

Office of Inspector General



**August 17, 2001
Evaluation Report No. 01-002**

**Review of FDIC's Background Investigation
Process for Prospective and Current Employees**

Office of Audits - Corporate Evaluations



August 17, 2001

Honorable Sue W. Kelly
Chairwoman
Subcommittee on Oversight and Investigations
Committee on Financial Services
House of Representatives
Washington, D.C. 20515

Dear Madam Chairwoman:

This report responds to your request as Chairwoman of the U.S. House of Representatives Subcommittee on Oversight and Investigations (Subcommittee) that the Office of Inspector General (OIG) evaluate the Federal Deposit Insurance Corporation's (FDIC) policies, procedures and practices under which it conducts, adjudicates, and documents background investigations of prospective and current employees. In addition, at the FDIC's request, we assessed whether the Corporation had effectively implemented a process to ensure proper risk designations had been assigned to positions.

This report provides information addressing both of those areas, as well as recommendations we made to the Corporation and its response. The FDIC tentatively agreed with the eight recommendations in this report. The Corporation will issue a memorandum to the OIG by September 15, 2001, summarizing planned corrective actions for each of the recommendations in the report, including expected completion dates and documentation that will confirm completion. The OIG will evaluate the FDIC's planned corrective actions and provide the results of our analysis to the Subcommittee.

As you requested, we have also provided the Subcommittee with a copy of FDIC Circular 2120.1, *Personnel Suitability Program*, dated September 24, 1999, which established the responsibilities, policy requirements, and procedures for the Corporation's position risk designation and background investigation processes.

Should you have any questions or need additional information, please call me at 202-416-2026 or Russell A. Rau at 202-416-2543.

Sincerely,

[Electronically produced version; original signed by Patricia M. Black for Gaston L. Gianni, Jr.]
Gaston L. Gianni, Jr.
Inspector General

TABLE OF CONTENTS

INTRODUCTION	4
RESULTS IN BRIEF	4
BACKGROUND	5
SUITABILITY POSITION RISK DESIGNATION PROCESS	7
The FDIC Has Not Completed Position Designation Records for All Positions	8
USOPM Criteria Were Not Always Consistently Applied in Determining Position Risk Levels	9
The FDIC’s Safety and Soundness and Compliance Examiner Positions Have a Lower Risk Level Designation Than Public Trust Positions	10
ADP Responsibilities Were Not Always Considered in Position Risk Designations	11
BACKGROUND INVESTIGATION PROCESS	13
1. Has the Corporation issued policies for conducting, adjudicating, and documenting background investigations of prospective and current employees?	13
2. Has the Corporation issued or adopted a set of procedures, known to personnel officers and program managers, under which the policies for investigations of prospective and current employees are to be implemented?	14
3. Have the procedures been recently reviewed and revised?	14
4. How does the FDIC monitor compliance with these procedures?	15
5. What evidence do you have to demonstrate that the Corporation has implemented these procedures in a manner that minimizes the risk of improper access, use, or manipulation of sensitive private financial data?	16
6. Are background investigations of prospective employees conducted prior to hiring? Provide analysis demonstrating that Corporation managers adjudicate the results in a timely manner, so troublesome cases are quickly resolved prior to final employment decisions. Provide proof that the results of the investigations are documented in personnel files.	18

7. Are current employees periodically re-investigated throughout their careers, and are such re-investigations adjudicated and documented to the same extent as investigations for prospective employees?	19
CONCLUSIONS AND RECOMMENDATIONS	19
CORPORATION COMMENTS AND OIG EVALUATION	20
APPENDIX I	21
Evaluation Methodology	
APPENDIX II	22
Excerpts of USOPM Guidance for Position Risk Designations	
APPENDIX III	33
Results of Background Investigation Testing	
APPENDIX IV	34
Corporation Comments	

INTRODUCTION

We conducted this review at the request of the Subcommittee on Oversight and Investigations (Subcommittee), Committee on Financial Services, U.S. House of Representatives. In its April 25, 2001 request letter, the Subcommittee discussed how important background investigations are in helping to minimize the risk that sensitive and private financial data utilized by federal financial regulatory agencies is improperly accessed, used, or manipulated.

The Subcommittee asked the OIG to conduct an evaluation of the policies, procedures, and practices under which the FDIC conducts, adjudicates, and documents background investigations of prospective and current employees. In addition, the FDIC requested that we assess whether the Corporation had effectively implemented a process to ensure that proper risk designations had been assigned to FDIC's positions.

Based on the Subcommittee's and FDIC's requests, the objectives of this review were to (1) evaluate FDIC's process for conducting, adjudicating, and documenting background investigations of prospective and current employees and (2) assess whether the FDIC has effectively implemented a process to ensure that positions have appropriate risk designations.

The scope of our review included the FDIC employees on board as of June 2, 2001, all individuals hired by the FDIC from January 1, 2000 through June 2, 2001, and all promotions and reassignments made at that same time. Details of our methodology are included as Appendix I of this report.

We conducted our evaluation between May 14 and August 15, 2001, in accordance with the President's Council on Integrity and Efficiency's *Quality Standards for Inspections*.

RESULTS IN BRIEF

The FDIC designed its Personnel Suitability Program to help ensure that the Corporation employs and retains in employment only those individuals who meet all federal requirements for suitability and whose employment or conduct would not jeopardize the accomplishment of FDIC's duties or responsibilities. The Program includes designating each FDIC position at the high, moderate, or low risk level, based on the documented duties and responsibilities of the positions. The designations determine the type of background investigation required and how closely an individual is screened for a position.

Background investigations are the foundation for, but only a part of, the FDIC's Personnel Suitability Program to determine whether employment or continued employment would protect the integrity and promote the efficiency of the Corporation. Other mechanisms include ethics and financial disclosure reporting for employees, continuing evaluations of employee performance and workplace behavior, and employee education. Although background investigations do not guarantee that individuals will not later engage in unsuitable activities, they remain a critical step in identifying those who are suitable and serve as a preventive measure to help ensure employment and retention of suitable employees.

Risk designations drive the type and timing of background investigations that employees undergo, as well as the adjudication of investigation results. The FDIC needs to do more to ensure that all corporate positions have risk designations and that such designations are commensurate with assigned responsibilities and reflected accurately in corporate databases. Most significantly, the FDIC assigned a low risk designation to nearly all of its safety and soundness and compliance examiners. In addition, the FDIC did not always consider automated data processing (ADP) implications for positions outside of its information resources management division. Because of the significance of these issues, we are presenting them in the first finding section of our report.

As for the Subcommittee's questions regarding background investigations, FDIC policies and procedures comply with provisions of applicable federal laws and regulations. The FDIC also generally conducted, adjudicated, and documented the investigations for current and prospective employees in accordance with policies and procedures. We have organized the information related to background investigations consistent with the questions included in your request letter as a second finding section.

BACKGROUND

It is the FDIC's policy that employees and applicants for employment undergo appropriate background investigations commensurate with positions held or being advertised and in accordance with relevant laws and federal suitability regulations. According to USOPM, suitability refers to identifiable character traits and past conduct that are sufficient to determine whether a given individual is likely or not likely to be able to carry out the duties of a federal job with appropriate efficiency and effectiveness. 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.

FDIC Circular 2120.1, *Personnel Suitability Program*, dated September 24, 1999, establishes the responsibilities, policy requirements, and procedures for the Corporation's process for designating the risk level of each employment position and using that designation to determine the investigation requirements for the position. The Security Management Section (SMS), Acquisition and Corporate Services Branch, Division of Administration (DOA) has the responsibility to administer the Corporation's Personnel Suitability Program.

The FDIC uses draft U.S. Office of Personnel Management (USOPM) guidance for designating position risk levels, determining the type of investigative review to be conducted, and adjudicating suitability based on the results of the investigations. Excerpts of USOPM guidance are included as Appendix II of this report. The FDIC also uses the USOPM to conduct all of its background investigations.

USOPM personnel suitability guidance provides for designating positions at the high, moderate, or low risk level commensurate with the responsibilities and attributes of the position in relation

to the efficiency of the service being provided by the organization in which the position resides. The three suitability position risk levels are defined as follows:

- High Risk Positions involve duties that are especially critical to the agency or program mission with a broad scope of responsibility and authority, such as: policy-making, policy-determining, and policy-implementing; higher level management duties and assignments, or major program responsibility; and independent spokespersons or non-management positions with authority for independent action.
- Moderate Risk Positions involve duties of considerable importance to the agency or program mission with significant program responsibility or delivery of service, such as: assistants to policy development and implementation; mid-level management duties and assignments; and delivery of service positions that demand public confidence or trust.
- Low Risk Positions involve duties and responsibilities of limited relation to an agency or program mission, so the potential for impact on the integrity and efficiency of the service is limited.

Included in USOPM guidance and FDIC's Circular 2120.1 are provisions for determining a Computer/ADP position risk level at the high, moderate, or low risk levels defined as follows:

- High Risk Positions have the potential for exceptionally serious impact involving duties especially critical to the agency mission with broad scope and authority and with major program responsibilities which affect a major Computer/ADP system(s).
- Moderate Risk Positions have the potential for moderate to serious impact involving duties of considerable importance to the agency mission with significant program responsibilities that affect large portions of a Computer/ADP system(s).
- Low Risk Positions have the potential for impact involving duties of limited relation to the agency mission through the use of Computer/ADP system(s).

The position risk designation system described above determines the type of investigation needed for the position. Minimum investigative requirements for the position risk levels are:

- High Risk – Background Investigation which consists of a Personal Subject Interview (PRSI); a basic National Agency Check (NAC) plus credit search; personal interviews with employment, residence, educational sources; and law enforcement searches going back 5 years. The cost for a Background Investigation is \$2,365, \$2,570, or \$2,775, depending on the speed of service (120 days, 75 days, and 35 days, respectively).
- Moderate Risk – Limited Background Investigation (LBI) or Minimum Background Investigation (MBI) may be conducted. An LBI consists of a PRSI; NAC plus credit search; personal interviews with employment (3 years), residence and educational sources (3 years); and law enforcement searches (5 years). An MBI consists of a PRSI and NAC plus credit

search covering a 5-year period. The cost for an LBI ranges from \$1,950 to \$2,260, depending on the speed of service. An MBI costs \$395.

- Low Risk – The NAC plus written inquiries sent to employers, educational institutions, law enforcement agencies, and references are required. The FDIC also requires that a credit search be conducted in conjunction with a National Agency Check and Inquiries (NACI) upon initial entry to duty for all appointees. The NACI costs \$82.

Though not a substitute for background investigations, the FDIC does have additional means for collecting data to determine employees' suitability and potential conflicts of interest. The FDIC administers the filing of public and confidential financial disclosure reports required by law for federal employees. For example, all employees, once employed by the FDIC, must file the Confidential Report of Interest in FDIC-Insured Depository Institutions Securities (FDIC Form 2410/07) and Employee Certification and Acknowledgment of Standards of Conduct Regulation (FDIC Form 2410/09). In addition, certain employees, including safety and soundness examiners and compliance examiners, are required to file Confidential Report of Indebtedness (FDIC Form 2410/06), Confidential Statement of Credit Card Obligation in Insured State Nonmember Bank and Acknowledgment of Conditions for Retention – Notice of Disqualification (FDIC Form 2410/10), and Confidential Financial Disclosure Report (FDIC Form 2410/05) (for examiners graded CG-12 and above), each on an annual basis.

SUITABILITY POSITION RISK DESIGNATION PROCESS

The FDIC has adopted the Risk Designation System established by USOPM to provide corporate officials a systematic, consistent, and uniform way of determining risk levels of positions. The Risk Designation System requires FDIC officials to designate risk levels for every position in FDIC. Circular 2120.1 directs each FDIC Division or Office Director, or designee, to determine the sensitivity level of the positions in the respective organizations. SMS is responsible for administering the designation process and making adjustments in the designations as deemed necessary. SMS is also responsible for maintaining the Position Designation Records (PDR) prepared by officials in the FDIC's divisions and offices as documentation for the designations. A copy of the PDR form can be found in Appendix II.

The Risk Designation System consists of three parts:

- Program Placement. The agency (FDIC) identifies both the impact and scope of an agency program as related to the integrity and efficiency of the service. Program placement categories are major, substantial, moderate, or limited. SMS is responsible for ensuring that each corporate program is properly designated.
- Position Risk Points. The agency determines the degree of risk that a position poses to the agency or an agency program as related to the efficiency of the service. Each of five risk factors – degree of public trust, fiduciary responsibilities, importance to program, program authority level, and supervision received -- is ranked using point values of “1” to “7” with

the higher point value being applied to the higher degree of risk. The point values are totaled to provide the total “position risk points” for a position.

- Position Placement. The Program Placement and Position Risk Points are applied to determine the risk level “position placement.” At this point, any pertinent adjustments can be made, including unique factors specific to positions as well as organizational factors, to provide uniformity of operations.

Upon completion of the three parts of the Risk Designation System, an agency decides the final placement of the position and the type of investigation to conduct. Final placement of a position falls into high risk, moderate risk, or low risk.

The USOPM Risk Designation System also includes criteria for designating Computer/ADP position risk levels. Determining a Computer/ADP position risk level is an adjustment factor on the PDR for both uniqueness and uniformity and tends to raise the risk level designation. USOPM guidance states that its Computer/ADP risk level definitions for high, moderate, and low risk positions should be applied in determining placement for any position with Computer/ADP duties. Because positions can involve determinations of risk level for both employment suitability and Computer/ADP, the higher of the two risk levels is used for final position placement. The Computer/ADP definitions are identified in the Background section of this report and can also be found in Appendix II.

The FDIC Has Not Completed Position Designation Records for All Positions

Circular 2120.1 includes a requirement that corporate officials designate risk levels for **every** (emphasis added) position in the Corporation. Such designations must be commensurate with the responsibilities and attributes of the positions as they relate to the efficiency of the Corporation’s operations. The Position Description (PD) – the official record of management’s assignment of duties, knowledge, skills, required abilities, and supervisory relationships of the position – serves as the basis for designating suitability risk levels. The divisions and offices document the designations for each PD in the PDR. SMS is responsible for maintaining the PDRs for the Corporation's positions.

The FDIC has had a long-standing initiative starting in 1994 to complete risk level designation records on all PDs in the Corporation. The completion of this initiative has been interrupted by conflicting demands on SMS resulting from major events such as: the FDIC/RTC merger; PD rewrites; National Treasury Employees Union (NTEU) objections to the Position Risk Designation Project; long-term arbitration activities to resolve NTEU concerns; corporate reorganizations; a complete revamping of the Personnel Suitability Program; and an emphasis on initiating background investigations on high risk positions. Some FDIC divisions and offices completed PDRs in 1997, 1998, and 1999 while SMS continued to identify individuals without background investigations on file. SMS officials could not be certain that all PDs in the Corporation have been properly designated. However, they were certain that all employees in high risk positions and most of the moderate and low risk employees have the proper background investigations in process or completed.

We cannot say with certainty that the FDIC has completed PDRs for every PD in the Corporation for the following reasons:

- The FDIC has not filed all of its PDRs into its Security database, the Employee Background Investigations Tracking System (EBITS).
- We found numerous instances where the Corporation's Personnel database contained inaccurate designations. For example, the Personnel database reflects low-risk, moderate-risk, and high-risk designations for OIG employees, but all OIG positions have been designated as high risk or critical sensitive for National Security purposes. We attempted to reconcile the discrepancies we found in the Personnel database and provided SMS our information for final resolution. The SMS agreed to coordinate its efforts with DOA's Personnel Services Branch (PSB).
- Some divisions and offices were completing their PDRs during the course of our review. Only a small percentage of these designations applied to new PDs.
- The PD Library on the FDIC internal Web site does not include all PDs. The PSB is in the process of revamping the FDIC's PD files and anticipates having an accurate count of the FDIC's PDs upon completion of the revamping project.

USOPM Criteria Were Not Always Consistently Applied in Determining Position Risk Levels

Most division and office officials told us they used the USOPM criteria in designating risk levels for positions in their respective organizations. We reviewed approximately 1,650 PDRs and found inconsistencies in the way some divisions and offices applied USOPM criteria to their positions. Some divisions and offices did not use the program placement level assigned by SMS in factoring the risk levels, resulting in some positions being either under-designated or over-designated. For example, one office under-designated 32 positions by determining a "limited" program placement rather than the "substantial" program placement the SMS designated for this office's program. Using USOPM criteria and SMS's "substantial" program placement, we determined that 10 of the 32 positions should be designated as high-risk, 13 positions should be designated moderate-risk with a LBI, and 9 positions should be designated moderate-risk with a MBI.

We also found that some divisions and offices designated their Administrative Officer positions as moderate risk while the same positions were designated as low-risk in other divisions and offices. Some divisions and offices designated their Secretary to the Director positions as moderate-risk, but other organizations designated this position as low risk. FDIC administratively decided that all executive positions in the Corporation are high-risk positions.

Some divisions and offices did not always appropriately consider the supervisory factor for some positions. For example, one office assigned a 3-point score to the degree of supervision received to each non-executive position in the organization, despite the fact that the grade levels of these positions ranged from grade 6 to grade 15. This office did not complete the position

risk points for its executive position, given the global high-risk designation for all executive positions.

In addition, we will be providing our analyses in this area to SMS for further review and consideration.

The FDIC's Safety and Soundness and Compliance Examiner Positions Have a Lower Risk Level Designation Than Public Trust Positions

We determined that the FDIC assigned a low-risk designation to nearly all of its safety and soundness examiner positions and its compliance examiner positions. In making its determinations, the FDIC assigned 2 points to each of the five risk factors -- degree of public trust, fiduciary responsibilities, importance to program, program authority level, and supervision received -- resulting in a total 10 points to numerically reflect the degree of risk in the safety and soundness examiner position. The 10-point score was assigned to all but one safety and soundness examiner position ranging from grades CG-11 to CG-15. The FDIC identified the program placement for the division in which safety and soundness examiners are employed as substantial. The FDIC did not use the "adjustments" feature of the Risk Designation System in determining the designations for the examiner positions. FDIC's point-assignment for its compliance examiner positions ranged from a 7-point score for examiner positions CG-5 through CG-9 to a 17-point score for examiner positions at the CG-14 grade level

Because of the low-risk designation, safety and soundness examiners and compliance examiners were only required to undergo a basic NACI, the least comprehensive investigation required, for basic employment suitability determination. According to USOPM guidelines, positions at the high or moderate risk levels are referred to as "Public Trust" positions. Based on this USOPM statement, it appears that FDIC's safety and soundness examiners and compliance examiners do not hold "Public Trust" positions. However, the duties identified for a safety and soundness examiner position recently advertised by FDIC imply that an examiner position is one that demands public confidence or trust. Specifically, on July 11, 2001, the FDIC announced an opening for a CG-13 examiner position identified as a low-risk position, involving the following duties:

"The incumbent will primarily examine insured depository institutions. The individual serves as Examiner-in-Charge of FDIC examinations, with primary responsibility for the preparation of the related report of examination. The incumbent evaluates and prepares written reports on institutions' trust departments and information systems (IS) departments. The incumbent identifies factors and causes, unsafe and unsound practices, and violations of laws and regulations that have affected, or may affect, the financial condition and soundness of financial institutions. This position involves analyzing and classifying assets; analyzing liabilities and capital; reviewing dividend and charge-off policies; analyzing earnings trends and future prospects; evaluating management and soundness of policies, procedures, and practices; analyzing liquidity and sensitivity to market risks; reviewing trust department and IS department operations and policies; and determining compliance with laws and

regulations. The incumbent will meet with insured depository institution officials and/or boards of directors to discuss the findings of an examination, corrective programs, and commitments for correction of deficiencies; develop recommendations for correcting weaknesses or deficiencies; write comments and analyses for inclusion in reports of examination; investigate financial institutions applying for deposit insurance; and participate in examinations with other federal and state examiners.”

The duties stipulated for this examiner position exceed the representative duties and responsibilities identified in USOPM guidance for a low-risk designation, namely duties and responsibilities of limited relation to an agency or program mission, so the potential for impact on the integrity and efficiency of the service is limited. The duties for the examiner position also exceed the FDIC’s definition of a low-risk position that states: “Low Risk (LR) positions involve duties with limited relations to the Corporation’s mission which have little effect on the efficiency of the Corporation’s operations or programs.”

Other financial regulatory agencies have designated their examiner positions –safety and soundness examiners and compliance examiners – at a higher than a low-risk level. The Office of the Comptroller of the Currency (OCC) designated its associate and assistant examiner positions as moderate risk with a MBI. The OCC’s examiner positions at higher grades have been designated as moderate risk requiring a more extensive LBI. The OCC’s examiner positions in its International Banking Finance group have been designated at the high-risk level and have National Security Clearances. The Office of Thrift Supervision (OTS) designated its examiner positions – safety and soundness examiners and compliance examiners – as moderate-risk positions requiring an MBI. Given the FDIC’s backup authority to participate in safety and soundness examinations of insured institutions for which the Corporation is not the primary federal regulator, it would seem appropriate that position risk designations for FDIC’s examiner positions would be at least comparable to examiner positions at other regulatory agencies such as the OCC and OTS.

ADP Responsibilities Were Not Always Considered in Position Risk Designations

Circular 2120.1 includes the following explanation for Computer/ADP position risk levels: “In accordance with Office of Management and Budget (OMB) Circular A-130, *Security of Federal Automated Information Resources*, Division of Information Resources Management (DIRM) has established personnel security policies and procedures to assure an adequate level of security for the Corporation’s automated information services. These policies include requirements for screening all individuals having access to sensitive data.” For computer/ADP positions, the level of background checks or investigations ranges from a minimal check to a full background investigation, depending upon the sensitivity of the information to be handled and the risk and magnitude of loss or harm that could be caused by the individual.

The FDIC appropriately used USOPM criteria for computer/ADP positions in determining position risk designations for the positions within DIRM and one other division. However, the other divisions and offices did not always consider the computer/ADP criteria for positions with ADP responsibilities, as implied in the title of the position. Such considerations would have

been reflected in the adjustments section of the PDR, and in our review of approximately 1,650 records, we found few examples, other than for DIRM and another division, of adjustments being made due to consideration of the computer/ADP criteria. For example, positions such as Chief, Information Management Section; Examiner (Information Systems); Supervisory Instructional Systems Design Specialist; Personnel Systems Specialist; Senior Information Management Analyst; Financial Systems Specialist; and Payroll/Personnel Systems Specialist were assigned low-risk designations, and the PDRs reflected no adjustments to the designation based on Computer/ADP considerations.

FDIC divisions and offices have Information Security Officers (ISO) with assigned security responsibilities for the systems within their respective organizations. In many cases, the ISO's security responsibilities are considered collateral duties. We identified 162 ISOs from the FDIC Web site and used the Personnel database listing of FDIC employees on board as of June 2, 2001, to determine the position risk designations for the positions held by the ISOs. We found that 61 percent of the ISOs work in positions that have been designated as low risk positions by their respective divisions and offices.

GAO recommended in its June 26, 2001 management letter, *Financial Audit: Continuing Weaknesses in FDIC's Information System General Controls*, that the FDIC study and analyze the ISO role and responsibilities and develop a process to ensure that security responsibilities are consistently applied across the FDIC. In its July 26, 2001 response to GAO, the FDIC said its Chief Information Officer initiated a project to evaluate the ISO program and to ultimately develop a "Model ISO" organization. A major aspect of the program includes establishing in all divisions full-time Information Security Manager positions, and it is expected to be implemented by December 31, 2001. DOA will have to coordinate with the Chief Information Officer to ensure that the new positions are properly designated and appropriate background checks conducted.

The area of personnel security was included in the weaknesses identified for the FDIC's information system general controls by the U. S. General Accounting Office (GAO) in its 1998, 1999, and 2000 audits of the FDIC's financial statements. GAO recognized the establishment of FDIC's *Personnel Suitability Program* in its June 26, 2001 management letter. In its letter, GAO reaffirmed its recommendations including one related to personnel security. Specifically, GAO recommended that as the FDIC identifies sensitive positions through risk assessments and security reviews of general control systems and major applications, the FDIC should ensure that users in these positions undergo the appropriate background checks. In its July 26, 2001 response to GAO, the FDIC agreed that sensitive positions should be properly identified so that the appropriate level of background check can be performed. The FDIC referenced this OIG evaluation of the FDIC's background investigations process and added that DOA planned to evaluate the results of the OIG review and make appropriate changes to the personnel suitability program as deemed necessary.

With regard to GAO's finding that risk assessments and security reviews had not been completed, the FDIC indicated in its July 26, 2001, response to GAO that Independent Security Reviews (ISR) will be completed on 28 of 29 major applications and general support systems by December 31, 2001. As these reviews are completed, DOA will have to be informed of all

employees identified as systems users with access to sensitive data for the respective applications and general support systems reviewed so that DOA can revisit the risk designations of those employees. To illustrate, the FDIC issued a report, *Independent Security Review of the FDIC Mainframe*, on December 29, 2000, which included a recommended action that the FDIC ensure procedures are in place to alert DOA of all new personnel assignments into sensitive positions to prevent any disconnect between the procedures for granting system access to users with a “sensitive” designation and DOA procedures for initiating and conducting the appropriate background checks.

BACKGROUND INVESTIGATION PROCESS

The Subcommittee requested that our review consider a series of questions related to policies and procedures of the FDIC in conducting, adjudicating, and documenting background investigations of prospective and current employees. The following sections contain responses to those questions.

1. Has the Corporation issued policies for conducting, adjudicating, and documenting background investigations of prospective and current employees?

The FDIC issued its policies and procedures for conducting, adjudicating, and documenting investigations of prospective and current employees in Circular 2120.1. We reviewed Circular 2120.1 and determined that the Circular complied with major provisions of applicable federal laws and regulations related to personnel suitability.

The directive states that it is the FDIC’s policy that employees and applicants for employment undergo a NACI with Credit, or other appropriate background investigation according to the positions held, in order to comply with the Resolution Trust Corporation Completion Act (RTCCA) and relevant federal suitability regulations. The FDIC’s policy is to employ and retain in employment only those persons who meet all federal requirements for suitability – character, reputation, honesty, integrity, trustworthiness – and whose employment or conduct would not jeopardize the accomplishment of the Corporation’s duties or responsibilities.

Circular 2120.1 states that applicants, appointees, and employees will be subject to mandatory bars outlined in 12 CFR Part 336, *Minimum Standards of Fitness for Employment with the Federal Deposit Insurance Corporation*, which prohibit any person from becoming employed by, or providing service to, the FDIC. The mandatory bars are: felony convictions, removal from or prohibition from participating in the affairs of an insured institution, defalcation in obligations to insured institutions, and causing substantial loss to deposit insurance funds. These mandatory bars are also included in the RTCCA. The FDIC requires a credit search with its background checks to comply with the RTCCA.

2. Has the Corporation issued or adopted a set of procedures, known to personnel officers and program managers, under which the policies for investigations of prospective and current employees are to be implemented?

Circular 2120.1 establishes the responsibilities, policy requirements, and procedures for the FDIC's Personnel Suitability Program. The Circular describes general provisions of the FDIC's Personnel Suitability Program, discusses the suitability position risk designation system, and provides information on investigative requirements, suitability adjudication, record keeping, and program administration matters. The Circular was issued to all employees on September 24, 1999. The provisions of Circular 2120.1 apply to all applicants, appointees, and employees of the Corporation.

Although FDIC employees have access to Circular 2120.1 through the FDIC internal Web site, the directive is not accessible to applicants for corporate positions on the FDIC's external Web site. We reviewed recent FDIC vacancy announcements and found the announcements included a statement on the position sensitivity and type of background investigation required for the advertised position. For instance, a recent announcement for an examiner-in-charge position included the following:

"Position Sensitivity: Low Risk--National Agency Check Investigation
Required: see Circular 2120.1, dated 9/24/1999."

However, the Circular is not accessible to an applicant without contacting the FDIC to obtain a copy. DOA should consider establishing a link to Circular 2120.1 on the vacancy announcement to provide external applicants an easy access to the Circular and an explanation of the background investigation required for the advertised position.

3. Have the procedures been recently reviewed and revised?

The FDIC's current Circular 2120.1, issued on September 24, 1999, is a revision of Circular 2120.1, *Personnel Security Program*, dated July 3, 1978. When the FDIC created SMS in late 1995, the Corporation recognized that the personnel security directive was out of date and required significant revisions. SMS drafted a revision to the directive. However, a number of objections were raised by NTEU, and the directive could not be finalized until NTEU's concerns were resolved. Ultimately, SMS met with the NTEU and a federal mediator to resolve the concerns, and a Memorandum of Understanding (MOU) was signed by NTEU and the Corporation representing the agreements reached concerning the implementation of the FDIC's security and suitability program insofar as it affects bargaining unit employees.

The MOU, signed in September 1999, includes the following provisions:

- That NTEU be consulted about high risk designations before notifying the employees.
- That a notification to the employee must include an explanation of the reasons why the position has been designated as high risk.
- That all job announcements or other solicitations of interest for positions should identify the position risk designation and the nature of the investigation required.

- That only those employees in positions designated as “High Risk” will be subject to periodic reinvestigations, which shall occur not more than one in every five years.

4. How does the FDIC monitor compliance with these procedures?

SMS is responsible for implementing the FDIC's suitability program. Since its creation in late 1995, SMS has been involved in various initiatives to monitor and improve the personnel suitability program. Recent efforts include the following:

- In 1999, SMS reviewed security and personnel records in Headquarters and regional offices for employees identified as not having suitability investigations. SMS focused its efforts on high risk employees followed by moderate and low risk employees. The Assistant Director, SMS, was very confident that background investigations for all employees designated high risk were either in process or completed. SMS requested that USOPM complete 782 investigations during the period from October 1, 2000 to June 15, 2001.
- SMS has a database, EBITS, to track information related to the personnel suitability program. SMS said that EBITS had not been populated with background investigation information on all employees. FDIC's DIRM recently made SMS-requested modifications to EBITS, but those fields have not been populated with data. SMS does not rely on EBITS, but instead uses Excel spreadsheets, tickler files and manual reports to track background investigations.
- The Assistant Director, SMS, is a member of a multi-agency task force, Security Clearance Automation Laboratory, Phase II (SECLEAR II), whose goal is to identify best practices of security management tracking systems. SECLEAR II membership includes representatives from the Departments of Justice, Commerce, and Energy, as well as the FDIC and the USOPM. According to its charter, the mission of SECLEAR II is “..to create a process to achieve efficient and timely staffing of critical positions by integrating automated security forms and processing capabilities.” The Assistant Director, SMS, told us that one of the advantages of his participation in SECLEAR II is to learn about best practices that could be applied to EBITS to meet reporting requirements and better integrate EBITS with other personnel systems.
- SMS provides DOA senior management and the FDIC’s Office of Internal Control Management a biweekly report on the status of background investigations. As mentioned earlier, SMS uses Excel spreadsheets, tickler files, and manual reports to track the status of background investigations. The latest report, dated August 1, 2001, contained the following:

Table 1: DOA Status Report 08/01/2001

Category	Total Number	Completed Investigation	Pending Adjudication	In process at USOPM	Forms pending completion by employee	Forms pending completion for interns
High Risk	605	549	4	36	16	n/a
Low and Moderate Risk	5,951	5,684	45	201	17	4
Total	6,556	6,233	49	237	33	4

Source: DOA Background Investigation Status Report 08/01/2001

- The DOA Management Review Group (MRG) completes Administrative Compliance Reviews (ACR) for DOA's Washington and regional offices. For example, an ACR of the Washington office, dated March 28, 2000, reported that background investigations were completed on all employees hired between January 1999 and June 1999.
- The Personnel Suitability Program was reviewed as a part of GAO's audit of FDIC's financial statements.
- SMS is currently completing a self-assessment at the request of and under the supervision of the USOPM.

5. What evidence do you have to demonstrate that the Corporation has implemented these procedures in a manner that minimizes the risk of improper access, use, or manipulation of sensitive private financial data?

The Subcommittee's request letter emphasizes the importance of background investigations in helping to minimize the risk that sensitive and private financial data utilized by federal financial regulatory agencies is improperly accessed, used, or manipulated. The letter states:

"That risk could arise not only from contractors whose backgrounds have not been sufficiently investigated, but also from the Corporation's own employees, prospective and current. It is critical to the safety and security of the financial services industry, and to consumers' confidence in the industry's ability to protect personal financial data, that federal employees with actual or potential access to such data meet stringent security conditions and are subject to periodic investigations throughout their career. Recent disclosures in the intelligence community are an embarrassing reminder that we cannot assume that veteran employees need not be periodically re-investigated. "

The FDIC's personnel suitability program was designed to help ensure that the Corporation employs and retains in employment only those individuals who meet all federal requirements for suitability and whose employment or conduct would not jeopardize the accomplishment of the FDIC's duties or responsibilities. Our review showed that the FDIC generally conducted, adjudicated, and documented background investigations for current and prospective employees in accordance with corporate personnel suitability requirements. However, we cannot demonstrate that the FDIC's implementation of its personnel suitability program completely minimizes the risk of improper access, use, or manipulation of sensitive private financial data due to the issues discussed earlier in this report regarding the FDIC's position risk designation process.

We reviewed security folders or Official Personnel Folders for 236 of the 240 employees in our sample to determine if background investigations were performed and adjudicated. No folders were available for 4 of the 240 employees because they were no longer employed by the FDIC.

In our review of the 236 folders, we found that the FDIC generally conducted, adjudicated, and documented background investigations according to FDIC policies and procedures except for the following:

- Background investigations were not completed for two newly hired employees who worked in positions designated as low risk.
- Folders for nine employees did not contain background investigations.
- Folders for eight employees, who work in positions designated as moderate risk, contained evidence of a NACI, a less extensive investigation than the required LBI or MBI for a moderate risk position.

In regard to the nine employees whose folders contained no evidence of background investigations, SMS officials told us that other sources, such as USOPM, could be used to determine if background investigations had been completed for the nine employees. However, we did not complete that alternative testing because we chose to review documentation maintained by the FDIC.

Appendix III summarizes the results of our testing. In addition, we will be providing our detailed analysis in this area to SMS for further review and resolution.

We reviewed the timeliness of the adjudication process for background investigations after the FDIC hires an applicant. The FDIC contracts with USOPM to complete background investigations. After the investigation is completed, USOPM forwards the investigation and a preliminary adjudicating suitability assessment. USOPM may identify issues and grade them on a scale of A-D, of which D is the most serious. SMS officials could not recall any FDIC cases that were graded D. Furthermore, SMS officials stated that most issues identified by USOPM are related to overseas travel and small credit issues.

SMS reviews the background investigation and if necessary completes additional research. In some cases, SMS contacts the employee orally or in writing to get more information. If an issue may have a potential effect on a person's employment with the FDIC, SMS contacts the Labor and Employee Relations Section of the PSB.

SMS uses USOPM guidance to make an adjudication decision. In addition to adjudicating the case based on USOPM standards, SMS reviews each case file to make sure that there are no violations of the RTCCA.

We obtained information from security folders on investigations requested and adjudicated by SMS. We did not include employees whose background investigations were completed by another agency. There were 98 cases within our sample of 240 employees that included sufficient information to determine the timeliness of the adjudication process.

As shown in Table 2, the average time from completed investigation to FDIC adjudication for 98 cases was 19 days.

Table 2: Average Days from Completed Investigation to Adjudication

Category	Number of cases with information on FDIC investigation and adjudication	Average Days from Completed Investigation to Adjudication
High Risk	54	22
Moderate Risk	11	20
Low Risk	7	10
Promotions and Reassignments	10	16
New Hires	16	17
Total	98	19

Source: OIG analysis of selected security folders

6. Are background investigations of prospective employees conducted prior to hiring? Provide analysis demonstrating that Corporation managers adjudicate the results in a timely manner, so troublesome cases are quickly resolved prior to final employment decisions. Provide proof that the results of the investigations are documented in personnel files.

The FDIC performs pre-employment checks on prospective employees before they are hired. Once an applicant is selected for a vacancy, the hiring office sends the applicant's OF-306 (Declaration for Federal Employment) or resume to SMS. SMS, based on information in the OF-306 or resume, does the following:

- Completes a background check,
- Contacts USOPM to see if they have any record of investigation on the applicant, and
- Contacts any federal agencies where the applicant has been employed.

If there are no issues, SMS notifies the hiring office by electronic mail that the applicant can be hired by the FDIC. If issues arise during the pre-employment checks that may preclude employment, SMS discusses the issues with the hiring office and PSB. PSB may request additional information or explanation from the applicant. SMS officials said they could not remember a recent case of a prospective employee being denied employment at the FDIC.

We selected a sample of 30 employees hired by the FDIC during the period January 1, 2000 through June 2, 2001. We found that pre-employment checks were conducted for 24 of the 30 employees prior to hiring. Those pre-employment checks were completed an average of 29 days prior to hiring. The following information is related to the remaining six cases:

- Pre-employment checks were not completed for two employees until after they were hired. The pre-employment check was completed an average of 10 days after hiring. However, appropriate background investigations were adjudicated favorably for the two employees.
- There was no information in one employee's security folder. The employee was a secretary who is now on leave without pay.
- There were no security folders for three employees because they were no longer employed by FDIC.

7. Are current employees periodically re-investigated throughout their careers, and are such re-investigations adjudicated and documented to the same extent as investigations for prospective employees?

FDIC Circular 2120.1 states: "The incumbents of Public Trust Positions designated High Risk are subject to periodic reinvestigation at least once every 5 years after placement."

Our sample of 240 employees included 26 employees whose periodic reinvestigations were in process (5 cases) or completed (21 cases). Based on our review, we found that:

- The FDIC sent 18 cases to USOPM for investigation an average of 1,810 days after the previous background investigation. The Circular requires a reinvestigation every 5 years (1,825 days).
- The FDIC did not send eight cases to USOPM within 5 years. Those cases were sent to USOPM for investigation an average of 1,982 days after the previous background investigation. The median for the eight cases was 1,907 days.

We found that the 26 periodic reinvestigations in our sample were documented to the same extent as the previous background investigations.

CONCLUSIONS AND RECOMMENDATIONS

We determined that the FDIC has implemented a process for determining suitability risk levels for its positions. However, the FDIC needs to do more to ensure that all corporate positions have risk designations, they are commensurate with assigned responsibilities, and are reflected accurately in corporate databases. We also determined that the FDIC generally conducted, adjudicated, and documented background investigations for current and prospective employees in accordance with the Corporation's policies and procedures.

While the FDIC has undertaken a series of initiatives designed to improve the personnel suitability program, further actions are needed. We recommend that the FDIC:

1. Involve SMS in the Position Description revamping project.
2. Assess the need to complete new Position Designation Records for position risk designations where FDIC divisions and offices inconsistently applied USOPM criteria in making the designations.
3. Consult with the Division of Supervision and Division of Compliance and Consumer Affairs to re-designate position sensitivity levels for their examiner positions to reflect their public trust responsibilities.
4. Ensure that divisions and offices alert SMS of all personnel assignments to positions where users have access to sensitive computer systems or data.

5. Ensure that SMS coordinates with the Chief Information Officer to ensure that new Information Security Manager positions are properly designated and appropriate background checks are performed.
6. Ensure that all position risk designations are completed and accurately reflected in the Corporation's databases.
7. Establish a specific schedule to update the Corporation's employee security database, EBITS.
8. Consider establishing a link to Circular 2120.1, *Personnel Suitability Program*, in position vacancy announcements.

CORPORATION COMMENTS AND OIG EVALUATION

On August 15, 2001, the Director, DOA, provided a written response to the draft report. The Director, DOA, tentatively agreed with the eight recommendations. The response is presented in Appendix IV of this report.

The Director, DOA, stated that since the recommendations involve a number of FDIC divisions and offices, the DOA Security Management Section will assess each recommendation and will work with the other affected divisions and offices to develop specific action plans. The Director, DOA, will issue a separate memorandum to the OIG by September 15, 2001, summarizing the planned corrective actions and providing expected completion dates along with the documentation that will confirm completion. The OIG will evaluate the FDIC's planned corrective actions and provide the results of our analysis to the Subcommittee.

Evaluation Methodology

To address the first objective of evaluating FDIC's process for conducting, adjudicating, and documenting background investigations of prospective and current employees, our methodology included:

- Identifying employees on board as of June 2, 2001 and selecting a statistical sample of 240 employees to include 30 employees in each of the following categories:
 1. High Risk Positions located in Headquarters.
 2. High Risk Positions located in the eight Regional Offices.
 3. Moderate Risk Positions located in Headquarters.
 4. Moderate Risk Positions located in the eight Regional Offices.
 5. Low Risk Positions located in Headquarters.
 6. Low Risk Positions located in the eight Regional Offices.
 7. Employees hired by the FDIC during from January 1, 2000 through June 2, 2001.
 8. Promotions from January 1, 2000 through June 2, 2001.
- Selecting security folders and Official Personnel Folders for the 240 employees to review for evidence of background investigations and adjudicative activities.
- Comparing information in the FDIC's Personnel database to the FDIC's Employee Security database.
- Reviewing applicable laws, regulations, USOPM guidance, and FDIC procedures on the requirements for background investigations.
- Interviewing key officials in SMS, divisions, and offices.
- Reviewing management reports, prior audit reports, and Administrative Compliance Review reports.

To address the objective of assessing whether the FDIC has effectively implemented a process to ensure that positions have appropriate risk designations, our methodology included:

- Reviewing applicable laws, regulations, USOPM guidance related to its Risk Designation System, and FDIC procedures on the requirements for position risk designations.
- Interviewing SMS officials and officials in 16 FDIC divisions and offices to obtain an understanding of the FDIC's position risk designation process.
- Reviewing approximately 1,650 Position Designation Records completed by 16 divisions and offices.
- Interviewing officials in the Office of the Comptroller of the Currency and Office of Thrift Supervision regarding position risk designations for examiner positions.
- Reviewing U.S. General Accounting Office audit reports, independent security review report, and FDIC vacancy announcements.

Excerpts of USOPM Guidance for Position Risk Designations

DRAFT

731-7

Subchapter 2. Suitability Position Risk Criteria and Levels**2-1. GENERAL REQUIREMENTS**

Every competitive service position must be designated at a position risk level commensurate with the public trust responsibilities and attributes of the position as they relate to the efficiency of the service. The suitability risk levels are ranked according to the degree of adverse impact on the efficiency of the service that an unsuitable person could cause.

2-2. RISK DESIGNATION SYSTEM

To determine position risk levels under this chapter, a Risk Designation System is used to assure that positions are designated uniformly and consistently by Federal agencies. Appendix A provides the requirements and steps of the Risk Designation System.

Federal agency positions designated under FPM chapters 731, issued in FPM basic installments 311 and 347, will not require re-designation until positions are filled or new positions are established. Those positions previously designated as sensitive, but did not have national security duties and/or access to classified information, will be considered to fall under the position risk levels described in this chapter. For example:

- Special-Sensitive and Critical-Sensitive positions would be considered to be at the High Risk Level.
- Noncritical-Sensitive positions would be considered to be at the Moderate Risk Level.
- Non-Sensitive positions would be considered to be at the Low Risk Level and remain as Non-Sensitive.

Accordingly, future actions taken on previously designated positions as described above should be in accordance with the procedures of this chapter.

2-3. CRITERIA AND LEVELS

a. **Public Trust Positions** are those which have the potential for action or inaction by their incumbents to affect the integrity, efficiency, effectiveness, of assigned Government activities. The potential for adverse effect includes action or inaction which could diminish public confidence in the integrity, efficiency, or effectiveness of Government activities, whether or not actual damage occurs.

Certain Government activities by their nature can be adversely affected by the action or inaction of most employees associated with the activity in any responsible capacity. Such activities include law enforcement, public safety and health, collection of revenue, and regulation of business, industry, or finance. Other Government activities, not by their nature having as great an impact upon the Nation generally, include particular functions having the potential for damage. Thus, positions having authority to commit Government funds through grants, loans, loan guarantees, or contracts, would be public trust positions. Finally, positions in any activity which are responsible for managing programs or operations require a high degree of public trust because of their ability to affect the accomplishment of the activity's mission to a significant degree. Included in this latter category are positions responsible for managing a significant portion of a program, such as a geographic district or area.

Excerpts of USOPM Guidance for Position Risk Designations

DRAFT

731-8

CHAPTER 731. PERSONNEL SUITABILITY

b. **Risk Levels.** The three suitability position risk levels are as follows:

<i>SUITABILITY POSITION</i>	
<i>ADVERSE IMPACT ON THE EFFICIENCY OF THE SERVICE</i>	
High Risk (HR) Public Trust Position	Positions included are those that have the potential for <i>exceptionally serious</i> impact involving duties especially critical to the agency or a program mission with broad scope of policy or program authority such as: <ul style="list-style-type: none"> — policy development and implementation; — higher level management assignments; or — independent spokespersons or non-management positions with authority for independent action.
Moderate Risk (MR) Public Trust Position	Positions included are those that have the potential for <i>moderate to serious</i> impact involving duties of considerable importance to the agency or program mission with significant program responsibilities and delivery of customer services to the public such as: <ul style="list-style-type: none"> — assistants to policy development and implementation; — mid-level management assignments; — non-management positions with authority for independent or semi-independent action; or — delivery of service positions that demand public confidence or trust.
Low Risk (LR)	Potential for impact involving duties of <i>limited relation</i> to the agency mission with program responsibilities which affect the efficiency of the service.

In most cases, particularly at the Low Risk level, position risk is relatively clear, and the application of special designating procedures may not prove necessary. Similarly, essentially identical positions may require only occasional case-by-case analysis. But in all these cases, even where risk levels may appear to be "obvious," the designation should be tested by random application of specific procedures. Agencies with unique missions or unique suitability and/or Computer/ADP requirements may propose for OPM's approval alternative procedures better suited to agency needs. At the very least, each agency must demonstrate that it has adopted an OPM-approved system for designating suitability-based risk levels. The system need not conform in every detail to the one adopted and recommended by OPM, but it must include the same factors as listed in appendix A and should result in substantially the same designation as under the OPM system. OPM examines these procedures in its ongoing evaluation of agency operations.

2-4. RELATIONSHIP BETWEEN SUITABILITY RISK LEVELS AND NATIONAL SECURITY SENSITIVITY LEVELS

a. FPM chapter 732 describes national security position sensitivity, which includes suitability considerations. With some exceptions, the national security positions, exclusive of suitability, relate to requirements for access to classified information and sensitive, restricted facilities.

b. Suitability is a consideration for every position. Fewer positions are subject to the national security considerations in sensitivity designations under FPM chapter 732. Those positions deemed sensitive on the basis of national security requirements are subject primarily to the requirements of FPM chapter 732.

Inst.
August 16, 1991

DRAFT

Federal Personnel Manual

PM 13-7

Excerpts of USOPM Guidance for Position Risk Designations

DRAFT

731-23

Subchapter 7. Computer/ADP Position Risk Criteria and Levels

7-1. SECURITY OF FEDERAL AUTOMATED INFORMATION SYSTEMS

Under OMB Circular No. A-130 (December 12, 1985), the Director, Office of Personnel Management, is to maintain personnel security policies for Federal personnel associated with the design, programming, operation, maintenance, or use of Federal automated information systems. Agencies are instructed to establish and manage personnel security policies and procedures to assure an adequate level of security for Federal automated information systems. In accordance with OMB Circular A-130, agency policies and procedures for the security of Federal automated information systems must conform to the OPM guidance in this subchapter, which applies to all Federal employees.

Policies established and maintained by the agencies are to include requirements for screening all individuals participating in the design, development, operation, or maintenance of sensitive applications as well as those having access to sensitive data. The level of screening required by these policies is to vary from minimal checks to full background investigations, depending upon the sensitivity of the information to be handled and the risk and magnitude of loss or harm that could be caused by the individual.

7-2. COMPUTER SECURITY ACT OF 1987 (P.L. 100-235)

The Computer Security Act of 1987 (P.L. 100-235) requires Federal agencies to identify each computer system that contains sensitive infor-

mation and to prepare a plan for the security and privacy of each such system. It further requires that agencies provide for periodic training in security awareness for all personnel involved in the use or operation of these systems.

"Sensitive information" is defined as any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has *not* been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

7-3. CRITERIA AND RISK LEVELS

The Computer/ADP risk levels and criteria are to be used as an integral part of Suitability Position Risk Designation Systems described in appendix A. In determining position placement, in addition to public trust criteria, any position with Computer/ADP duties should have the following criteria applied.

a. The three Computer/ADP position risk levels are as follows:

COMPUTER/ADP RISK LEVELS	ADVERSE IMPACT ON COMPUTER/ADP SECURITY
High Risk (HR) Public Trust Position	Potential for <i>exceptionally serious</i> impact involving duties especially critical to the agency mission with broad scope and authority, and with major program responsibilities which affect a major Computer/ADP system(s).
Moderate Risk (MR) Public Trust Position	Potential for <i>moderate to serious</i> impact involving duties of considerable importance to the agency mission with significant program responsibilities which affect large portions of a Computer/ADP system(s).
Low Risk (LR)	Potential for impact involving duties of <i>limited relation</i> to the agency mission through the use of Computer/ADP system(s).

DRAFT

Excerpts of USOPM Guidance for Position Risk Designations

DRAFT

731-24

CHAPTER 731. PERSONNEL SUITABILITY

b. Risk Level Criteria:

High Risk. Includes any position at the highest level of risk to the Computer/ADP system. This is to include positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; has a major responsibility for the direction, planning, and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with relatively high risk for causing grave damage or realizing a significant personal gain. Such positions may involve:

- Responsibility for the development and administration of agency computer security programs, and also including direction and control of risk analysis and/or threat assessment.
- Significant involvement in life-critical or mission-critical systems.
- 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 grave damage or realizing significant personal gain.
- Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of \$10 million per year or greater, or (2) lesser amounts if the activities of the individual are not subject to technical review by higher authority to insure the integrity of the system.
- Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.
- Other positions as designated by the agency head that involve relatively high risk for effecting grave damage or realizing significant personal gain.

Moderate Risk. Includes positions in which the incumbent is responsible for the direction, planning, design, operation, or main-

tenance of a computer system, and whose work is technically reviewed by a higher authority at the high risk level to insure the integrity of the system. Such positions may involve:

- Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority at the High Risk level, to insure the integrity of the system. This level includes, but is not limited to:
 - (a) access to and/or processing of proprietary data, Privacy Act of 1974, and Government-developed privileged information involving the award of contracts;
 - (b) accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than \$10 million per year.
- Other positions as designated by the agency head that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in High Risk positions.

Low Risk. Includes all Computer/ADP positions not falling into one of the above risk levels.

c. In order to establish uniformity and objectivity agencies must make Computer/ADP risk designations in a systematic manner. Agencies should refer to instructions in appendix A of this chapter and FPM chapter 732 for specific guidelines that may be applicable to the final designation.

7-4. SUITABILITY RISK LEVEL - COMPUTER/ADP RISK LEVEL INTER- RELATIONSHIPS

As positions may involve determinations of risk levels for both Suitability and Computer/ADP, the higher of the two is used to determine possible adverse impact of the position and final risk level.

DRAFTInst.
August 15, 1991

Federal Personnel Manual

Excerpts of USOPM Guidance for Position Risk Designations

DRAFT

731-A-1

APPENDIX A**Risk Designation System**

Introduction: This designation system provides a systematic way of obtaining uniformity in Risk Level designations:

To Determine General Risk Criteria:

— For placement of agency, programs, and positions

To Apply Criteria:

— For Suitability
..... FPM 731 Subchapter 2

— For Computer/ADP
..... FPM 731 Subchapter 7

— For National Security
..... FPM 732 Subchapters 2 and 6

To Obtain Final Position Risk Level:

— High Risk FPM 731

— Moderate Risk FPM 731

— Low Risk FPM 731

— National Security Sensitivity Levels FPM 732

When an agency, a program, or a position/group of positions is fully or predominantly involved in national security/access to classified information, the criteria and designation procedures in FPM chapter 732 may apply in full or together with the Public Trust criteria of chapter 731.

The Risk Designation System: The Risk Designation System process is divided into three parts:

- I:** Designation of an agency and program for its impact (Major, Substantial, Moderate, or Limited) and scope (Worldwide, Governmentwide, Multi-agency, or Agency) as related to the efficiency of the service.
See page 731-A-2.
- II:** Designation of the position(s) for its degree of risk upon the program as related to the efficiency of the service. Degree of risk is divided into four categories (Major, Substantial, Moderate, and Limited), and is calculated in five factor description areas (Degree of Public Trust, Fiduciary

(Monetary) Responsibility, Importance to Program, Program Authority, and Supervision Received).

See page 731-A-3.

- III:** Final designation of position risk includes using parts I and II to determine Position Placement, followed by adjustments which include descriptions of *unique* factors specific to positions and organizational *uniformity* of operations. These steps should be taken to arrive at the final designation of the position. When it is obvious that part III will place the position at a higher risk level, then the other steps may not be needed.

See page 731-A-4.

Adjustments: Adjustments made to the Sensitivity Designation System in Basic Installment 347, September 29, 1988, Chapter 731, Appendix A, will not require agencies to re-designate existing positions with the Risk Designation System in this appendix.

The adjustments made reflect the changes made to FPM chapters 731, 732, and 736, and are intended to retain position designation based on risks as described. The principal adjustments were made to consolidate and reduce the number of factors used to arrive at levels in parts I and II. The end result is to prevent over- or under-designation in determining low, moderate, and high risk levels and compatibility with the three levels of position sensitivity in FPM chapter 732.

DRAFT

Excerpts of USOPM Guidance for Position Risk Designations

DRAFT

731-A-2

CHAPTER 731. PERSONNEL SUITABILITY

If a program has more than one area of primary focus, or if questions arise as to placement of a program at one of two impact descriptions (e.g., Substantial or Moderate), decision should be based on the best interests of the agency mission. If the program is primarily based on national security, apply FPM chapter 732.

(2) **Scope of Operations in Terms of the Efficiency of the Service:** Scope of operations is described in the columns of the table below.

(3) **Determining Program Placement:** The program placement is designated at the intersection of the appropriate row and column.

(4) **Examples:** Substantial impact + Multi-agency scope = Substantial; and Limited impact + Worldwide scope = Moderate.

I: DESIGNATING PROGRAM PLACEMENT

(1) **Impact on the Efficiency of the Service:** Impact of the program, described in the rows of the table below, is determined by identifying the area of primary program focus, and then relating that area to one of these impact descriptions:

- accounting for, auditing or disbursement of public funds;
- administrative, regulatory or policy control over public and/or private programs or operations;
- protection of the national security;
- enforcement of Federal laws; or
- protection of life or property.

	SCOPE OF OPERATIONS			AGENCY: Operations of the agency, or an agency's region or area, with primary focus extending to the elements in the private sector impacted by the agency.
	WORLDWIDE: Operational activity is carried out worldwide, with primary focus in either the public or the private sector.	GOVERNMENTWIDE: Operational activity is carried out Governmentwide, to all sectors, with primary focus on the public sector Governmentwide.	MULTI-AGENCY: Nationally or regionally with primary focus extending to more than one agency in the public sector, or to the elements in the private sector impacted by the agencies.	
IMPACT				
MAJOR: Impacts directly on the survival, stability, and continued effectiveness of Government operations, the promotion of major Government fiscal goals, or a primary social, political, or economic interest of the nation.	MAJOR	MAJOR	SUBSTANTIAL	MODERATE
SUBSTANTIAL: Impacts directly on the efficiency and effectiveness of a sizeable segment of the Federal workforce, or the interests of large numbers of individuals in the private sector.	MAJOR	SUBSTANTIAL	SUBSTANTIAL	MODERATE
MODERATE: Impacts directly on the effectiveness of an agency's operations, the fiscal interests of an agency, or affects the social, political or economic interests of individuals, businesses or organizations in the private sector.	SUBSTANTIAL	MODERATE	MODERATE	LIMITED
LIMITED: Limited impact on the operational effectiveness of one or a few programs in an agency, or the interests of a limited number of individuals in the private sector.	MODERATE	MODERATE	LIMITED	LIMITED

PROGRAM PLACEMENT

1st
August 15, 1991

DRAFT

DM 12-77

Federal Personnel Manual

Excerpts of USOPM Guidance for Position Risk Designations

Appendix A. Risk Designation System

DRAFT

731-A-3

II: DESIGNATING POSITION RISK POINTS

degree of impact (points may also be assigned at the 2, 4, and 6 points values). The greater the impact, the more points assigned. After points are assigned for all five risk factors, the sum is used to arrive at the position risk points.

(1) In designating position placement, the duties and responsibilities of the position must be considered in the context of the program and the risk that position has for damage or abuse to the program. Criteria for national security in FPM chapter 732 should be used in lieu of the descriptions below when appropriate.

(2) Points are assigned under each risk factor, to reflect numerically the

(3) *Example:* Substantial Degree of Public Trust (6 points), Substantial (Monetary) Fiduciary Responsibility (6 points), Limited Importance to Program (1 point), Limited Program Authority (1 point), and Moderate Supervision (3 points) = 16 position risk points (5+6+1+1+3=16)

DEGREE	RISK FACTOR DESCRIPTIONS					DEGREE
	DEGREE OF PUBLIC TRUST: The consensus of confident expectation for honesty, integrity, reliability, or responsibility, or justice placed in a position.	FIDUCIARY (MONETARY) RESPONSIBILITY: Authority or ability to obligate, control or expend public money or items of monetary value (bonds, etc.) value.	IMPORTANCE TO PROGRAM: Impact the individual position has, due to status, influence on the program as a whole, either individually or collectively.	PROGRAM AUTHORITY: Ability to manipulate authority or control the outcome or results of all or key portions of a program or policy.	SUPERVISION RECEIVED: Frequency work is reviewed and nature of the review.	
MAJOR: Potential for independently compromising the integrity and effectiveness of a major program element or component, or in conjunction with others, damaging all phases of program operations.	7	7	7	7	7	Limited: Occasional review only with respect to major policy issues by superior without expertise in the technical aspects of program policy and operations.
SUBSTANTIAL: Potential for reducing the efficiency of overall program operations, or the overall operations of major program elements or components independently, or through collective action with others.	5	5	5	5	5	Periodic: Ongoing spot review of policy and major operational considerations of work by superior, with some knowledge of program operations, but with minimal technical program expertise.
MODERATE: Potential for reducing the efficiency of the overall or day-to-day operations of a major program element or component, through independent action or collectively with others.	3	3	3	3	3	Moderate Technical: Ongoing spot review of work in connection with important operational issues by superior with technical program expertise.
LIMITED: Potential for damage not meeting above criteria.	1	1	1	1	1	Close Technical: Continuing review of all phases of work by superior with technical program expertise.

POSITION RISK POINTS

DRAFT

Excerpts of USOPM Guidance for Position Risk Designations

DRAFT

731-A-4

CHAPTER 731. PERSONNEL SUITABILITY

III: PLACEMENT AND ADJUSTMENTS

when such investigation is considered warranted. An agency may also make written recommendation to OPM-OPI to conduct another type of background investigation with justification on how it would meet its mission and requirements.

(1) Placement: The results of Part I and Part II placement are next applied to the chart below to obtain Placement into Risk Levels, and to pair each risk level with the type of background investigation required. None of the required investigations are intended to restrict an agency from conducting a more comprehensive investigation than that prescribed

(2) Examples: I. Moderate + II. 22 points = III. Moderate Risk (MBI); I. Major + II. 9 points = III. Low Risk (NACI).

		II. POSITION RISK POINTS					
		5-10	11-17	18-23	24-29	30-33	34-35
I. PROGRAM PLACEMENT	MAJOR	Low Risk (LR) NACI	Moderate Risk (MR) LBI	Moderate Risk (MR) LBI	High Risk (HR) BI	High Risk (HR) BI	High Risk (HR) BI
	SUBSTANTIAL	Low Risk (LR) NACI	Moderate Risk (MR) MBI	Moderate Risk (MR) LBI	Moderate Risk (MR) LBI	High Risk (HR) BI	High Risk (HR) BI
	MODERATE	Low Risk (LR) NACI	Low Risk (LR) NACI	Moderate Risk (MR) MBI	Moderate Risk (MR) MBI	Moderate Risk (MR) LBI	High Risk (HR) BI
	LIMITED	Low Risk (LR) NACI	Low Risk (LR) NACI	Low Risk (LR) NACI	Low Risk (LR) NACI	Moderate Risk (MR) LBI	High Risk (HR) BI

POSITION RISK LEVEL AND TYPE OF BACKGROUND INVESTIGATION

(3) Adjustments: Some positions, by the very nature of the duties and responsibilities of the program or the positions, will require designation at certain levels of risk. Final adjustment in the designation process must take into account *unique* factors specific to positions and the organizational need for *uniformity* of operations.

(a) Uniqueness: Factors that are unique and are not fully accounted for in the program or position designation system that can cause adjustments include:

- Special investigative or criminal justice duties;
- Control of an automated monetary system (key access entry);

— Few-of-a-kind positions with special duties (Special Assistant to Agency Head);

— Support positions with no responsibilities for preparation or implementation of Public Trust program policies and plans, but involving regular contact with, and ongoing knowledge of, all or most of such material (e.g., Budget Analyst);

— Any of the criteria appearing in FPM chapter 732, 2-3.

— Any other factors the agency thinks relevant (must be documented).

DRAFT

Excerpts of USOPM Guidance for Position Risk Designations

DRAFT

Appendix A. Risk Designation System

731-A-5

HIGH RISK (HR)
 MODERATE RISK (MR)
 LOW RISK (LR)

Examples of all parts in the process:

- I = Moderate Program
 II = Position Risk Points: 20
 III = Placement: Moderate Risk (MBI)
 Adjustments: Special Assistant (Criminal Justice)
 Final Placement: Moderate Risk (LBI)
- I = Substantial Program
 II = Position Risk Points: 29
 III = Placement: Moderate Risk (LBI)
 Adjustments: None
 Final Placement: Moderate Risk (LBI)

(b) Uniformity: Clearly indicated needs for uniformity in position designations, because of authority level or program placement level that may serve as a basis for making the adjustments include:

- Agency head may adjust position designations at the same authority level to assure uniformity within the agency (e.g., managers of major agency programs at the same level of authority may be placed at the same level of risk).
- If the placement level of the program is determined to be so overriding as to negate any specific risk considerations associated with individual positions within the program, the agency head may designate all positions within the program at the risk level that is required to best protect the efficiency of the service.
- In assigning position risk points in part II, adjustments may also be made by assigning points at the 2, 4, and 6 points values.

Only after careful analysis of the position in terms of these factors and this need should any decision on adjustment be made. Final position risk levels will be one of the following:

DRAFT

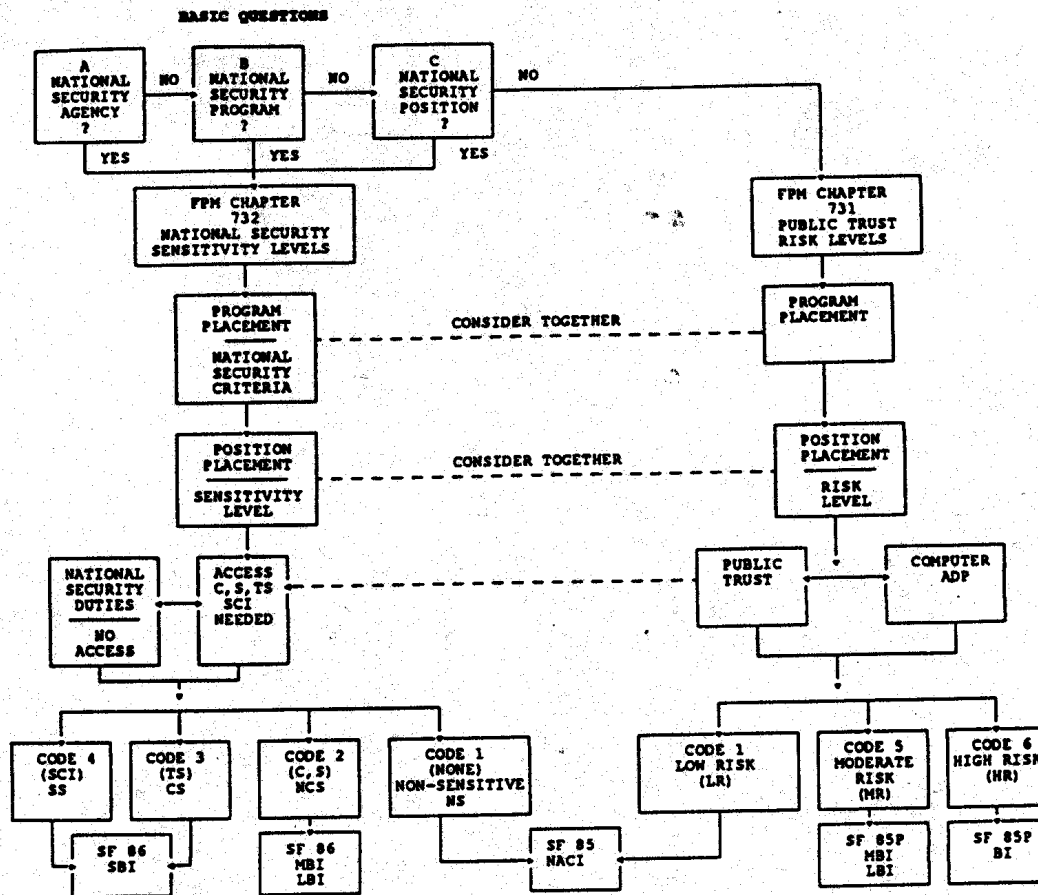
Excerpts of USOPM Guidance for Position Risk Designations

DRAFT

731-A-6

CHAPTER 731. PERSONNEL SUITABILITY

Position Designation Matrix - FPM 731 Public Trust and/or FPM 732 National Security:



EXAMPLES OF POSITIONS:

(1) Access (SCI): Special-Sensitive (SS) - highest requirements - use SF 86 (clearly national security) - do SBI (required) - no need to perform position sensitivity or risk level designations.

(2) National Security duties based on principal agency mission/No access to classified information: Noncritical-Sensitive (NCS) (low points) - Computer/ADP (High Risk) - use SF 86 (because of national security duties) - do BI (because of public trust risk)

(3) Public trust position - Moderate program - 22 points/with access (C): Moderate Risk (MR) (MBI) - use SF 86 (because of (C) access) - Risk level moderate and 22 points = (MBI)

(4) Public trust position - High Risk/No access to classified information: (No Sensitivity) - use SF 85P - do BI (required for High Risk (HR))

Inst. August 15, 1991

Federal Personnel Manual

Excerpts of USOPM Guidance for Position Risk Designations

DRAFT

Appendix A. Risk Designation System

731-A-7

Position Designation Records:

Agency Personnel Offices will maintain a record of the suitability designation process or it may be kept by the Agency Security Offices with National Security Sensitivity Designation record as outlined in FPM chapter 732. The form below, or

its agency equivalent, is subject to review by OPM during periodic appraisals of agency suitability programs, or on a case-by-case basis, as required, to assure that positions are properly designated in terms of the efficiency of the service.

POSITION DESIGNATION RECORD	
AGENCY: _____	PROGRAM: _____
POSITION TITLE: _____	
POSITION DESCRIPTION #: _____	
RISK DESIGNATION SYSTEM	
<u>I. PROGRAM PLACEMENT:</u>	
Impact on Efficiency of Service:	_____
Scope of Operations for Efficiency of Service:	_____
Placement (Major, Substantial, Moderate, Limited):	_____
<u>II. POSITION PLACEMENT:</u>	
<u>Risk Factors</u>	<u>Risk Points</u>
a. Degree of Public Trust (7-1):	_____
b. Fiduciary Responsibilities (7-1):	_____
c. Importance to Program (7-1):	_____
d. Program Authority Level (7-1):	_____
e. Supervision Received (7-1):	_____
TOTAL POINTS	_____
<u>III. POSITION PLACEMENT (HR; MR; LR):</u>	
Adjustments (Include Computer-ADP Position Risk Criteria):	_____
Comments:	_____
<u>FINAL PLACEMENT (Risk level/Sensitivity level/Access level):</u>	

Signature of Agency Designator	

Date	

DRAFT

Results of Background Investigation Testing

The following table is a summary of the testing for each sample subset:

Category	Universe	Sample Size	Security Folders Reviewed	# of Background Investigations Completed or In Process	Official Personnel Folders Reviewed	# of Background Investigations Completed or In Process	Total Background Investigations Completed and In Process	Evidence of No Background Investigation	Number of Cases Without Background Investigation Information
High Risk - DC	347	30	29	29	1	0	29	0	1
High Risk - Region	103	30	29	29	1	1	30	0	0
Moderate Risk - DC	780	30	9	9	21	19	28	0	2
Moderate Risk - Region	524	30	8	8	22	20	28	0	2
Low Risk - DC	1,314	30	8	8	22	19	27	0	3
Low Risk - Region	3,427	30	5	5	25	24	29	0	1
New Hires	467	30	27	25	0	0	25	2	3 (No longer employed by the FDIC)
Promotions	1,832	30	13	13	16	16	29	0	1 (No longer employed by the FDIC)
Total	8,794	240	128	126	108	99	225	2	13

Source: OIG Analysis of Security Folders and Official Personnel Folders

Corporation Comments


**FDIC**

Federal Deposit Insurance Corporation
550 17th Street, NW, Washington, DC 20429

Division of Administration

August 15, 2001

MEMORANDUM TO: Stephen M. Beard
Assistant Inspector General

FROM: Arleas Upton Kea 
Director, Division of Administration

SUBJECT: Management Response to the OIG Report: *Evaluation of FDIC's Background Investigation Process for Prospective and Current Employees*

The Division of Administration (DOA) is in receipt of the subject Office of Inspector General (OIG) report. We appreciate the review performed by the OIG and its recommendations to enhance and improve the overall Personnel Suitability Program at the Federal Deposit Insurance Corporation (FDIC). DOA understands the importance of background investigations in minimizing the risk that sensitive and private financial data could be accessed, misused, or manipulated. The safety and security of the financial services industry and the consumer's confidence in the FDIC's ability to protect personal financial data is tantamount to our mission.

The OIG lists in its report eight recommendations addressed to the FDIC's Division of Administration (DOA). We tentatively agree with the recommendations. However, since the recommendations involve a number of FDIC division and offices, the DOA Security Management Section will assess each recommendation fully and, working with the other affected divisions and offices, will develop specific action plans. A separate memorandum will be issued to the OIG by September 15, 2001, summarizing these planned corrective actions and providing expected completion dates along with the documentation that will confirm completion.

If you have any questions regarding the response, our point of contact for this matter is Andrew Nickle, Audit Liaison for the Division of Administration. Mr. Nickle can be reached at (202) 942-3190.

cc: Michael Rubino
William Kmetz
Vijay Deshpande