The National Counterintelligence Strategy of the United States

Office of the National Counterintelligence Executive

March 2005

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
00 MAR 2005	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The National Counterintelligence Strategy of the United States	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the National Counterintelligence Executive, Washington, DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
Phone (703) 602-4500 for further information., The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**22**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

National Counterintelligence Strategy of the United States

PREFACE

The Counterintelligence Enhancement Act of 2002 (50 USC 401) directs that the Office of the National Counterintelligence Executive produce, on an annual basis, a strategy for the counterintelligence programs and activities of the United States Government. This is the first national counterintelligence strategy promulgated pursuant to that Act. President George W. Bush approved *The National Counterintelligence Strategy of the United States* on March 1, 2005.

Counterintelligence, as defined in the National Security Act of 1947, is "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorist activities."

As used in this *Strategy*, counterintelligence includes defensive and offensive activities conducted at home and abroad to protect against the traditional and emerging foreign intelligence threats of the 21st Century.

TABLE OF CONTENTS

INTRODUCTION

The National Security Strategy of the United States seeks to defend the peace by fighting terrorists and tyrants, to preserve the peace by building good relations among the great powers, and to extend the peace by encouraging free and open societies on every continent.

These fundamental objectives of our great Nation are not easily won. The terrorists and tyrants, the opponents of peace and freedom, are not passively watching from the sidelines. They are actively engaged in efforts to undermine the United States and our allies, and these efforts include some dimension of intelligence activities directed against us. Specifically, foreign adversaries seek to:

- penetrate, collect, and compromise our national security secrets (including sensitive information, plans, technology, activities, and operations) to advance their interests and defeat United States objectives.

- manipulate and distort the facts and reality presented to United States policy-makers by manipulating the intelligence we gather, and by conducting covert influence operations.

- detect, disrupt and counter national security operations including clandestine collection and special activities, special operations, other sensitive intelligence, and military and diplomatic activities.

- acquire critical technologies and other sensitive information to enhance their military capabilities or to achieve an economic advantage.

Collectively, these foreign intelligence activities present a threat to the Nation's security and prosperity. The United States requires national, systematic, and well-defined policies to counter them. A key to success in defeating these threats is a strategic counterintelligence response that supports the National Security Strategy.

The National Counterintelligence Strategy of the United States has four essential objectives:

- Identify, assess, neutralize, and exploit the intelligence activities of foreign powers, terrorist groups, international criminal organizations, and other entities who seek to do us harm.

- Protect our intelligence collection and analytic capabilities from adversary denial, penetration, influence, or manipulation.

- Help enable the successful execution of our sensitive national security operations.

- Help safeguard our vital national security secrets, critical assets, and technologies against theft, covert foreign diversion, or exploitation.

To achieve these objectives, we will draw upon the full range of counterintelligence capabilities including counterespionage, counter-deception, and offensive operations against hostile intelligence activities. Each of these national security tools must be strategically driven and employed to protect the United States from foreign threats, and to advance our national interests.

This document sets forth the national counterintelligence strategy of the United States in the context of our broad national security objectives and the foreign intelligence threats we face.

COUNTERINTELLIGENCE AND NATIONAL SECURITY

America faces substantial challenges to its security, freedom and prosperity. To meet them we must defeat global terrorism, counter weapons of mass destruction, ensure the security of the homeland, transform defense capabilities, foster cooperation with other global powers, and promote global economic growth. Our ability to meet these challenges is threatened by the intelligence activities of traditional and non-traditional foreign powers. Foreign intelligence services and others (e.g., terrorists, foreign criminal enterprises, cyber intruders, etc.) use clandestine activities and operations to harm and disadvantage U.S. national security interests. Counterintelligence is a key strategic national security tool that we use to defeat these foreign threats.

I. We will extend the safeguards of strategic counterintelligence to the Global War on Terrorism.

During the Cold War, our adversaries gained access to vital secrets of the most closely guarded institutions of our national security establishment. These included the clandestine, technical, and analytic directorates of the CIA; the counterintelligence division of the FBI; sensitive National Security Agency operations; Naval intelligence operations; nuclear weapons information; cryptographic keys for our secure communications; operational war plans for the defense of Europe; and plans for ensuring the survival of United States leadership in the event of war.

These peacetime losses resulted in grave damage in terms of secrets compromised, intelligence sources and methods degraded, and lives lost. Moreover, these compromises could have had even greater consequences had we been forced to go to war. Today we are engaged in a war on terrorism which has invaded our shores and threatens Americans around the globe. In this war, the potential consequences of counterintelligence failures are more immediate than during the Cold War, and put in jeopardy our combat operations, deployed forces, intelligence officers, diplomats, and other U.S. citizens.

Terrorist groups gain significantly when they have the support of state sponsors, which means that the intelligence services of these regimes can be links in the global terrorist support network. In Afghanistan and Iraq, we have seen limited examples where enemy intelligence operations have enabled terrorists to target Americans. In addition, Al Qaida and other terrorist organizations have employed classic intelligence methods to gather information, recruit sources, and run assets. In order to operate clandestinely, terrorist groups often act like intelligence organizations by conducting pre-operational planning, compartmented operations, covert communications, and training. The global

war on terrorism requires an effective counterintelligence strategy to help counter these hostile activities.

II. U.S. counterintelligence will shift from a reactive posture to a proactive strategy of seizing advantage.

If the purpose of intelligence operations and analysis is to understand an adversary's plans and intentions, the purpose of counterintelligence is to be aware of and exploit the adversary's intelligence operations. We need to be aggressive and creative in exposing the activities of foreign intelligence services. Utilizing a proactive counterintelligence strategy can help identify specific intelligence collection techniques, and gauge an appropriate response to counter the interests of an adversary. This requires a tighter coupling between organizations that collect foreign intelligence, and counterintelligence organizations, in order to fully exploit collection, analysis, and offensive operations. We need to incorporate counterintelligence considerations into strategic and tactical planning, operations, and training. The Intelligence Reform and Terrorism Prevention Act of 2004, which created a Director of National Intelligence, with a National Counterintelligence Executive under the Director, takes a significant step toward increasing community-wide coordination.

Since 1985, nearly 80 Americans have been arrested for crimes related to passing classified information to foreign governments. These spies were able to operate undetected for too long with disastrous results.

- The Walker ring in the Navy – over 17 years.
- The Conrad group in the U.S. Army – over 18 years.
- The Ames case in CIA – over 9 years.
- The Hanssen case in the FBI – over 21 years.
- The Montes case in DIA – over 15 years.

Although each of these cases represents an individual success in terms of a criminal prosecution, taken as a whole they reveal a larger systemic vulnerability in our national security. In the past, a comprehensive focus was lacking in the intelligence community's approach to protecting secrets. The counterintelligence mission must be transformed into a more coordinated, community-wide effort to help neutralize penetrations of our government. Within the United States, we must transform both our operational and analytical focus from a case-driven approach to a more strategic assessment of an adversary's presence, capabilities and intentions. Strategic

counterintelligence analysis must drive operations. This requires looking beyond customary targets, such as known intelligence officers, to a larger population of foreign visitors and others whose activities suggest they might be involved in intelligence collection activities against the United States.

III. U.S. counterintelligence will help protect the sensitive technologies that are the backbone of our security.

The U.S. national defense strategy is based on a continuous transformation that utilizes cutting-edge capabilities, and places a premium on sensitive technologies that provide an advantage. Plans that ensure strategic superiority can be jeopardized if essential secrets are stolen and incorporated into an adversary's weapons systems. The United States spends billions of dollars developing weapons systems, which often rest on essential technological secrets. If foreign intelligence services steal these technological secrets, both our resource investment and our national security advantage are lost.

Today, more than 90 countries target sensitive U.S. technologies. Many employ collection techniques that extend beyond simple clandestine operations, and include tasking visiting businessmen, scientists, foreign students, trade shows, and debriefing visitors upon their return home. Counterintelligence planning and execution must proceed from a national counterintelligence strategy and be an inherent part of the mission at research laboratories, defense establishments, and with partners in industry. Counterintelligence and security considerations should not be an afterthought imposed on scientists, researchers, and those who develop sensitive technology. Coordinated and integrated counterintelligence information and analysis will be made available to senior government leaders, and, when appropriate, to security managers in the private sector.

Comprehensive risk management, valid security practices, and an informed strategic worldview are among the best guarantors of success against foreign intelligence threats. We will reach out to the private sector, especially those in the science and technology community, to increase intelligence threat awareness by providing threat information, and educating these audiences to the variety of ways our adversaries acquire and steal information.

The departments and agencies charged with protecting the homeland are building new channels for information sharing across government, including at the state and local level, with private industry, and with foreign partners. We must ensure our adversaries do not exploit these new arrangements, which could defeat the very goal of information sharing. In the global war on terrorism, we have entered into partnerships with foreign governments and international organizations whose many views and interests may be different from our own. We must ensure that intelligence sharing is measured against potential risks and that sensitive intelligence sources, methods, and operations are safeguarded.

IV. U.S. counterintelligence will safeguard the integrity of intelligence operations and analysis, and defeat foreign intelligence operations.

Intelligence is vital to the formulation and execution of U.S. national security policy and to the Nation's security. Today, the integrity of our intelligence is increasingly challenged as adversaries seek to deny us insight into their plans and mislead our decision-makers. Therefore, ensuring the reliability of intelligence becomes a key function of counterintelligence and is a necessary precondition to its very usefulness.

Foreign intelligence services have acquired significant amounts of our classified information, including sensitive U.S. intelligence capabilities. As a result of this knowledge, some countries have become very adept at deceiving and misleading us. These foreign powers attempt to present a false picture of reality through denial and deception operations which increases our uncertainty about their capabilities and intentions. It is the goal of counterintelligence operations and analysis to pierce that false picture, and the threats posed by these adversaries.

An intelligence capability is only as strong as the counterintelligence practices that ensure its integrity. Significant failures in counterintelligence can result in significant failures in positive or foreign intelligence. For example, while a given collection system may yield a wealth of intelligence, it may be useless and misleading if it has been corrupted to show only what an adversary wants us to see. While there are no guarantees that our intelligence collection efforts and our analysis are always accurate, we must establish rigorous procedures to help ensure the integrity of the intelligence that reaches decision-makers. Counterintelligence can supply techniques by which the reliability of a collection system, the *bona fides* of an asset, or the accuracy of an analytic judgment can be validated to ensure its integrity.

V. U.S. counterintelligence will seek to ensure a level economic playing field so that business and industry are not disadvantaged by foreign intelligence operations.

The United States is a nation of commerce and we value the freedom of trade as both a personal liberty and a cornerstone of national wealth. However, if adversaries can exploit the technological accomplishments of industry and gain an unfair advantage, not all trade inures to the Nation's good. While most foreign economic competition is open and lawful, it is not exclusively so. Some business competitors, supported by foreign intelligence services, employ classic intelligence methods in an attempt to gain an advantage over American companies. The outflow of sensitive trade secrets and proprietary information erodes our comparative economic advantage, and undermines national security. Foreign companies that unlawfully acquire U.S. technology are able to

compete unfairly against U.S. firms, which bear heavy research and development costs associated with innovative technology.

As our economy moves toward dependency on the benefits of information technology and networked data systems, our economic well-being and our national security could become vulnerable to foreign intelligence intrusion and manipulation of our cyber systems. We must ensure that we identify, understand, and counter these threats.

We will seek to identify foreign intelligence operations conducted against U.S. business and industry and we will provide the appropriate threat information to enable them to take such risk mitigation measures as they deem prudent.

VI. The intelligence community will ensure that counterintelligence analytic products are available to the President and his national security team to inform decisions.

To the extent we can observe them, the intelligence activities of foreign powers are a window into their respective interests and plans. Insights into the foreign intelligence activities of others can confirm or shape the prospects for cooperation. Effective counterintelligence analysis can connect the seemingly detached, illuminate hidden relationships, and reveal patterns of activity and behavior previously not observed. In this manner, counterintelligence can supply unique insights into the actions of our adversaries and the actions directed against us, as well as provide opportunities for advancing our own interests.

Counterintelligence represents a philosophic approach that can help bring coherence to many areas of national policy. Effective counterintelligence and security are integral to program efficiency, combat, and operational effectiveness, and foreign policy success. For each national security program, military endeavor, and foreign policy undertaking, there should be consideration for a corresponding counterintelligence plan to help ensure success.

This page left blank intentionally.

BUILDING A NATIONAL COUNTERINTELLIGENCE SYSTEM

The counterintelligence capabilities of the United States evolved over time to fit the shape and mission of the disparate institutions in which they are housed. The defined missions of some counterintelligence elements are non-specific, and taken together, these missions do not necessarily provide a response equal to the breadth of the threats arrayed against the United States. Together with their parent national security agencies, these counterintelligence elements must transform to meet the threats of the 21st Century.

Until recently, counterintelligence was an enterprise with no single leadership voice. The counterintelligence community's structure was fragmented and too tactically oriented to provide comprehensive protection to the Nation. The community was not designed to accomplish a strategic mission; rather, the various counterintelligence elements were part of a loose confederation of independent organizations with narrow and differing responsibilities, jurisdictions, and capabilities. Operations tended to focus on individual cases and were conducted with insufficient strategic overview of the potential impact of a synergistic effort.

In the future, each member of the counterintelligence community must be prepared to assume new responsibilities, and join together in a unity of effort, as the *National Counterintelligence Strategy* matures. To be effective, the *National Counterintelligence Strategy* requires that essential processes and features be inculcated into government structures and business models. A national system is needed to integrate, direct, and enhance United States counterintelligence in support of national security decision-making. The features of the National Counterintelligence System include:

National policy leadership and strategic direction. The Director of National Intelligence and the National Counterintelligence Executive, supported by the National Counterintelligence Policy Board, will chart the national counterintelligence mission and will direct and coordinate the resources of the counterintelligence community to accomplish a number of national-level goals including:

- A national program for counterintelligence activities that is strategic, coordinated, and comprehensive in understanding foreign intelligence threats.

- An array of strategic counterintelligence operational and informational options in foreign and defense policy for the President and his national security leadership team.

- A comprehensive assessment and description of foreign intelligence threats and risks to United States national security interests.

- The allocation of counterintelligence community resources prioritized against risk and opportunity.

- Specific counterintelligence policies for attacking foreign intelligence services systematically via strategic counterintelligence operations.

Facilities for cross-agency and cross-disciplinary work. Executing the national counterintelligence mission requires the careful orchestration and integration of many centers of analytic and operational expertise throughout the government. The Director of National Intelligence and the National Counterintelligence Executive will examine the need to establish a national counterintelligence center to integrate threat data, refine collection requirements, and provide a basis for initiating and supporting counterintelligence operations.

Damage assessment process. When national security secrets are lost through espionage or other disclosures, we must assess the loss and impact in order to mitigate damage. In the past, damage assessments received too limited a distribution because of security concerns. We must apply the lessons learned from damage assessments to ensure future vulnerabilities are mitigated. This will require the counterintelligence community take a more centralized approach to these assessments. We will improve the process to support more timely and thorough damage assessments, and ensure the findings are made available to decision-makers with relevant responsibilities.

Resources and performance measurement. The success of any intelligence initiative, sensitive technology development, or national security program depends in part on effective counterintelligence and security. In the past, counterintelligence support was viewed as an unfunded or underfunded mandate with little consideration of requirements or costs. The planning and budgeting processes should ensure that dedicated funding for counterintelligence and security requirements is integrated into sensitive plans and programs. We should seek to ensure the best use of resources is measured against the *National Counterintelligence Strategy* by including performance metrics to chart progress against strategic goals and objectives.

Training and standardization of the counterintelligence cadre. The training and education of collectors, analysts, investigators, and operators in the counterintelligence community has not always been equal to the performance we have demanded of them. The complexity of this subject requires a mastery of many disciplines and skills. The counterintelligence profession needs a set of common standards across many counterintelligence missions. We need to reach across departments and agencies to find centers of training excellence, address deficiencies, and upgrade the availability and uniformity of training.

Intelligence warning process. The discipline of counterintelligence, with its focus on patterns of and anomalies in activities and behaviors, can provide unique insights into foreign intelligence capabilities and intentions. We must ensure the perspectives gained from counterintelligence operations and analysis are incorporated into the intelligence indication and warning process.

This page left blank intentionally.

CONCLUSION

At the dawn of the 21st Century, the prospects for freedom, peace and prosperity have never been brighter. Yet we are a Nation at war, and we have suffered grievous attacks on our homeland. The threats we face are grave and diverse, and the intelligence threats that accompany them are equally complex. To respond to these threats, *The National Counterintelligence Strategy of the United States* calls for a proactive response utilizing all of our counterintelligence resources.

The components of this strategic response include:

- improvements to each of our counterintelligence capabilities to meet the range of foreign intelligence threats: human, technical and cyber.

- all-source counterintelligence analysis and strategic planning to drive operations in order to identify, assess, neutralize and exploit foreign intelligence activities before they can do harm to the United States.

- coordination, integration, and strategic orchestration of the activities of the counterintelligence elements of the government.

- counterintelligence support to, and involvement by, all national security policy elements of the government.

This page left blank intentionally.

NCIX Publication
Number 2005-10007
March 2005

Office of the National Counterintelligence Executive

March 2005