- Homeland Security Presidential Directive-12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors
- Security Executive Agent Directive-7 (SEAD-7), Reciprocity of Background Investigations and National Security Adjudications
- Federal Information Processing Standard (FIPS) Publication 201-3, Personal Identification Verification (PIV) of Federal Employees and Contractors
- Office of Personnel Management (OPM) and Office of the Director of National Intelligence (ODNI), Federal Personnel Vetting Core Doctrine
- OPM and ODNI, Federal Personnel Vetting Guidelines
    - Federal Investigative Standards, December 2012
    - Federal Personnel Vetting Core Doctrine, April 2021

- Federal Personnel Vetting Guidelines, February 2022
- Federal Personnel Vetting Investigative Standards, May 2022
- Federal Personnel Vetting Adjudicative Standards, July 2022
- Federal Personnel Vetting Performance Management Standards, September 2022

APPENDIX B – FORMS

All, or a combination of, the following forms may be required for contractor and contractor personnel vetting based upon initial background investigation, reinvestigation, and fitness determination:

- FDIC Form 1600/04, Background Investigation Questionnaire for Contractor Personnel and Subcontractors
- FDIC Form 1600/07, Background Investigation Questionnaire for Contractors
- 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
- FDIC Form 3700/25, Pre-Exit Clearance/Transfer Record for Contractor Personnel
- Optional Form 306, Declaration for Federal Employment
- Standard Form (SF) 85, Questionnaire for Non-Sensitive Positions
- SF 85P, Questionnaire for Public Trust Positions
- SF 86, Questionnaire for National Security Positions
- SF 86C, Standard Form 86 Certification

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 felony convictions, removal from or prohibited from participating in the affairs of an insured depository institution as a result of a federal banking agency final enforcement action, has a pattern or practice of defalcation, or 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 the 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 inquiries or through personal contacts to determine the suitability, eligibility, or qualifications of individuals for federal employment, work on federal contracts, or unescorted access to FDIC facilities, FDIC networks/systems, or FDIC sensitive information.

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 EO 12968. The levels of classified national security information are Confidential, Secret, and Top Secret.

Continuous Vetting: An ongoing review of an individual's background at any time using automated checks to determine whether an individual continues to meet applicable requirements (e.g., for suitability, fitness, eligibility, or credentialing).

Contractor: A corporation, partnership, or joint-venture that enters into a contract with the FDIC to provide goods or services, including subcontractors.

Contractor Company Screening: A generic term that describes a screening process PSU completes on contractors to ensure they meet minimum Integrity and Fitness standards as set forth by the FDIC. These may include checks of various on-line databases related to a company's financial health or General Services Administration (GSA) status, which refers to the GSA eLibrary (GSA Federal Acquistion Service), and if a GSA bar is found against a company during the "Contractor Company Screening."

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

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, including Personally Identifiable Information (PII) and FDIC-developed privileged information (including user level access to FDIC networks/systems and information systems, system security, and network defense systems, or to system resources providing visual access or ability to input, delete, or otherwise manipulate 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; or
    - 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 CIOO, 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 or risk 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).

Modified Vetting: The process by which select individuals who are working for 180 or less undergo evaluation and adjudication of whether they are suitable or fit to work for or on behalf of the FDIC.

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

Onboarding or Off-Boarding: The action or process of integrating a person into or separating a person from the FDIC.

Pattern or Practice of Defalcation: A situation where a person who has a legal responsibility for the payment on at least two obligations that are: to one or more insured depository institutions; more than 90 days delinquent in the payment of principal, interest, or a combination thereof; and more than $50,000 each.

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.[7]

Reciprocity: As applicable to background investigations, the practice of accepting background investigations, suitability decisions, and security eligibility decisions conducted by other authorized agencies.

[7] See definitions in 12 CFR Part 366, Minimum Standards of Integrity and Fitness for an FDIC Contractor, at https://www.fdic.gov/regulations/laws/rules/2000-8800.html.

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 Position: Any position within or in support of a department or agency, the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security, regardless of whether the occupant has access to classified information, and regardless of whether the occupant is an employee, a military service member, or a contractor (as defined in EO 13764).

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.

Transfer of Trust: A process for ensuring that investigative information is available and accessible, as appropriate, when individuals transfer across departments or agencies and across roles working for or on behalf of the government.

Vetting: The process by which individuals undergo investigation, evaluation, and adjudication of whether they are suitable or fit, eligible to occupy a sensitive position or access classified information, and/or eligible for a personal identity verification credential.

GLOSSARY OF ACRONYMS

CIOO: Chief Information Officer Organization

eWORKS: Enterprise Workforce Solution

HR: High Risk

IT: Information Technology

OM: Oversight Manager

PSU: Personnel Security Unit

SEPS: Security Enterprise Programs Section