FEDERAL DEPOSIT INSURANCE CORPORATION

DIRECTIVE SYSTEM

TYPE AND NUMBER	Circular 1600.7
CONTACT	ITCIP-INFO@FDIC.GOV
DATE	September 20, 2016
DATE OF CANCELLATION *(Bulletins Only)*	

TO: All Personnel

FROM: Arleas Upton Kea, Director, Division of Administration

SUBJECT: FDIC Insider Threat and Counterintelligence Program

1. Purpose

a. The purpose of the FDIC Insider Threat and Counterintelligence Program (ITCIP) is to provide an integrated framework for FDIC personnel to affirmatively protect the FDIC using a defensive program to address internal and external threats and risks posed to its personnel, facilities, assets, resources, and classified and sensitive information, by insider threats and foreign entities.

b. All FDIC personnel have a responsibility to protect the FDIC by observing and reporting activities that could pose risks to the FDIC's mission and assets. This Directive establishes that framework within which effective and responsible actions can be focused to exercise individual responsibility to prevent, detect, mitigate, and deter internal and external threats.

c. The ITCIP is guided by these core principles:

(1) Privacy Protection. Personnel privacy will be protected with stringent privacy controls;

(2) Employee Wellbeing. Established employee support mechanisms will be leveraged, as needed (e.g., WorkLife Program);

(3) Balanced Approach. Mission accomplishment and the agility of the workforce will be balanced effectively with responsible threat prevention, detection, mitigation and deterrence;

(4) FDIC Reputation. Public confidence will be maintained by effectively mitigating risk and protecting FDIC assets; and

(5) Risk Based Monitoring. Anomalous activities will be monitored commensurate with the level of perceived risk posed to FDIC assets.

Purpose (cont.)

d. The ITCIP addresses threats, manages information, and implements strategies to mitigate risks to the FDIC or national security involving potential outside adversaries and insider threats due to inadvertent disclosures or intentional breaches of sensitive information by personnel who may be compromised by external sources, or personnel who may be disgruntled or seeking personal gain, or to damage the reputation of the FDIC, or acting for some other reason.

e. Insider Threats occur as a result of:

(1) Malicious Intent. When personnel intentionally abuse their privileged access to cause damage to the FDIC;

(2) Complacency. When personnel expose the FDIC to external risks due to a lax approach to policies, procedures, and information security; or

(3) Ignorance. When personnel expose the FDIC to external risks due to a lack of awareness of security policies, procedures, and protocols.

f. The ITCIP framework:

(1) Identifies risks to our personnel, operations, facilities, and information;

(2) Establishes safeguards and protocols to protect FDIC assets, information resources, mission and business processes and programs that are of particular interest to insider threats and outside adversaries;

(3) Detects and assesses inadvertent disclosures and intentional breaches of classified or sensitive information by insider threats;

(4) Provides awareness to all Divisions and Offices of applicable Federal authorities, policies, and directives relating to the roles and responsibilities in implementing an ITCIP; and

(5) Ensures that procedures are in place to inform FDIC Senior Leadership of potential risks and threats and uses established escalation protocols to enable a timely and informed response to suspected or confirmed insider threats.

2. Scope

The provisions of this Directive apply to all FDIC personnel, as defined in Section 5.

3. Background

This Directive establishes the roles, responsibilities, and associated activities of the ITCIP per applicable laws, whistleblower protections, civil rights, and privacy policies, including:

a. EO 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, dated October 7, 2011, directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. This EO directs Federal agencies to establish, implement, monitor, and report on the effectiveness of insider threat programs to protect classified national security information as defined by EO 13526.

b. EO 13526, *Classified National Security Information*, dated December 29, 2009, prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism.

c. EO 12333*, United States Intelligence Activities*, dated December 4, 1981, as amended, directs that all Federal agencies implement effective counterintelligence (CI) to detect, deter, mitigate, counter and neutralize espionage and other threat activities from foreign powers, intelligence services, or terrorist entities directed against the United States.

d. Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs,* dated November 21, 2012, provides direction and guidance to promote the development of effective insider threat programs to deter, detect, and mitigate actions by personnel who may represent a threat to national security. The Minimum Standards outline the minimum elements necessary to establish effective insider threat programs including the capability to gather, integrate, and centrally analyze and respond to key threat-related information; monitor employee use of classified networks; provide the workforce with insider threat awareness training; and protect the civil liberties and privacy of all personnel.

e. National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013, outlines the controls and guidelines that apply to insider

Background (cont.)

threat programs that can be effectively applied in an unclassified environment to improve the security of non-classified systems and safeguard sensitive information.

f. Presidential Decision Directive/NSC-12 (PPD-12), *Security Awareness and Reporting of Foreign Contacts*, dated August 5, 1993, requires that each agency maintain a formal security and/or counterintelligence program and that government employees report all contacts with individuals of any nationality, either within or outside the scope of the employee's official activities, in which illegal or unauthorized access is sought to classified or otherwise sensitive information.

---

4. Policy

It is the FDIC's policy to:

a. Develop and maintain an integrated ITCIP to identify risks to FDIC personnel, assets, operational resources, information, and facilities.

b. Establish a centralized reporting process to assess, analyze, and act upon all reported suspicious activity, anomalous behavior, or potential threats to FDIC's personnel, assets, operational resources, information, and facilities.

c. Refer suspected insider threat matters to the Office of the Inspector General (OIG) for criminal investigation when no foreign connection is evident, or provide an information referral to the Federal Bureau of Investigation (FBI) for suspected criminal matters relating to national security or espionage activity in compliance with Section 811 of the Intelligence Authorization Act of 1995, codified at 50 USC § 3381.

d. Provide Insider Threat and Counterintelligence Awareness Training to all new FDIC personnel within 30 days of commencing employment.

e. Annually provide Insider Threat Awareness Training to all FDIC personnel.

f. Annually provide Counterintelligence Awareness Training to all FDIC personnel possessing an active national security clearance.

g. Develop and maintain an effective Foreign Visitor Program to protect the FDIC from external hostile threats by vetting and screening foreign visitors through the Intelligence Community and Federal partner agencies to identify any FIE affiliations.

Policy (cont.)

h. Develop and maintain a Foreign Travel Program requiring personnel with active Top Secret national security clearances with access to Sensitive Compartmented Information to self-report all official and unofficial foreign travel.

i. Develop and maintain a Foreign Contact Reporting Program requiring personnel with active national security clearances to self-report:

(1) Close and continual unofficial contact with foreign nationals;

(2) Official or unofficial contact with foreign nationals exhibiting undue interest in FDIC personnel or their duties;

(3) Attempts by foreign nationals to obtain sensitive or classified information;

(4) Attempts by foreign nationals to place FDIC personnel under obligation in any way; or

(5) Attempts by foreign nationals to establish business relationships outside the scope of normal official duties.

5. Definitions

Terms specific to this Directive are defined as follows:

a. Anomalous Activity. Activity that is inconsistent with or deviates from what is usual, normal, or expected. Irregular or unusual activity could be an indicator of an insider threat emanating from trusted personnel who are disgruntled, seeking personal gain, attempting to damage the reputation of the FDIC, or have been compromised by a foreign entity or government.

b. Asset. Any resource—person, group, relationship, instrument, installation, process, property, or supply—at the disposition of an organization for use in an operational or support role.

c. Classified Information. Any data, file, paper, record, or computer or mobile device screen containing information associated with the national defense or foreign relations of the U.S., bearing the classification markings of Confidential, Secret, or Top Secret, requiring protection against unauthorized disclosure.

d. Cleared Personnel. Personnel who have been granted authorized access to classified information.

Definitions (cont.)

e. Close and Continual Unofficial Foreign Contact. Recurring contacts with any foreign entity or foreign national not related to official duties; that is social, business-related, romantic, or sexual in nature; or is marked by bonds of affection, obligation, or other commitment; or with whom the individual shares a residence. This does not refer to incidental, one-time contact with foreign nationals where there will be no continuing relationship.

f. Counterintelligence (CI). Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including an agency's normal personnel, physical, document, or communications security programs.

g. Defensive Travel Brief. A classified or unclassified brief on a specific country or countries to which FDIC personnel will travel in the near future. The travel brief will include information concerning the foreign intelligence threat, technical threat (e.g., laptop computers and cellular phones), criminal threat, and, if known, the health threat, facing the traveler. The brief will give the traveler strategies to mitigate those threats and provide helpful in-country telephone numbers, such as the American Embassy or nearest American Consulate.

h. Espionage. The act of obtaining, delivering, transmitting, communicating, or receiving information with the intent or reason to believe that the information may be used to the injury of the U.S. or to the advantage of any foreign nation. The offense of espionage applies in time of war and peace.

i. FDIC High Value Assets (HVA). Those information resources, mission and business processes, and critical programs that are of particular interest to potential or actual adversaries. Information that a threat actor, either foreign or internal to the FDIC, would find of high value (e.g., personally identifiable information, Living Wills, Examination Reports). These assets may contain sensitive information used in critical Federal operations, or house unique collections of data (by size or content) making them of particular interest to criminal, politically-motivated, or state-sponsored adversaries either for direct exploitation of the information in question, to cause disruption to the delivery of critical services, or to cause a loss of confidence in the U.S. Government.

Definitions (cont.)

j. Foreign Intelligence Entity (FIE). Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. This term includes foreign intelligence and security services and international terrorist organizations.

k. Foreign National. Any person who is not a citizen or national of the U.S.

l. Insider. Any person with authorized access to any U.S. Government (USG) resource, to include personnel, facilities, information, equipment, networks, or systems.

m. Insider Threat. A threat posed to the FDIC or U.S. national security by someone who misuses or betrays, wittingly or unwittingly, his or her authorized access to any USG resource. This threat can include damage through espionage, terrorism, sabotage, unauthorized disclosure of classified information or unclassified sensitive information, or through the loss or degradation of FDIC resources or capabilities.

n. Personnel. All persons employed by, contracted to, or detailed or assigned to the FDIC, including: employees; interns; contractors; subcontractors; experts; consultants; licensees; grantees; secondees; and any other category of person who acts for or on behalf of the FDIC, whose business location is primarily within FDIC spaces, who is authorized unescorted facility access to these spaces, or who has authorized access to FDIC networks containing FDIC HVA or systems containing classified information.

o. Sabotage. An act or acts that deliberately and willfully destroys, damages, or obstructs any FDIC activities, processes, or property for any reason.

p. Self-radicalization. Significant steps an individual takes in advocating or adopting an extremist belief system for the purpose of facilitating ideologically-based violence to advance political, religious, or social change. The self-radicalized individual has not been recruited by and has no direct, personal influence or tasking from other violent extremists.

q. Subversion: Any act inciting FDIC personnel to violate laws, disobey, or attempt to circumvent, policy, directives, and regulations, or disrupt official activities with the willful intent to interfere with, or impair the loyalty, morale, or discipline of FDIC's personnel or mission.

Definitions (cont.)

r. Suspicious Activity. One or more reportable indicators as described under Section 7 below.

s. Terrorism. The unlawful use or threatened use of force or violence against individuals or property to coerce or intimidate persons, governments, or societies, often to achieve political, religious, or ideological objectives.

6. Responsibilities

a. The Deputy Director, Corporate Services Branch (CSB), is designated as the Senior Agency Official (SAO) for the ITCIP. The SAO shall:

(1) Provide management and oversight of the ITCIP and ensure all activities are established and operated in accordance with applicable laws, whistleblower protections, civil rights, and privacy policies;

(2) Establish guidelines and procedures for the retention, sharing, and safeguarding of records necessary to conduct insider threat and CI assessments; and

(3) Establish and co-chair, with the Chief Information Security Officer (CISO), the ITCIP Working Group (ITCIPWG) to provide a centralized analysis and response capability to gather, integrate, review, assess, and respond to information derived from ITCIP activities.

b. The Assistant Director, Security and Emergency Preparedness Section (SEPS) shall:

(1) Provide functional oversight of ITCIP activities;

(2) Ensure ITCIP activities and assessments are conducted in full compliance with applicable laws, whistleblower protections, civil rights, and privacy policies;

(3) Coordinate approval of ITCIP activities, through the SAO, with the ITCIP Executive Committee;

(4) Review all allegations, inquiries, reports, and observations of reportable indicators by any personnel and coordinate with the ITCIPWG;

(5) Establish and promote an internal network site accessible to all personnel to provide insider threat and CI reference material, including indicators of insider threat behavior, and applicable reporting requirements and procedures,

Responsibilities (cont.)

to include a process to facilitate anonymous reporting of observed behavioral indicators;

(6) Produce statistical reports, as necessary, regarding ITCIP activities;

(7) Identify ITCIP issues affecting policy and/or procedures on an Agency-wide basis;

(8) Establish and manage all implementation and reporting requirements, including self and independent assessments;

(9) Identify ITCIP training needs;

(10) Ensure employees complete Insider Threat and Counterintelligence Awareness Training within 30 days of commencing employment, and complete refresher training annually thereafter. Insider threat training applies to all personnel. Counterintelligence training applies only to personnel with an active security clearance;

(11) Coordinate, as permitted by applicable laws, regulations, and FDIC policies, with various Divisions and Offices to obtain access to all relevant information necessary for the conduct of authorized ITCIP assessments;

(12) Coordinate with the Division of Insurance and Research to permit vetting of foreign visitors in advance of planned visits to FDIC and to provide a pre-visit defensive CI briefing and post-visit debriefing to FDIC personnel meeting with foreign visitors, when appropriate. Recurring visits by the same foreign visitor meeting with the same FDIC personnel, require visitor vetting and personnel briefing only for the initial visit, unless deemed necessary by the SAO for any subsequent visit(s); and

(13) Provide foreign travel briefings and debriefings to personnel with active Top Secret national security clearances with access to Sensitive Compartmented Information.

c. When the Office of Inspector General (OIG) first becomes aware of a potential Insider Threat and/or Counterintelligence concern involving FDIC personnel, notice shall be provided to the ITCIPWG. In collaboration with the ITCIPWG, the OIG shall determine whether the matter should be responded to by the ITCIPWG or investigative jurisdiction assumed by the OIG. The OIG is responsible for coordinating insider threat

Responsibilities (cont.)

and/or counterintelligence investigations with other law enforcement agencies.

d. The CISO shall support the ITCIP on all relevant information technology matters related to the identification, analysis, assessment, and resolution of potential insider threat and/or counterintelligence matters and co-chair the ITCIPWG.

e. The Chief Privacy Officer shall provide guidance on individual privacy, civil rights, and civil liberties protections during ITCIP activities.

f. The General Counsel shall provide legal advice for the establishment, implementation, execution, management, and oversight of ITCIP activities.

g. All FDIC personnel shall report to their immediate supervisor and the Assistant Director, SEPS, any:

   (1) Incident of actual or suspected loss or compromise of FDIC information;

   (2) Reportable Indicators, as described under Section 7 below. (Note: The anonymous reporting process may be used when reporting personnel do not wish to reveal their identity);

   (3) Information regarding threats of espionage, terrorism, or sabotage; and

   (4) Plans to host foreign visitors for an official visit to FDIC with sufficient advance notice, when at all possible, to permit pre-visit vetting of the expected foreign visitors.

h. FDIC personnel with an active Top Secret national security clearance with access to Sensitive Compartmented Information must contact the FDIC Special Security Officer to receive a foreign travel briefing prior to conducting official or unofficial foreign travel.

i. Division and Office Managers and Supervisors shall:

   (1) Ensure that all information or allegations of actual or suspected insider threats or threats of espionage, sabotage, or terrorism received by management are immediately reported to the Assistant Director, SEPS; and

Responsibilities (cont.)

(2) Ensure that any reports of reportable indicators received by management are immediately reported to the Assistant Director, SEPS.

j. ITCIPWG

(1) The ITCIPWG is a cross-discipline group focused on detecting, identifying, assessing, mitigating, and preventing insider or external threat activity through the centralized and integrated analysis of threat information enhanced by technical and non-technical data as well as intelligence from the Intelligence Community and Federal partner agencies;

(2) The ITCIPWG consists of representatives from DOA, CIOO, OIG, and Legal;

(3) The ITCIPWG is co-chaired by the Deputy Director, CSB, and the CISO. As the SAO, the Deputy Director, CSB, has final decision authority for the ITCIPWG. The ITCIPWG is responsible to accomplish the following:

(a) Develop objectives and priorities for integrating and analyzing CI, security, information technology, user audits, and other applicable information for the FDIC;

(b) Work with FDIC Divisions and Offices to identify elements within their respective organizations to meet the FDIC's ITCIP mission requirements;

(c) Provide direction for accomplishing minimum standards and guidance for implementing the ITCIP within FDIC Divisions and Offices, ensuring that the national minimum standards and guidance described in the Presidential Memorandum for the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, dated November 21, 2012, or in other applicable guidance are met;

(d) Gather, integrate, and centrally analyze and respond to threat-related information;

(e) Identify patterns of problems contributing to insider threat behavior, such as, flawed business processes, ineffective communications, lack of buy-in, policy gaps, and insufficient training, which may lead to recommendations to change FDIC processes to address those patterns; and

Responsibilities (cont.)

(f) Conduct insider threat and/or counterintelligence assessments.

1. Provide an “Unfounded” decision when no evidence of insider threat and/or a counterintelligence concern is present;

2. Refer matters determined to be the result of complacent or ignorant insider activity that poses a threat to the FDIC to management for resolution; and

3. Forward a decision to the ITCIP Executive Committee to refer matters determined to be the result of malicious insider activity to the: (1) OIG for criminal investigation when no foreign connection is evident, or (2) FBI for suspected criminal matters relating to national security or espionage activity in compliance with Section 811 of the Intelligence Authorization Act of 1995, codified at 50 U.S.C. § 3381.

---

7. Reportable Indicators

FDIC personnel must report the following to their immediate supervisor and to the Assistant Director, SEPS, or through the anonymous reporting process:

a. Undue Interest

Attempts by anyone, regardless of nationality, to obtain or acquire unauthorized access to information concerning the FDIC, in the form of facilities, activities, personnel, technology, or material through any of the following methods: questioning, elicitation, trickery, bribery, threats, coercion, blackmail, photography, observation, collection of documents or material, correspondence (including electronic correspondence), or automated system intrusions.

b. Disregard for Security Practices

(1) Incidents in which authorized users of government information systems attempt to gain unauthorized access or attempt to circumvent security procedures or elevate their access privileges without approval, including use of another person’s account credentials, user ID and/or password, eToken, or PIV card;

(2) Repeated involvement in security violations;

Reportable Indicators (cont.)

(3) Transmission of FDIC HVA or classified information using unauthorized communications or computer systems;

(4) Known or suspected unauthorized disclosure of classified or sensitive information to those not authorized to have knowledge of such information, including leaks to the media;

(5) FDIC personnel who remove classified or sensitive information from the workplace without authority or who possess or store classified or sensitive information in unauthorized locations; and

(6) FDIC personnel who remove FDIC HVA from the workplace without authority or who possess or store such information in unauthorized locations.

c. Unusual Work Behavior

(1) Anomalous or uncharacteristic behavior, unusual activities, or other situations that suggest someone may pose a risk to FDIC information or operations;

(2) Attempts to expand access to sensitive or classified information by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities;

(3) Attempts to obtain information for which the person has no authorized access or need-to-know; and

(4) Using copiers, facsimile machines, document scanners, or other automated or digital equipment to reproduce or transmit sensitive material which appears to exceed official and authorized duties.

d. Financial Matters

(1) Unexplained or undue affluence without a logical income source;

(2) Free spending or lavish display of wealth which appears beyond normal income;

(3) A bad financial situation that suddenly reverses, opening several bank accounts containing substantial sums of money, or the repayment of large debts or loans;

(4) Sudden purchases of high value or luxury items where no logical income source exists; and

Reportable Indicators (cont.)

(5) Attempts to explain wealth as an inheritance, gambling luck, or a successful business venture, without facts supporting the explanation.

e. Foreign Influence or Connections

(1) Contact with an individual, regardless of nationality, under circumstances that suggest FDIC personnel may be the target of attempted recruitment by a foreign intelligence service or foreign or domestic terrorist organization;

(2) FDIC personnel engaged in actual or attempted acts of terrorism, sabotage, subversion, or espionage;

(3) FDIC personnel in contact with persons known, or suspected to be members of, or associated with, a foreign intelligence service or foreign or domestic terrorist organizations;

(4) FDIC personnel in contact with anyone possessing information about planned, attempted, suspected, or actual terrorism, sabotage, subversion, espionage, or other intelligence activities directed against the FDIC or the U.S;

(5) FDIC personnel suspected of providing financial or other material support to terrorist organizations or to someone suspected of being a terrorist;

(6) FDIC personnel associated with or having connections to known or suspected terrorists, or who are exhibiting behaviors of self-radicalization;

(7) FDIC personnel who are in contact with any official or citizen of a foreign country when the foreign official or citizen exhibits excessive knowledge of or undue interest in FDIC personnel or their duties beyond the normal scope of friendly conversation; attempts to obtain classified or sensitive information; attempts to place FDIC personnel under obligation through special treatment, favors, gifts, money, or other means; or attempts to establish business relationships that are outside the scope of normal official duties; and

(8) Incidents in which FDIC personnel or their family members traveling to or through foreign countries are contacted by persons who represent a foreign law enforcement, security, or intelligence organization, and are questioned about their duties; requested to provide classified or sensitive information; threatened, coerced,

Reportable Indicators (cont.)

or pressured in any way to cooperate with the foreign official or offered assistance in gaining access to people or locations not routinely afforded Americans.

f. Soliciting Others

(1) Attempts to encourage FDIC personnel to violate laws or disobey lawful orders or regulations for the purpose of disrupting governmental activities (subversion) or which could lead to blackmail or extortion;

(2) Requests to obtain sensitive information to which the requestor is not authorized access; and

(3) FDIC personnel participating and/or soliciting others in activities advocating or teaching the overthrow of the U.S. Government by force or violence, or seeking to alter the form of government by unconstitutional means (sedition).

---

8. References

a. Intelligence Reform and Terrorism Prevention Act, 2004.

b. Counterintelligence Enhancement Act of 2002, as amended.

c. Intelligence Authorization Act, Section 811, Public Law 103-359, codified at 50 USC § 3381, *Coordination of Counterintelligence Activities*, October 14, 1994.

d. The Banking Act, 1933, Public Law 73-66, June 16, 1933.

e. Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, October 7, 2011.

f. Executive Order 13556, *Controlled Unclassified Information*, November 4, 201.

g. Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, October 25, 2005.

h. Executive Order 12333, *Classified National Security Information*, December 29, 2009.

i. Executive Order 12333, *U.S. Intelligence Activities*, December 4, 1981, as amended.

References (cont.)

j. National Institute of Standards and Technology Special Publication 800-53 Revision 4, *Security Organizations and Privacy Controls for Federal Information Systems*, April 2013.

k. Office of National Counterintelligence Executive, *Defensive Counterintelligence Program Blueprint*, 2010.

l. National Counterintelligence Strategy of the United States of America, 2009.

m. Office of the National Counterintelligence Executive, *Protecting Key Assets, A Corporate Counterintelligence Guide.*

n. National Information Sharing Strategy, Successes and Challenges in Improving Terrorism-Related Information Sharing, October 2007.

o. President's Memorandum for the Heads of Executive Departments and Agencies, "*Guidelines and Requirements in Support of the Information Sharing Environment*," December 16, 2005.

p. Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, November 21, 2012.

q. Presidential Decision Directive/NSC-12 (PPD-12), *Security Awareness and Reporting of Foreign Contacts*, August 5, 1993.

9. Effective Date

The provisions outlined in this Directive are effective immediately.