

---

# Table of Contents

## VOLUME 1

### 1 Overview of Bank Security

---

¶ 1.01	THE NATURE OF PRIVATE SECURITY .....	1-1
	[1] A Brief History of Bank Security .....	1-1
	[2] The Growing Role of Private Security .....	1-2
¶ 1.02	THE BANK PROTECTION ACT OF 1968 .....	1-2
	[1] Regulations Under the Act .....	1-3
	[a] Security Officer .....	1-3
	[b] Security Devices .....	1-4
	[c] Security Procedures .....	1-4
	[d] Filing of Reports .....	1-4
	[2] The May 1991 Revision .....	1-5
	[a] Designation of Security Officer .....	1-5
	[b] Security Program .....	1-5
	[c] Report .....	1-6
	[d] Bank Secrecy Act Compliance .....	1-7
¶ 1.03	INDUSTRY COMPLIANCE WITH THE BANK PROTECTION ACT OF 1968 .....	1-7
¶ 1.04	SEC RULE 17F-1: REPORTING OF MISSING, LOST, COUNTERFEIT, OR STOLEN SECURITIES .....	1-7
	[1] Institutions Covered Under the Program .....	1-8
	[2] Reporting Requirements .....	1-8
	[3] Inquiry Requirements .....	1-9
	[4] Securities Information Center, Inc. ....	1-10
	[a] Access Codes .....	1-10
	[b] Responses to Hits .....	1-11
	[c] Inquiries .....	1-11
¶ 1.05	SEC RULE 17F-2: FINGERPRINTING REQUIREMENTS .....	1-12
	[1] Persons to Be Fingerprinted .....	1-12
	[2] Exceptions to the Rule .....	1-12
	[3] Records and Reporting .....	1-13
	[4] Fingerprinting Pursuant to Other Law .....	1-13
	[5] Fingerprinting Plans of Self-Regulatory Organizations .....	1-14
¶ 1.06	THE BANK SECRECY ACT .....	1-14
	[1] Compliance Procedures .....	1-14
	[2] Department of Treasury Regulation .....	1-14

### 2 Crimes Against Financial Institutions and Relevant Criminal Laws

---

¶ 2.01	GROWTH AND IMPACT OF CRIMES AGAINST FINANCIAL INSTITUTIONS .....	2-1
	[1] Growth of Violent Crimes .....	2-1
	[2] Growth of White-Collar Crimes .....	2-2
	[a] Impact on Banks .....	2-2

## TABLE OF CONTENTS

	[b] FDIC Improvement Act of 1991.....	2-4
	[c] Increased Prosecution Efforts.....	2-5
	[d] FDIC Bank Failure Analysis 1985–1995.....	2-6
	[e] Civil Actions Against Directors, Officers, and Institution-Affiliated Parties.....	2-6
<b>¶ 2.02</b>	<b>VIOLENT CRIMES</b> .....	2-7
	[1] Bank Robbery .....	2-7
	[a] Profile of Bank Robbers .....	2-7
	[b] Bank Robbery Prosecutions.....	2-9
	[c] Bank Robbery Statistics.....	2-9
	[2] Burglary .....	2-12
	[3] Kidnapping and Extortion.....	2-14
	[4] Attacks on Customers.....	2-15
	[a] ATM Violent Crime.....	2-15
	[b] Night Depository Violent Crime.....	2-16
	[c] Civil Liability Considerations .....	2-16
<b>¶ 2.03</b>	<b>WHITE-COLLAR CRIME</b> .....	2-19
	[1] Causes for Increase in White-Collar Crime.....	2-20
	[a] Less Stringent Punishment Through the Courts .....	2-20
	[b] Insufficient Preemployment Screening.....	2-20
	[c] Diminishing Role of Federal Law Enforcement Officials .....	2-21
	[d] Changing Morality .....	2-21
	[e] Expanding International Technology.....	2-21
	[2] Embezzlement, Theft, or Misapplication of Bank Funds .....	2-21
	[a] Embezzlement and Misapplication Statutes.....	2-22
	[b] Bank Fraud Statute.....	2-25
	[c] False Bank Entries.....	2-26
	[d] Embezzler Traits .....	2-27
	[3] Loan Fraud .....	2-28
	[a] Commercial and Consumer Loans.....	2-29
	[b] Mortgage Loans .....	2-29
	[c] “Prime Bank” Notes.....	2-31
	[4] Check Fraud .....	2-31
	[a] Check Forgery .....	2-32
	[b] Check Kiting.....	2-32
	[5] Card Fraud.....	2-33
	[a] Credit Card.....	2-33
	[b] Debit (ATM and POS) Card .....	2-36
	[c] Credit and Debit Card Criminal Laws.....	2-36
	[6] Advance-Fee Schemes.....	2-37
	[7] Shell Corporations .....	2-38
	[a] Offshore Shell Banks .....	2-39
	[8] Brokered-Loan Fraud.....	2-40
	[9] Computer Crime.....	2-43
	[a] Computer Fraud Laws .....	2-46
	[b] Computer Crime Surveys.....	2-47
	[10] Traveler’s Check Fraud.....	2-47
	[11] Counterfeiting .....	2-48

**TABLE OF CONTENTS**

	[a] U.S. Currency .....	2-48
	[b] Securities .....	2-48
	[c] Commercial Instruments .....	2-49
	[12] Theft of Securities .....	2-49
	[13] Wire Fraud .....	2-50
	[14] Bank Bribery .....	2-50
	[15] Interstate Commerce of Stolen Property .....	2-51
	[16] Telemarketing Fraud .....	2-53
	[17] Mail Fraud .....	2-53
	[18] Racketeer Influenced and Corrupt Organizations Act (RICO) .....	2-54
	[19] OFAC Laws, Embargoed Countries, Penalties .....	2-55
	[a] Trading With the Enemy Act (TWEA) .....	2-55
	[b] International Emergency Economic Powers Act (IEPPA) .....	2-55
	[c] Iraq Sanctions Act .....	2-55
	[d] United Nations Participation Act (UNPA) .....	2-55
	[e] International Security and Development Corporation Act (ISDCA) .....	2-55
	[f] Title 18 of the U.S. Criminal Code .....	2-55
	[20] Identity Theft .....	2-56
	[21] Money Laundering .....	2-56
	[22] The Economic Espionage Act of 1996 .....	2-56
	[23] Telephone Records and Privacy Protection Act of 2006 .....	2-57
	[24] Financial Institutions Preventing Child Pornography .....	2-57
<b>¶ 2.04</b>	<b>SUSPICIOUS ACTIVITY REPORTING .....</b>	<b>2-57</b>
	[1] Federal Reserve Board .....	2-60
	[2] Comptroller of the Currency .....	2-60
	[3] Federal Deposit Insurance Corporation .....	2-60
	[4] Office of Thrift Supervision .....	2-60
	[5] National Credit Union Administration .....	2-61
	[6] Preparation Guidelines for Suspicious Activity Report .....	2-61
	[a] FinCEN Guidelines .....	2-61
	[b] FBI Guidelines .....	2-61

**3 Security Department: Structure and Function**

---

<b>¶ 3.01</b>	<b>RESPONSIBILITIES AND DUTIES OF THE SECURITY DEPARTMENT .....</b>	<b>3-1</b>
	[1] Physical Security .....	3-1
	[2] Personnel Security .....	3-4
	[3] Information Security .....	3-4
	[4] Crime Prevention and Detection .....	3-5
	[5] Investigations .....	3-5
<b>¶ 3.02</b>	<b>STRUCTURE OF THE SECURITY DEPARTMENT STAFF .....</b>	<b>3-7</b>
	[1] Position Description .....	3-7
	[a] Security Officer .....	3-7
	[b] Protection Manager .....	3-8
	[c] Investigations Manager .....	3-9
	[2] Stress in the Security Operation .....	3-9
	[3] Security Officer Designation .....	3-10
	[a] Security Officer Qualifications .....	3-10

[b]	Psychological Screening for Bank Security Officers .....	3-11
[c]	Certification for Bank Security Officers .....	3-11
[4]	Reporting Level.....	3-13
<b>¶ 3.03</b>	<b>RISK MANAGEMENT .....</b>	<b>3-13</b>
[1]	Security Officer's Role .....	3-14
[a]	Asset Identification.....	3-14
[b]	Team Approach .....	3-15
[2]	Special Considerations for Identification of Information and Information Systems.....	3-15
[a]	Classify and Rank Sensitive Data, Systems, and Applications .....	3-15
[b]	Assess Threats and Vulnerabilities .....	3-16
[c]	Evaluate Control Effectiveness .....	3-16
[d]	Assign Risk Ratings .....	3-17
[3]	Types of Insurance Coverage .....	3-17
[a]	Financial Institution Bond .....	3-17
[b]	Financial Institution Bond Deductibles .....	3-19
[c]	Master Trust Policies .....	3-19
[d]	Miscellaneous Policies .....	3-19
[4]	Environmental Risk .....	3-20
[a]	Environmental Risk Analysis.....	3-21
[b]	Loan Documentation.....	3-21
[c]	Monitoring .....	3-21
[d]	Training .....	3-21
[5]	Standards for Safety and Soundness .....	3-22
<b>¶ 3.04</b>	<b>ROLE OF THE SECURITY DEPARTMENT IN CORPORATE PLANNING .....</b>	<b>3-22</b>
[1]	Bank Profitability and the Security Function.....	3-22
[2]	Auditing the Performance of the Security Department.....	3-23
[3]	The Security Officer's Role in the Audit .....	3-24
<b>¶ 3.05</b>	<b>USE OF OUTSIDE SECURITY CONSULTANTS .....</b>	<b>3-25</b>
[1]	Selecting the Consultant .....	3-25
[2]	Working With the Consultant .....	3-26
[3]	A Word About Fees.....	3-26
<b>¶ 3.06</b>	<b>CODE OF ETHICS FOR SECURITY PERSONNEL.....</b>	<b>3-26</b>
[1]	ASIS Code of Ethics .....	3-27
<b>¶ 3.07</b>	<b>WRITTEN SECURITY PROCEDURES .....</b>	<b>3-28</b>
[1]	Model Security Procedure.....	3-33

## **4 Physical Security for the Institution**

---

<b>¶ 4.01</b>	<b>SECURITY OFFICER RESPONSIBILITIES .....</b>	<b>4-1</b>
[1]	Physical Security Equipment Inventory.....	4-2
[2]	UL-Approved Security Equipment.....	4-2
<b>¶ 4.02</b>	<b>ALARM SYSTEMS.....</b>	<b>4-3</b>
[1]	Alarm System Definitions.....	4-3
[2]	Burglar Alarm Systems .....	4-5
[a]	Local Alarm Systems .....	4-6
[b]	Police Station-Connected Systems.....	4-6
[c]	Central Station Alarm Systems .....	4-7

## TABLE OF CONTENTS

	[d] Proprietary Systems.....	4-10
	[e] Transmission Line Security.....	4-10
[3]	Protection of Building's Perimeter and Interior.....	4-11
[4]	Vault, Safe, ATM, and Night Depository Alarms.....	4-11
	[a] Vaults.....	4-12
	[b] Safes.....	4-12
	[c] Night Depositories and ATMs.....	4-12
[5]	Holdup Alarms.....	4-13
	[a] Holdup Buttons.....	4-13
	[b] Holdup Footprints.....	4-14
	[c] Money Clips.....	4-14
[6]	Fire Alarms.....	4-14
[7]	Importance of Maintaining an Up-to-Date System.....	4-14
<b>¶ 4.03</b>	<b>CAMERA SURVEILLANCE EQUIPMENT.....</b>	<b>4-15</b>
[1]	Selecting Equipment.....	4-16
	[a] Closed-Circuit Television.....	4-17
	[b] Sequence Bulk Film Cameras.....	4-19
	[c] Demand Bulk Film Cameras.....	4-20
	[d] Lens Selection.....	4-20
[2]	Positioning Surveillance Camera Equipment.....	4-20
<b>¶ 4.04</b>	<b>PROTECTIVE LIGHTING.....</b>	<b>4-21</b>
[1]	Applications for Financial Institutions.....	4-21
	[a] Vault Illumination.....	4-22
	[b] High-Exposure Area Illumination.....	4-22
	[c] Customer-Service Area Illumination.....	4-22
	[d] Parking Lot Illumination.....	4-22
[2]	Selecting Equipment.....	4-23
	[a] Types of Protective Lighting.....	4-23
	[b] Sources of Light.....	4-23
[3]	Positioning of Lighting.....	4-24
<b>¶ 4.05</b>	<b>LOCKS.....</b>	<b>4-24</b>
[1]	Key Locks.....	4-24
[2]	Combination Locks.....	4-25
[3]	New Key Technology.....	4-27
[4]	Delayed-Action Time Locks.....	4-27
[5]	Electromechanical Locks.....	4-28
[6]	Developing a Control System.....	4-28
	[a] Keylock Control.....	4-28
	[b] Combination Control.....	4-29
[7]	Lock Installation.....	4-30
<b>¶ 4.06</b>	<b>SAFES: PHYSICAL SPECIFICATIONS.....</b>	<b>4-30</b>
[1]	UL-Approved Chests.....	4-30
	[a] UL-Approved Safes.....	4-30
	[b] Night Depositories.....	4-32
[2]	Previously Approved Chests.....	4-33
	[a] Auxiliary Safes.....	4-33
	[b] Night Depositories.....	4-33

	[c] ATMs .....	4-34
	[3] Selection of Equipment—Safes and Night Depositories .....	4-34
<b>¶ 4.07</b>	<b>VAULTS</b> .....	4-34
	[1] Vault Standards Formerly Required by the Bank Protection Act.....	4-35
	[2] Insurance Service Office Standards.....	4-35
	[3] ASTM Standard .....	4-35
	[4] Modular Vaults .....	4-36
	[5] Vault Doors .....	4-37
<b>¶ 4.08</b>	<b>ACCESS CONTROL AND IDENTIFICATION SYSTEMS</b> .....	4-37
	[1] Access Control.....	4-37
	[2] Identification.....	4-37
	[3] Biometric Personal Identification Systems .....	4-38
	[a] Fingerprints .....	4-39
	[b] Eye Scan.....	4-40
	[c] Hand Geometry.....	4-40
	[d] Finger Vein.....	4-40
	[e] Voice Patterns.....	4-40
	[f] Signature.....	4-40
	[g] Face Image .....	4-40
	[h] Facial Thermogram.....	4-40
	[i] Biometric Examples .....	4-40.1
	[4] Radio-Frequency Identification (RFID) Systems .....	4-40.1
<b>¶ 4.09</b>	<b>BANKING OFFICE DESIGN</b> .....	4-41
	[1] Visibility.....	4-43
	[2] Design and Layout.....	4-43
	[a] Customer Entrance .....	4-44
	[b] Teller Counter .....	4-44
	[c] Bullet-Resistant Barriers .....	4-45
	[d] Window Film .....	4-46
	[3] Landscaping Safety Considerations.....	4-46
<b>¶ 4.10</b>	<b>COUNTER AUDIO</b> .....	4-46.1
	[1] Listening Devices.....	4-46.1
	[2] Countermeasures .....	4-47
<b>¶ 4.11</b>	<b>USE OF GUARDS</b> .....	4-48
	[1] Justifying Guards .....	4-48
	[a] Research Phase .....	4-48
	[b] Risk Checklist .....	4-49
	[c] Implementing the New Approach .....	4-49
	[2] Choosing a Contract Guard Service .....	4-50
	[3] Using Public Police as Guards.....	4-51
	[a] Liability for Actions .....	4-52
	[b] Control of Work.....	4-52
	[c] Deep Pockets.....	4-53
	[4] Using Bullet-Proof Vests .....	4-53
	[a] Concealability and Comfort.....	4-53
	[b] Construction of the Vest.....	4-54
	[5] Armed vs. Unarmed Guards .....	4-54

**TABLE OF CONTENTS**

	[6] Private Security Officer Employment Authorization Act .....	4-55
<b>¶ 4.12</b>	<b>DYE PACKS</b> .....	4-56
<b>5</b>	<b>Computer Security for Financial Institutions</b>	
<b>¶ 5.01</b>	<b>COMPUTER EXPOSURE</b> .....	5-1
	[1] Risk Assessment .....	5-1
	[a] Lessons Learned From the Year 2000 Project .....	5-2
	[2] Safety and Soundness .....	5-4
	[a] GAO Concerns About Safety and Soundness .....	5-5
	[3] Legal .....	5-6
	[4] Data Processing Terms .....	5-6
	[5] Computer Risks .....	5-6
	[a] Theft of Currency and Other Financial Assets .....	5-7
	[b] Theft or Destruction of Computer Hardware or Software .....	5-7
	[c] Loss of Data Processing Capability .....	5-7
	[d] Theft of Customer or Institutional Data .....	5-8
	[e] Computer Viruses .....	5-9
	[f] Service Contracts .....	5-11
	[g] Vulnerabilities on the Internet .....	5-11
<b>¶ 5.02</b>	<b>COMPUTER FRAUD LEGISLATION</b> .....	5-11
	[1] Federal Laws .....	5-12
	[a] Computer Fraud and Abuse Act of 1986 .....	5-12
	[b] Telecommunications Law .....	5-12
	[c] Federal Computer Crime Law—Statute and OCC Guidance .....	5-12
	[2] State Computer Crime Laws .....	5-13
<b>¶ 5.03</b>	<b>COMPUTER SECURITY PROGRAM</b> .....	5-14
	[1] Architectural Guidelines .....	5-15
	[2] Organization Principles .....	5-15
	[a] Control Domains .....	5-15
	[b] Levels of Understanding .....	5-16
	[3] Baseline Security Controls .....	5-16
	[a] The Baseline Concept .....	5-16
	[b] Control Objectives .....	5-17
	[c] Baseline Control Benefits .....	5-17
	[4] Security Monitoring .....	5-18
<b>¶ 5.04</b>	<b>COMPUTER SECURITY PROGRAM CONTROL DOMAINS</b> .....	5-18.1
	[1] Management Control .....	5-18.1
	[a] Assignment of Responsibility .....	5-18.1
	[b] Users .....	5-18.1
	[c] Data Processing Management .....	5-18.1
	[d] Auditor .....	5-19
	[e] Data Security Officer .....	5-20
	[f] FDIC Auditing Checklist .....	5-21
	[2] Communications Control .....	5-22
	[a] Communications Networks .....	5-22
	[b] Information Integrity .....	5-23
	[3] Systems and Applications Controls .....	5-24

	[a] Authorized Access .....	5-24
	[b] Information Integrity .....	5-26
	[c] Privacy .....	5-26
	[d] Viruses .....	5-27
[4]	Operational Controls .....	5-27
	[a] Authorized Usage .....	5-27
	[b] Process Integrity .....	5-28
	[c] Verification .....	5-28
	[d] Change Management .....	5-29
[5]	Personnel Security .....	5-29
	[a] Systems Access .....	5-29
	[b] Systems Logging .....	5-30
[6]	Physical Security .....	5-31
	[a] Site Selection .....	5-31
	[b] Design and Construction Characteristics .....	5-31
	[c] Fire Protection .....	5-32
	[d] Access Control .....	5-33
	[e] Physical Security in Distributed Environments .....	5-34
[7]	Contingency Controls .....	5-35
	[a] Corporate Business Resumption and Contingency Planning .....	5-35
	[b] Federal Financial Institutions Examination Council Policy .....	5-36
<b>¶ 5.05</b>	<b>END-USER COMPUTING</b> .....	5-37
	[1] Risks Involved .....	5-38
	[2] Controls at the End-User Level .....	5-38

## **6 Contingency Planning for Financial Institutions**

---

<b>¶ 6.01</b>	<b>THE NEED FOR CONTINGENCY PLANNING</b> .....	6-1
	[1] The 9/11 Commission Report .....	6-2
	[a] A Nation at War .....	6-2
	[b] Knowing Your Enemy's Beliefs .....	6-2
	[c] Islamic Fundamentalism .....	6-3
	[d] Osama bin Laden .....	6-3
	[e] Al Qaeda—An International Organization .....	6-4
	[f] Key Points for Security Planning .....	6-4
	[2] Homeland Security Act of 2002 .....	6-5
	[a] U.S. Department of Homeland Security .....	6-6
	[3] President's Commission on Critical Infrastructure Protection .....	6-10
	[a] Financial Services Sector Coordinating Council .....	6-11
	[b] Financial Services Information Sharing and Analysis Center .....	6-11
	[c] Protected Critical Infrastructure Information Program .....	6-12
	[4] FFIEC Policy on Contingency Planning .....	6-12
	[5] International Terrorism .....	6-13
<b>¶ 6.02</b>	<b>LEVELS OF RESPONSIBILITY FOR CONTINGENCY PLANNING</b> .....	6-14
	[1] U.S. Government Preparedness .....	6-14
	[2] Financial Institution Responsibility .....	6-14
	[a] Corporate Capacity for Succession .....	6-15

## TABLE OF CONTENTS

	[b] Corporate Policy Statement .....	6-15
	[c] A Sample Policy Statement.....	6-15
<b>¶ 6.03</b>	<b>RISK ASSESSMENT IN CONTINGENCY PLANNING .....</b>	<b>6-15</b>
	[1] Assessing Risks.....	6-16
	[2] Human-Induced Events .....	6-17
	[a] IT System Intrusions and Systems Failures .....	6-17
	[b] Kidnapping, Hostage-Taking, and Extortion.....	6-18
	[c] Bomb Threats and Bombings.....	6-18
	[d] Terrorism.....	6-19
	[e] Sabotage.....	6-20
	[f] Nuclear War .....	6-20
	[g] Riots and Civil Disturbances .....	6-21
	[h] Electrical Blackouts and Brownouts .....	6-21
	[i] Fire.....	6-21
	[3] Natural Events and Pandemics.....	6-22
<b>¶ 6.04</b>	<b>DEVELOPING THE CONTINGENCY MANAGEMENT PLAN .....</b>	<b>6-22</b>
	[1] Contingency Management Planning Officer Responsibility.....	6-22
	[2] Designation of Contingency Management Team .....	6-23
	[3] Establishing Command Centers.....	6-23
	[4] Communications .....	6-23
	[5] Evaluating Critical Needs.....	6-24
	[a] Policies and Procedures .....	6-24
	[b] Key Personnel.....	6-24
	[c] Temporary Office Facilities .....	6-25
	[d] Information Technology Systems.....	6-25
	[e] Medical and HAZMAT Supplies .....	6-25
	[6] Recovery Priorities.....	6-25
	[7] Vital Records .....	6-26
	[8] Electronic Imaging Systems.....	6-26
<b>¶ 6.05</b>	<b>DEVELOPING AND WRITING THE CONTINGENCY PLAN .....</b>	<b>6-28</b>
	[1] Bomb Threats and Bombings .....	6-29
	[a] Intelligence Assessment .....	6-29
	[b] Precautions in Advance of Any Bomb Threat.....	6-29
	[c] Procedure if a Bomb Threat Is Received .....	6-30
	[d] Developing an Evacuation Procedure .....	6-30
	[e] Bombing Devices in Safe Deposit Boxes .....	6-31
	[f] Suspected Mail Bombs .....	6-31
	[2] Kidnapping, Hostage-Taking, and Extortion.....	6-33
	[a] Employee Training .....	6-33
	[b] Obtaining Information From the Perpetrator.....	6-33
	[c] If the Victim Is Brought to the Premises .....	6-34
	[d] Developing a Ransom Payment Policy .....	6-34
	[e] Guidelines for Ransom Payment .....	6-34
	[f] Key Points for the Kidnapping Plan.....	6-35
	[g] Insurance .....	6-35
	[3] Riots and Civil Disturbances .....	6-36
	[a] Legal Considerations .....	6-36

## TABLE OF CONTENTS

	[b] Personnel Safety.....	6-36
[4]	Electrical Failures.....	6-36
[5]	Fire.....	6-37
	[a] Fire Wardens .....	6-37
	[b] Evacuation .....	6-38
	[c] Training.....	6-38
[6]	Flooding, Snowstorms, Earthquakes, and Windstorms.....	6-38
[7]	Nuclear Attack.....	6-38
	[a] Property Protection .....	6-38
	[b] Personnel Protection.....	6-39
	[c] Storing Vital Records .....	6-39
	[d] Post-Attack Operations .....	6-39
[8]	Radiological Dispersion Device.....	6-42
[9]	Biological Weapons .....	6-42
	[a] Anthrax .....	6-43
[10]	Pandemics .....	6-46
	[a] The Federal Government.....	6-46
	[b] States and Localities.....	6-46.2
	[c] The Private Sector and Critical Infrastructure Entities.....	6-46.2
[11]	Chemical Weapons.....	6-46.3
	[a] Choking Agents.....	6-46.3
	[b] Blister Agents.....	6-46.3
	[c] Nerve Agents .....	6-46.3
	[d] Blood Agents.....	6-46.4
[12]	Potential Indicators of Weapons of Mass Destruction (WMD) Threats or Incidents .....	6-46.4
[13]	Exercise the Plan .....	6-46.4
	[a] Planning an Exercise .....	6-46.5
	[b] Performing an Exercise.....	6-46.5
<b>¶ 6.06</b>	<b>INTERAGENCY POLICY ON CONTINGENCY PLANNING FOR FINANCIAL INSTITUTIONS.....</b>	<b>6-46.6</b>

## **7 Security for the Human Resources Department**

<b>¶ 7.01</b>	<b>APPLICANT SCREENING .....</b>	<b>7-1</b>
	[1] Training the Personnel Interviewer .....	7-1
	[2] The Employment Application .....	7-2
	[a] Topics That Should Be Questioned .....	7-2
	[b] Questions Concerning Criminal Records .....	7-2
	[c] Consent Agreements .....	7-3
	[d] Applicant's Signature .....	7-3
	[3] Fingerprinting.....	7-3
	[a] How to Submit Fingerprint Cards .....	7-4
	[4] Federal Deposit Insurance Act, Section 19.....	7-5
	[a] General Guidelines .....	7-5
	[b] FDIC Consent Application.....	7-5
	[c] Revisions to Consent Applications.....	7-6
	[d] Persons Covered .....	7-6
	[e] Exclusions from Section Applicability.....	7-7

**TABLE OF CONTENTS**

	[f] FDIC Review Process for Consent Applications .....	7-7
	[g] Pending Employee Criminal Cases.....	7-7
[5]	Verification Procedures.....	7-8
	[a] Mail Reference Check.....	7-8
	[b] Investigative Agencies .....	7-9
	[c] Polygraph Tests.....	7-9
	[d] Using Pre-Employment Assessments.....	7-10
	[e] Computerized Source Records.....	7-13
[6]	Fair Credit Reporting Act .....	7-14
	[a] Amendments to the Fair Credit Reporting Act.....	7-14
	[b] Human Resources Impact.....	7-15
	[c] Civil Liability for Willful Noncompliance.....	7-15
	[d] Civil Liability for Negligent Noncompliance .....	7-16
[7]	Medical History .....	7-16
	[a] Controlled Substance Testing.....	7-16
	[b] Urinalysis and Hair Testing Chain of Custody.....	7-17
	[c] Drug Testing Statistics .....	7-18
[8]	Private Security Officer Employment Authorization Act .....	7-18
	[a] Definitions .....	7-18
	[b] Method for Conducting FBI Criminal History Searches.....	7-19
	[c] Criminal Penalties .....	7-19
<b>¶ 7.02</b>	<b>SECURITY ASPECTS OF SUBSTANCE ABUSE .....</b>	<b>7-19</b>
	[1] Suggested Written Policy Regarding Use of Alcohol .....	7-20
	[2] Suggested Written Policy Regarding Use of Controlled Substances .....	7-21
	[3] Signs of Alcoholism.....	7-22
	[4] Controlled Substance Abuse .....	7-22
	[a] Types of Controlled Substances .....	7-23
	[b] Some General Symptoms of Drug Abuse .....	7-24
	[c] Specific Symptoms .....	7-24
	[d] Noninvasive Detection .....	7-27
<b>¶ 7.03</b>	<b>COMPULSIVE GAMBLING .....</b>	<b>7-28</b>
	[1] Signs of Gambling.....	7-28
	[2] Suggested Written Policy Regarding Gambling .....	7-29
<b>¶ 7.04</b>	<b>CODE OF CONDUCT.....</b>	<b>7-29</b>
	[1] Elements of a Code of Conduct .....	7-30
	[2] Foreign Corrupt Practices Act of 1977 .....	7-32
	[3] Bank Bribery Law.....	7-33
	[a] Justice Department Policy.....	7-34
	[b] Federal Banking Supervisory Guidelines .....	7-34
	[4] Implementing an Effective Ethics Program .....	7-38
<b>¶ 7.05</b>	<b>THE AMERICANS WITH DISABILITIES ACT .....</b>	<b>7-38.2</b>
	[1] Disability Defined .....	7-38.2
	[2] Preemployment Screening.....	7-38.2
	[3] Reasonable Accommodation .....	7-40
<b>¶ 7.06</b>	<b>WORKPLACE VIOLENCE .....</b>	<b>7-40</b>
	[1] Situational Example .....	7-41
	[2] Historical Violence in America .....	7-41

[3]	Violence in the American Workplace .....	7-41
[4]	Significant Workplace Problem .....	7-42
[5]	Interpersonal Acts of Violence .....	7-43
	[a] Warning Flags.....	7-43
[6]	Written Plan .....	7-45
[7]	Prevention Controls .....	7-46
	[a] Management’s Position.....	7-46
	[b] Policies and Procedures .....	7-46
	[c] Training of Managers .....	7-47
	[d] New Employee Screening.....	7-47
	[e] Communications .....	7-47
	[f] Employee Input.....	7-47
[8]	Employee Assistance Program.....	7-48
[9]	Employee Terminations .....	7-48
[10]	Security Program Interface .....	7-48
[11]	Security Personnel Training.....	7-49
[12]	Criminal Justice System.....	7-49
[13]	Problem Reaction .....	7-49
[14]	Incident Management .....	7-49
<b>¶ 7.07</b>	<b>VACATION POLICIES .....</b>	<b>7-49</b>
	[1] Situational Example .....	7-50
	[2] Industry Standard.....	7-50
	[3] Exceptions to Industry Standard.....	7-51
	[4] FDIC Policy.....	7-51

## **8 Data Security and the Internet**

---

<b>¶ 8.01</b>	<b>FINANCIAL TRANSACTIONS AND THE INTERNET .....</b>	<b>8-1</b>
	[1] The Internet .....	8-1
	[2] Electronic Data Interchange.....	8-2
	[3] Federal Criminal Laws and the Internet .....	8-3
	[a] Procedures for Suspected Computer Crime .....	8-3
	[b] Types of Computer Crimes Investigated by the FBI.....	8-4
	[c] CSI Computer Crime Survey.....	8-4
	[4] Corporate Financial Exposure .....	8-4
<b>¶ 8.02</b>	<b>SECURITY RISKS ASSOCIATED WITH THE INTERNET .....</b>	<b>8-5</b>
	[1] Technological Advances .....	8-5
	[2] Security Concerns.....	8-6
	[a] Data Privacy and Confidentiality .....	8-6
	[b] Data Integrity.....	8-6
	[c] Authentication .....	8-6
	[d] Nonrepudiation.....	8-6
	[e] Access Control and System Design.....	8-6
	[3] The Pitfalls of the Internet .....	8-8
	[a] Cyber Crime and Terrorism.....	8-9
	[b] Theft and Denial-of-Service Attacks by Hackers.....	8-13
	[c] Computer Viruses .....	8-13
	[d] Foreign Government Threats .....	8-14

**TABLE OF CONTENTS**

	[e] Competitors and the Theft of Proprietary Information .....	8-14
	[f] Identity Theft .....	8-14
[4]	Web-Linking Risks .....	8-17
[5]	Wireless Technology.....	8-17
[6]	Software Vulnerabilities .....	8-18
[7]	Surviving Internet Attacks .....	8-18
[8]	Voice Over Internet Protocol.....	8-19
<b>¶ 8.03</b>	<b>SECURITY REQUIREMENTS FOR ONLINE FINANCIAL TRANSACTIONS .....</b>	<b>8-19</b>
[1]	Internet Security Policy .....	8-19
[2]	Data Privacy and Confidentiality .....	8-20
[3]	Data Integrity .....	8-20
[4]	Identification and Authentication .....	8-20
[5]	Nonrepudiation.....	8-21
[6]	Access Control/System Design.....	8-21
<b>¶ 8.04</b>	<b>SECURITY CONTROLS FOR ONLINE FINANCIAL TRANSACTIONS .....</b>	<b>8-21</b>
[1]	Encryption .....	8-21
	[a] Public Keys .....	8-22
	[b] Secret Keys.....	8-22
	[c] Control of Cryptographic Keys .....	8-22
	[d] Private Sector Cryptographic Systems .....	8-22.1
	[e] Quantum Cryptography.....	8-22.1
[2]	Digital Signatures.....	8-22.2
	[a] Digital Signature Laws .....	8-22.3
	[b] ABA Digital Signature Rules .....	8-22.3
[3]	Certificates & Certificate Authorities.....	8-23
[4]	Authentication and System Access Control .....	8-24
	[a] Passwords .....	8-24
	[b] Tokens .....	8-25
	[c] Password-Generating Token .....	8-25
	[d] Smart Cards.....	8-25
	[e] Biometrics .....	8-25
	[f] One-Time Password Scratch Card .....	8-26.1
	[g] Second Channel Authentication.....	8-26.1
	[h] Mutual Authentication .....	8-26.1
[5]	Firewalls.....	8-26.2
	[a] Necessity of Firewalls .....	8-26.2
	[b] Types of Firewalls .....	8-28
	[c] Need for Constant Evaluation .....	8-28
	[d] Data Transmission .....	8-28
[6]	Intrusion Detection .....	8-28
	[a] Intrusion Detection Terminology .....	8-29
	[b] Characteristics of a Good Intrusion Detection System .....	8-29
	[c] Publicly Available Intrusion Detection Systems.....	8-31
	[d] Commercial Intrusion Detection Systems .....	8-31
[7]	Web Linking .....	8-31
	[a] Implementing Web-Linking Relationships .....	8-31
	[b] Monitoring Web-Linking Relationships.....	8-32

	[c] Managing Service Providers .....	8-32
[8]	Wireless Technology.....	8-32
[9]	Software Patches.....	8-33
	[a] Identifying Patch Information.....	8-33
	[b] Evaluating the Impact of Patches.....	8-34
	[c] Testing and Installing Software Patches .....	8-34
[10]	Internet Security Controls for PC Users .....	8-34
[11]	Virus Protection.....	8-35
[12]	VoIP Protection .....	8-36
<b>¶ 8.05</b>	<b>ONLINE PRIVACY AND INFORMATION SECURITY—REGULATORY GUIDANCE AND DEVELOPMENTS .....</b>	<b>8-37</b>
[1]	FDIC Guidance on Online Privacy and Security .....	8-37
	[a] Financial Institution Letter on Online Privacy .....	8-37
	[b] FDIC Paper on Security Risks Associated With the Internet.....	8-39
	[c] Safeguarding Customers Against E-Mail and Internet-Related Fraudulent Schemes .....	8-40
	[d] Guidance on Instant Messaging.....	8-42
[2]	OCC and Dept. of Treasury Guidance and Initiatives .....	8-43
	[a] Technology-Related Risk Management Guidance and Checklists.....	8-43
	[b] The Consumer Electronic Payments Task Force Recommendations (Dept. of Treasury).....	8-45
	[c] Automated Clearinghouse Risks.....	8-46
[3]	FRB Sound Practices Guidance for Information Security for Networks .....	8-48
[4]	Securities Regulation of Confidentiality of Information.....	8-49
	[a] October 1995 Interpretive Release .....	8-49
	[b] May 1996 Interpretive Release .....	8-50
	[c] Internet Surveillance Program.....	8-50
	[d] Elimination of Social Security Filing Requirement.....	8-51
[5]	FDIC Study on Account Hijacking and Identity Theft .....	8-51
	[a] Ways of Perpetrating Account Hijacking .....	8-51
	[b] Industry Responses to Identity Theft.....	8-52
	[c] Interagency Final Rule and Guidelines on Identity Theft “Red Flags” .....	8-53

## **9 Security Training for Bank Employees**

<b>¶ 9.01</b>	<b>IMPORTANCE OF A GOOD TRAINING PROGRAM .....</b>	<b>9-1</b>
[1]	Required by the Bank Protection Act Regulations .....	9-1
	[a] Board of Directors Responsibility .....	9-1
	[b] Security Officer Responsibility .....	9-2
	[c] Employee Responsibility .....	9-2
[2]	Prevention of Crimes of Violence.....	9-2
[3]	Prevention and Detection of White-Collar Crime .....	9-2
[4]	Protection of Customer Information .....	9-2
<b>¶ 9.02</b>	<b>TRAINING FOR BANKING OFFICE PERSONNEL .....</b>	<b>9-3</b>
[1]	Opening Procedures.....	9-3
[2]	Closing Procedures.....	9-4
[3]	Security During Banking Hours.....	9-4
	[a] Cash Control .....	9-4
	[b] Keys and Locks.....	9-7

**TABLE OF CONTENTS**

[4]	Bank Robbery .....	9-8
	[a] Prevention.....	9-8
	[b] Bait Money Procedures.....	9-8
	[c] Bank Robbery Response .....	9-9
	[d] Coping with a Robbery Attack.....	9-10
[5]	Burglary Response .....	9-11
[6]	Kidnapping, Extortion, and/or Hostage Situation .....	9-11
	[a] Preventive Techniques .....	9-11
	[b] Response Training.....	9-15
[7]	Safe Deposit Operations.....	9-15
	[a] Common Problems .....	9-15
	[b] Checklist of Safeguards .....	9-16
[8]	“Know Your Customer” Procedures .....	9-16
	[a] Objectives .....	9-17
	[b] Identifying the Customer .....	9-17
	[c] Suspicious Conduct and Transactions Checklist .....	9-17
[9]	Loan Fraud Prevention .....	9-19
	[a] Mortgage Fraud .....	9-20
[10]	Detecting Counterfeit Currency, Securities, and Checks .....	9-21
	[a] Counterfeit Currency.....	9-21
	[b] Securities .....	9-22.1
	[c] Checks.....	9-23
[11]	Preventing Wire Transfer Fraud.....	9-23
[12]	Security Equipment Testing.....	9-24
	[a] Robbery Alarms .....	9-24
	[b] Burglar Alarms .....	9-24
	[c] Surveillance Cameras.....	9-25
	[d] Other Security Equipment.....	9-25
<b>¶ 9.03</b>	<b>TRAINING FOR ALL EMPLOYEES .....</b>	<b>9-25</b>
	[1] Customer Privacy Protection .....	9-25
	[2] Avoiding Pretext Phone Calling .....	9-26
	[3] Preventing Money Laundering .....	9-27
	[4] Bomb Threat .....	9-27
	[5] Fire.....	9-28
<b>¶ 9.04</b>	<b>SPECIAL TRAINING FOR CUSTOMERS.....</b>	<b>9-28</b>
	[1] Confidence Schemes.....	9-28
	[2] Robbery Prevention .....	9-29
<b>10</b>	<b>Investigation of White-Collar Crime</b>	
<b>¶ 10.01</b>	<b>THE FEDERAL CRIMINAL JUSTICE SYSTEM .....</b>	<b>10-1</b>
	[1] Judicial Districts .....	10-1
	[2] Investigation.....	10-2
	[3] Prosecution .....	10-2
	[4] Incarceration .....	10-2
<b>¶ 10.02</b>	<b>FEDERAL GOVERNMENT RESTRAINTS ON WHITE-COLLAR CRIME INVESTIGATIONS .....</b>	<b>10-3</b>
<b>¶ 10.03</b>	<b>THE INTERNAL INVESTIGATIVE UNIT .....</b>	<b>10-3</b>

## TABLE OF CONTENTS

[1]	Qualities to Look for When Hiring for These Positions.....	10-3
[2]	Threat Analysis Teams .....	10-4
[3]	Outsourcing the Investigative Function .....	10-5
<b>¶ 10.04</b>	<b>STARTING THE INVESTIGATION.....</b>	<b>10-6</b>
[1]	Reporting Criminal Activity.....	10-7
[2]	Planning the Investigation.....	10-8
	[a] Determining Objectives.....	10-9
	[b] Gathering Documentation .....	10-9
	[c] Identifying the Suspect.....	10-10
<b>¶ 10.05</b>	<b>INTERVIEWING .....</b>	<b>10-11</b>
[1]	Objectives .....	10-11
[2]	Planning for Good Questions.....	10-11
	[a] Precise Questions.....	10-12
	[b] Extended Answer Questions.....	10-12
	[c] Leading Questions .....	10-13
	[d] Questions to Avoid.....	10-13
	[e] Complex Questions.....	10-13
	[f] The Five Interrogatives .....	10-13
	[g] Question Sequence .....	10-14
	[h] Controlled Answer Interviewing Techniques.....	10-14
	[i] Free Narrative.....	10-14
	[j] Direct Examination.....	10-14
[3]	Interview Environment .....	10-15
[4]	Investigator's Demeanor.....	10-15
[5]	Conducting the Interview .....	10-16
[6]	Recognizing Psychological Factors in Interviewing.....	10-16
	[a] The Emotions.....	10-16
	[b] The Physical Guilt Symptoms of Emotion .....	10-17
	[c] Perception.....	10-17
	[d] Memory.....	10-18
	[e] Suggestion.....	10-19
	[f] Bias.....	10-19
	[g] Deception.....	10-19
<b>¶ 10.06</b>	<b>INTERROGATION.....</b>	<b>10-19</b>
[1]	Objectives .....	10-20
[2]	Methodology .....	10-20
[3]	Written Statements .....	10-21
<b>¶10.07</b>	<b>POLYGRAPH AND PSE TESTS.....</b>	<b>10-22</b>
[1]	Polygraph.....	10-22
[2]	Psychological Stress Evaluator.....	10-23
[3]	Interpreting Test Results.....	10-23
[4]	Legal Considerations .....	10-23
	[a] Federal Polygraph Legislation.....	10-24
	[b] State Polygraph Legislation .....	10-24
<b>¶ 10.08</b>	<b>FORENSIC USE OF HYPNOSIS .....</b>	<b>10-25</b>
[1]	An Investigative Aid .....	10-25
[2]	Guidelines for Use .....	10-26

## TABLE OF CONTENTS

<b>¶ 10.09</b>	<b>IMPLICATIONS OF THE <i>MIRANDA</i> RULING</b> .....	10-27
	[1] Private Security Personnel Excluded .....	10-27
	[2] Malicious Prosecution .....	10-27
	[3] Employee's Rights .....	10-27
<b>¶ 10.10</b>	<b>ELECTRONIC SURVEILLANCE</b> .....	10-28
	[1] Wiretapping and Electronic Surveillance .....	10-28
	[2] Telephone Conversations .....	10-28
<b>¶ 10.11</b>	<b>INVESTIGATING COMPUTER CRIME</b> .....	10-29
	[1] Areas of Vulnerability .....	10-29
	[2] Definition of Computer Crime .....	10-30
	[3] Computer Abuse Methods and Detection .....	10-30
	[4] Clues to the Existence of Fraud .....	10-33
	[5] Zeroing in on Suspects .....	10-33
	[6] Special Training Needs of the Computer Crime Investigator .....	10-34
	[7] Damage Control and Incident Response .....	10-34
	[8] Evidence .....	10-38
<b>¶ 10.12</b>	<b>BAD DEBT INVESTIGATION</b> .....	10-39
	[1] Commercial and Consumer Loans .....	10-40
	[2] Real Estate Loans .....	10-40
	[3] Uncovering Hidden Assets .....	10-41
<b>¶ 10.13</b>	<b>SEARCH</b> .....	10-42
	[1] Power to Search .....	10-42
	[a] Searches by Private Security Personnel .....	10-42
	[b] Private Sector Workplace Searches .....	10-43
	[2] Evidence Obtained From Searches .....	10-44
<b>¶ 10.14</b>	<b>ARREST</b> .....	10-44
	[1] Definition of an Arrest .....	10-44
	[2] Arrest With a Warrant .....	10-45
	[3] Arrest Without a Warrant .....	10-45
	[a] Common-Law Rule: Private Security Officer Is Treated as a Private Citizen .....	10-45
	[b] Statutory Provisions .....	10-46
	[c] Deputization Powers .....	10-46
<b>¶ 10.15</b>	<b>REPORT WRITING: THE OUTCOME OF THE INVESTIGATION</b> .....	10-46
	[1] Report Elements .....	10-46
	[2] Sample Report .....	10-47
<b>¶ 10.16</b>	<b>AVOIDING PITFALLS</b> .....	10-49
<b>¶ 10.17</b>	<b>FILES</b> .....	10-49
<b>¶ 10.18</b>	<b>PRESENTING CASES TO THE U.S. ATTORNEY</b> .....	10-50
	[1] Fast Track Programs .....	10-50
	[2] Guidelines for Fast Track Prosecution .....	10-51
	[3] Participation in a Fast Track Program .....	10-52
<b>¶ 10.19</b>	<b>INTERPOL</b> .....	10-52
	[1] Interpol's History .....	10-52
	[2] Interpol's Organization .....	10-53
	[a] General Secretariat .....	10-54