The National Counterintelligence Strategy of the United States of America

2007

The National Counterintelligence Strategy of the United States of America (2007) was drafted in coordination with the National Counterintelligence Policy Board. Chaired by the National Counterintelligence Executive, the National Counterintelligence Policy Board consists of senior personnel of departments and elements of the United States Government, appointed by the head of the department or element concerned, as follows:

the Department of Justice,
including the Federal Bureau of Investigation;
the Department of Defense,
including the Joint Chiefs of Staff;
the Department of State;
the Department of Energy;
the Central Intelligence Agency; and
the Department of Homeland Security.

PREFACE

This *National Counterintelligence Strategy of the United States of America* elaborates the fundamental responsibility for US intelligence to warn of and help prevent terrorist attacks against the homeland, engage other asymmetric threats, and provide reliable intelligence on traditional and enduring strategic issues. It also describes a way forward by which the counterintelligence organizations of the US government will engage elements in the public and private sectors to address the threat posed by the intelligence activities of foreign powers and groups and protect our nation's secrets and the means by which we obtain those secrets.

The *Strategy* has been produced by the National Counterintelligence Executive, coordinated across the counter-intelligence elements of the US government, and endorsed by the National Counterintelligence Policy Board.

Approved by the President as required by Section 402a of Title 50 of the United States Code, the Strategy provides guidance for the conduct of the counterintelligence programs and activities of the US government. I am confident that when implemented, it will enhance the integration and effectiveness of the nation's counterintelligence elements, as Congress intended in the National Counterintelligence Enhancement Act of 2002.

J.M. McConnell
Director of National Intelligence

FOREWORD

Counterintelligence is "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 personnel, physical, document or communications security programs." (Executive Order 12333 as amended)

The United States faces substantial challenges to its security, freedom, and prosperity. Transnational terrorism, continued proliferation of weapons of mass destruction (WMD), asymmetric warfare, extremist movements, and failed states present severe challenges to a just and stable international order. Our ability to meet these challenges is threatened by the intelligence activities of traditional and non-traditional adversaries. Our adversaries – foreign intelligence services, terrorists, foreign criminal enterprises and cyber intruders – use overt, covert, and clandestine activities to exploit and undermine US national security interests. Counterintelligence is one of several instruments of national power that can thwart such activities, but its effectiveness depends in many respects on coordination with other elements of government and with the private sector.

The agencies and departments that make up the counterintelligence community derive their authorities from the National Security Act of 1947, Exec.Ord. 12333, the Counterintelligence Enhancement Act of 2002, and the Intelligence Reform and Terrorism Prevention Act of 2004.

During the Cold War, our nation's adversaries gained access to vital secrets of the most closely guarded institutions of our national security establishment and penetrated virtually all organizations of the US intelligence and defense communities. The resulting losses produced grave damage to our national security in terms of secrets compromised, intelligence sources degraded, and lives lost, and would have been catastrophic had we been at war. Today we are engaged in a war, fighting terrorists who have invaded our nation's shores and threaten Americans and our allies around the world. In this struggle – which has cultural, economic, diplomatic, and political as well as military dimensions – the potential consequences of counterintelligence failures can be immediate and devastating, putting in jeopardy our nation's vital information, infrastructure, military forces and a wide range of US interests, technologies and personnel around the world.

In the wake of the attacks of September 11, 2001, the counterintelligence community has begun to evolve from a confederation toward a unified enterprise able to bring the full range of counterintelligence capabilities to bear on national issues. The Counterintelligence Enhancement Act of 2002, as amended, and the Intelligence Reform and Terrorism Prevention Act of 2004 accelerated this evolution and charged the National Counterintelligence Executive (NCIX) with producing this *National Counterintelligence Strategy* and providing the President with reports on its implementation. Yet much remains undone.

Counterintelligence activities include but are not limited to collection, analysis, investigations, and operations.

Continuing the process of integrating counterintelligence activities is an urgent national requirement. The counterintelligence community must do this through increasingly rigorous policy, doctrine, standards, and technology, and by aligning policy and practice with the budgetary and operational

priorities of the Director of National Intelligence (DNI). Counterintelligence activities must be orchestrated and integrated to better protect America's secrets and vital assets while providing incisive intelligence to national security decision makers.

The counterintelligence capabilities of the United States evolved over time to fit the shape and mission of the disparate institutions that controlled them. Taken individually, these capabilities do not provide a response equal to the breadth of the threats arrayed against the nation, and they have not always functioned cohesively in support of focused national priorities. Furthermore, repeated legislation and executive directives have emphatically called attention to our failure to align our activities and resources with a unified national counterintelligence policy. In 2002 Congress created the position of the NCIX to serve as the head of counterintelligence for the US government. Three years later The Commission on the Intelligence Capabilities of the United States regarding Weapons of Mass Destruction emphatically called attention to the failure to align activities and resources with a unified counterintelligence policy and called for the creation of a "Mission Manager" for counterintelligence. Subsequently, in 2006, the DNI named the NCIX the Mission Manager for Counterintelligence. Consistent with these authorities, the NCIX and the Office of the NCIX (ONCIX) will guide the integration of the counterintelligence community and implement its responsibilities to identify, assess, prioritize, and counter the intelligence threats to the United States.

The National Counterintelligence Policy Board was authorized by the Counterintelligence Enhancement Act of 2002. It serves as the principal mechanism for developing policies and procedures for the approval of the President to govern the conduct of counterintelligence activities.

The NCIX, in consultation with the National Counterintelligence Policy Board, will shape and set priorities for a unified national counterintelligence program that will guide the conduct of all the nation's counterintelligence activities. Moreover, the NCIX will engage with other elements of the Intelligence Community, the broader US government, the law enforcement community, the private sector, and academia to thwart intelligence threats directed against the United States. Only through a unified approach can the counterintelligence elements of the federal government successfully execute our duties to enhance the security of our nation, the integrity of the intelligence system, our competitive economic advantages, our armed forces, and our government's decision-making processes.

In this setting, the counterintelligence community is poised to make measurable progress, and the DNI expects us to do so. This task is urgent. We must capture our successes and efforts in measurable ways. Moreover, because resources are finite and cannot be expected to grow in the near term, the NCIX will make the hard decisions necessary to improve the efficiency of the nation's counterintelligence elements. At the same time, the recommendations resulting from counterintelligence assessments done in the wake of penetrations and unauthorized disclosures will be

rigorously followed up and monitored to assure that suitable mitigation measures are implemented.

This *National Counterintelligence Strategy* is the product of an intensive consultation process across the Intelligence Community. It sets forth strategic objectives for the counterintelligence community, and it does so consistent with statutory requirements. The strategy will guide the organizational, programmatic, and budgetary priorities of all counterintelligence elements of the US government. It will do so consistent with the President's *National Security Strategy*, the DNI's *National Intelligence Strategy*, and other applicable guidance. Essential strategic goals do not and should not change every year; yet the process of risk management requires that the counterintelligence community continually assess challenges, opportunities, and vulnerabilities. The NCIX will therefore review this strategy every year and, supported by the National Counterintelligence Policy Board, will make adjustments as circumstances require.

Joel F. Brenner
National Counterintelligence Executive

THE STRATEGY

The nation's counterintelligence elements will operate as a unified, coherent community and will jointly conduct their activities consistent with their respective capabilities and authorities and according to the priorities established by the National Counterintelligence Executive (NCIX).

SECURE THE NATION AGAINST FOREIGN ESPIONAGE AND ELECTRONIC PENETRATION.

The United States faces a wide range of threats to its security from foreign intelligence activities, terrorist elements, and other non-traditional adversaries designed to achieve advantage over US military, diplomatic, and economic interests at home and abroad. The counterintelligence community must act jointly to understand, confound, manipulate, and thwart these threats, which exceed the ability or resources of any single US agency or department to overcome. When necessary, we will disrupt these activities through arrest and expulsion.

The counterintelligence community will therefore identify and prioritize adversarial intelligence activities targeting US interests and leverage its collection, analytical, investigative, and operational resources to defeat these activities. We will also expand our capabilities in cyberspace. The cyber environment provides unprecedented opportunities for adversarial activities and is particularly vulnerable because of the nation's heavy reliance on information systems. The counterintelligence community will exploit and defeat adversary intelligence activities through the application of the full range of intelligence techniques.

In collaboration with our colleagues in the broader Intelligence Community and pursuant to strategic threat guidance, counterintelligence

The NCIX takes strategic threat guidance from the National Intelligence Priorities Framework (NIPF), the National Threat Identification and Prioritization Assessment (NTIPA), and other authorities.

elements will assess the intelligence capabilities and activities of foreign powers and non-state groups including terrorists and will describe their resources, plans, methods of operations, and worldwide reach. Foreign intelligence establishments and terrorist groups acquire resources, train and deploy personnel, and execute both clandestine and covert intelligence operations against us. The counterintelligence community must understand who they are, who their intelligence allies are, what they do, why they do it, and what they can do. Counterintelligence elements will use this knowledge to direct activities that counter, exploit, and defeat adversary intelligence activities – particularly the rooting out of spies in our nation's midst.

Accordingly, the counterintelligence community will conduct aggressive, strategically directed operations against priority intelligence targets around the world using the full range of operational means. The intelligence activities of foreign powers afford us opportunities to exploit their operations and gain access to their intelligence in order to corrupt its integrity. We will conduct worldwide operations to disrupt or defeat our intelligence adversaries as they assess and respond to the United States. Each agency and department will contribute its own unique capabilities, authorities, and resources in a unified effort.

PROTECT THE INTEGRITY OF THE US INTELLIGENCE SYSTEM.

The US intelligence system must provide reliable information to the US

government and its allies. The integrity and reliability of this system – the people, the structure, the information systems, and the information they hold – depend on our ability to keep it free from penetration or influence. In pursuit of this objective, the counterintelligence community will work closely with our colleagues in security, acquisition, information assurance, and other relevant specialties across the US government. The effectiveness of security countermeasures in preventing penetration will be enhanced by intelligence concerning the current nature and scope of the adversarial intelligence threat. No single department or agency alone can ensure the integrity of the US intelligence system and of our vital national assets.

Vulnerabilities are inherent in the human and technological dimensions of our culture, practices, standards, tradecraft, methods, and resources. Assessing these vulnerabilities is an integral part of the essential and continual task of risk management. Recommendations to address these risks will include vulnerability mitigation measures such as the institution of countermeasures, rigorous standards and practices, and the identification of opportunities for exploitation.

The ability of foreign powers and hostile groups to threaten the integrity of the US intelligence system relies in part on their knowledge of our security practices as well as intelligence and counterintelligence capabilities. Some of that knowledge has been made available to them through the robust workings of an open, democratic, and remarkably transparent society. That knowledge has been profoundly increased by foreign penetrations of our own government and by the treasonous acts of our own citizens. Thwarting the threat posed by foreign intelligence operatives depends on our skill in learning what they know, as well as confirming what they do not know about us, and in leveraging and exploiting that knowledge. That skill depends in large part on our success in penetrating these same adversaries in order to understand their full range of operational and analytical means. To the extent we do this, we will better protect our own secrets and decision making processes while producing superior foreign intelligence.

Decision makers require intelligence free from hostile control or manipulation. Since every intelligence discipline is subject to manipulation by our adversaries, validating the reliability of intelligence from all collection platforms is essential. Accordingly, each counterintelligence organization will validate the reliability of sources and methods that relate to the counterintelligence mission in accordance with common standards. For other mission areas, we will examine collection, analysis, dissemination practices, and other intelligence activities and will recommend improvements, best practices, and common standards.

Intelligence is vulnerable not only to external but also internal threats. Subversion, treason, and leaks expose our vulnerabilities, our governmental and commercial secrets, and our intelligence sources and methods. This insider threat has been a source of extraordinary damage to US national security. Countering this threat will require an aggressive national effort. In coordination with organizations responsible for areas such as security, information assurance, intelligence and law enforcement, and science and technology, the counterintelligence community must develop new policies, tools, and methods to deter, discover, and negate insider threats. For example, electronic systems designed to discover unexplained patterns of activities or anomalous events must be put in place, and they must be monitored. Adding these new tools and techniques to our nation's existing arsenal, the counterintelligence community will seek to

manipulate foreign spies, conduct aggressive investigations, make arrests and, where foreign officials are involved, expel them for engaging in practices inconsistent with their diplomatic status.

The Intelligence Reform and Terrorism Prevention Act of 2004 directed the Director of National Intelligence (DNI) to "ensure maximum availability of and access to intelligence information within the intelligence community consistent with national security requirements." The *National Intelligence Strategy* responded to that directive by requiring the Intelligence Community to ensure that its members and customers "can access the information they need when they need it." More specifically, we have been required to do a much better job of sharing information and to jettison the notion of "ownership" of information – a notion that encourages hoarding rather than sharing. This mandate will receive the full support of the counterintelligence community. At the same time we must scrupulously protect those pockets of information that are so sensitive that they can be disseminated only to those that meet the criteria for access. Counterintelligence risk is in direct tension with the seamless sharing of information. That is, the more readily available one makes classified information, the more likely it is to be somehow compromised, and the easier it is to steal.

Several espionage cases have already highlighted this vulnerability and have done incalculable harm to our national security. No counterintelligence official can guarantee our nation will never suffer another incident of treason or espionage. We can, however, assure the President, the Congress, and the American people that we have measurably increased the rigor of our system of national intelligence and have put in place systems, practices, and procedures that make foreign penetration more difficult to accomplish and easier to detect. To do this we must expand our efforts into cyberspace. We must act jointly to counter espionage; those counterintelligence elements that do not include security and law enforcement must be more closely tied to their security and law enforcement colleagues.

SUPPORT NATIONAL POLICY AND DECISIONS.

Foreign powers and adversarial groups use intelligence activities to support their national security goals, project power in areas of vital interest, and in some cases threaten the national security of the United States and its allies. When understood, these activities can provide *indications* of their strategic capabilities, limitations, and plans, and provide *warning* of unacceptable intentions. Such intelligence is vital to senior policy and decision makers as well as mission planners and operators.

It is imperative that we enhance the Intelligence Community's ability to advise our nation's decision makers of impending threats, vulnerabilities and opportunities. The counterintelligence organizations will do this through a joint approach to strategic analysis and by collaboratively supporting intelligence investigations and operations. National security plans, including counterterrorism and counterproliferation operations and the indications and warning function of our nation's intelligence system, are vulnerable to foreign intelligence activities. As the intelligence capabilities of our adversaries evolve, our effectiveness in thwarting them will depend on our ability to identify and fill critical intelligence gaps in both collection and analysis. In meeting these goals, we will exploit all available sources including open-source information, and will leverage new technologies and relationships.

Counterintelligence considerations must be included in mission planning to

ensure the operational community is aware of adversarial attempts to manipulate, deceive, or thwart their missions. As operations progress, a continued counterintelligence perspective also permits mission planners to take advantage of intelligence gathering opportunities that would otherwise be missed. This perspective is critical as we conduct our analysis of adversarial intelligence services and their relationship to terrorist organizations.

The *National Intelligence Strategy* directs the NCIX to support the analysis of terror networks. In coordination with the National Counterterrorism Center, the counterintelligence community will produce actionable analysis to support the disruption of terrorist operations and safeguard US intelligence capabilities. To further support counterterrorism, the counterintelligence community will review operations and intelligence reporting to detect attempts by terrorist entities to penetrate or manipulate us. We will also assess how key foreign intelligence services advance or obstruct US efforts to fight terrorism and counter those activities that are hostile.

Assessing the capabilities of foreign intelligence adversaries means understanding their collection platforms and their programs and activities. We must know how they are structured, how they operate, how their decision-making process works, and where they are deployed against US interests. This is both a collection challenge that the counterintelligence community must support and an analytical challenge that we must meet. We will conduct a common effort to address the most critical gaps in our knowledge of these targets, and, based on those gaps, we will contribute to the integrated collection strategies of the Office of the Director of National Intelligence (ODNI).

We will also provide strategic analysis, counterintelligence insight, and policy options to the National Security Council, the President's Foreign Intelligence Advisory Board, and the DNI to support their national security deliberations. We will report our assessments of the intelligence environment on a regular basis and will suggest actionable alternatives as appropriate.

Even with the most rigorous of security and counterintelligence practices we can expect compromises of classified information and operations. We must therefore conduct prompt and appropriately coordinated damage assessments that provide a strategic evaluation of the risk to US national security while initiating actions to mitigate damage and prevent further loss. In consultation with the Department of Justice in those cases with criminal implications and as appropriate, the damage assessment process will in the future begin sooner and produce results faster. Merely reporting our losses is not enough. The NCIX will therefore implement a follow-up mechanism that will, in coordination with the appropriate inspectors general and budgetary authorities, drive actionable recommendations.

PROTECT US ECONOMIC ADVANTAGE, TRADE SECRETS AND KNOW HOW.

In collaboration with our colleagues throughout the government, the counterintelligence community will protect our vital national assets – critical infrastructure, sensitive technologies, key resources, networks, and knowledge – from intelligence-related attacks. Our water and sewer systems, electricity grids, financial markets, payroll systems, and air- and ground-traffic control systems – to name only the most obvious – are electronically controlled and subject to sophisticated attack by both state-sponsored and free-lance hackers. These attacks can be designed to steal our nation's intellectual property or manipulate information to cause financial or

logistical chaos. While protecting the country's physical infrastructure is a duty of other elements of the government, counterintelligence has an important role to play in understanding who is planning and carrying out those attacks or preparing the ability to do so in order to parry them, and in some cases, to turn them to our advantage.

We must assist in the identification and protection of the nation's vital assets that reside in myriad elements of the US government, the private sector, and academia, and whose significance may be unknown even to those that control them. Collaboration between these parties and counterintelligence, law enforcement, and security officials is crucial to identify those targets of interest to our nation's adversaries. It is also crucial to identify information that, if known to an adversary, would probably be targeted and the loss or compromise of which would be damaging to the nation's security. Counterintelligence elements will work with law enforcement and security to develop, sustain, and leverage knowledge of our adversaries' strategies, collection priorities, intentions, and technical needs, and we will translate this knowledge into proposed collection requirements. We will also provide threat information and warning to vital asset owners, including those outside the US government.

SUPPORT US ARMED FORCES.

Counterintelligence activities protect those who protect America – especially the armed forces of the United States. To maintain the viability of this instrument of national power, the counterintelligence community must neutralize and exploit adversarial intelligence activities targeting the armed forces.

The armed forces have long been a priority target of terrorist attacks and the adversarial intelligence activities that support them. In recent decades we have witnessed attacks such as the bombings of the Marine barracks in Beirut, Khobar Towers in Saudi Arabia, and the *USS Cole* in the port of Aden. Such terrorist acts are always preceded by intelligence operations to reconnoiter targets and plan attacks, and it is these operations that we must recognize and thwart. Executive Order 12333 directs the nation's counterintelligence elements to protect against espionage. The *National Intelligence Strategy* further directs the Intelligence Community to "[d]eploy effective counterintelligence measures that enhance and protect... our armed forces...." In accordance with these mandates, the counterintelligence community will employ offensive and defensive capabilities to neutralize and exploit the full spectrum of adversarial intelligence activities targeting the armed forces, whether in garrison, in transit, or in their areas of responsibility.

The counterintelligence community will counter adversarial intelligence threats to military plans, operations, capabilities, intentions, and global posture, including the location and disposition of forces. Counterintelligence elements will support the full gamut of military operations from tactical activity to strategic initiatives. The armed forces' effectiveness depends on their ability to conduct military operations uncompromised by adversaries' foreknowledge. The obligation to support such operations extends beyond the Department of Defense to the entire counterintelligence community, which must collaborate to neutralize adversarial intelligence activity directed against our armed forces, especially the intelligence activities that precede terrorist attacks.

MANAGE THE COUNTERINTELLIGENCE COMMUNITY TO ACHIEVE EFFICIENT COORDINATION.

The integration and effective management of the counterintelligence programs of the agencies and departments of the Executive Branch is the NCIX's top priority. Working with the DNI Chief Financial Officer (CFO), the Office of the National Counterintelligence Executive (ONCIX) will develop a plan to assess current program development and performance, identify unnecessary redundancy, and advise the DNI CFO of more efficient ways to apply resources. Counterintelligence elements will provide the NCIX with the resource data and operational visibility required to perform the statutory functions of the office. In addition, continuity of operations of counterintelligence programs during emergencies and other contingencies must be maintained.

IMPROVE TRAINING AND EDUCATION OF THE COUNTERINTELLIGENCE COMMUNITY.

The increasing complexity of counterintelligence challenges requires us to address an ever-expanding range of threats. Meeting these emerging threats demands an adaptive, innovative, and broadly educated workforce drawn from a wide range of backgrounds.

As directed by the Counterintelligence Enhancement Act of 2002, as amended, and in consultation with the counterintelligence community, the ONCIX will develop policy and standards for training and professional development of individuals engaged in counterintelligence activities. We will, consistent with the *Intelligence Community's Five Year Strategic Human Capital Plan* and other US government efforts, engage in a unified effort to establish best practices, baseline our community's competencies, create core training courses, set professional standards, and support research initiatives. To the extent feasible, we will integrate our training efforts and standards with those of the National Intelligence University.

We will also develop an adaptable, expert counterintelligence workforce to meet the challenge of evolving intelligence threats. Our efforts will focus on three key areas. First, we will recruit personnel with a broader range of skills and experiences from outside the counterintelligence community. Specifically, we will target those who have experienced other cultures, speak other languages, or have specialized skills in information technology. Second, we will provide this cadre with a core understanding in counterintelligence tradecraft, building on best practices from across the community. Third, we will develop structured career paths that emphasize professional growth by identifying key assignments and leadership development opportunities and by clearly articulating promotion goals and standards. This lifecycle approach to counterintelligence careers will be grounded in a rigorous assessment of needs and integrated into wider human capital development efforts in the Intelligence Community.

EXPAND NATIONAL AWARENESS OF COUNTERINTELLIGENCE RISK IN THE PRIVATE AS WELL AS PUBLIC SECTOR.

In order to better fulfill the mission of identifying, assessing, and countering the intelligence threats to the nation, we must reach outward to other elements of the US government, the private sector, and the general public. By engaging the private sector and academia in meaningful dialogue, there is much we can learn, and in turn we can provide a mechanism to

coordinate the public dissemination of information on intelligence threats to the nation.

Foreign intelligence activities extend beyond traditional targets in the Intelligence Community and other US national security structures. The private sector and academia are fertile breeding grounds for advanced scientific discovery, cutting-edge technology, and advanced research and development that make them irresistible "soft targets" for foreign intelligence collectors. It is imperative that the American public understand that the cyber networks that businesses, universities, and ordinary citizens use every day are the object of systematic hostile activities by adversarial intelligence organizations, and that these activities threaten the integrity and safety of the nation's infrastructure and electronic networks. The counterintelligence community will engage the private sector, academia, and the general public in an ongoing dialogue regarding the threats we face and our responses to those threats.

Counterintelligence elements will work with willing private sector and academic partners to advance intelligence community capabilities through research and development and to anticipate and identify emerging technical threats. Where the counterintelligence community can form liaisons with willing partners, it will reach outward for information critical to targeting foreign intelligence activities and defending national security.

CONCLUSION

These strategic objectives will guide counterintelligence community policy, planning, collection priorities, analysis, operations, programming, budgeting, and execution. The ONCIX, in consultation with the National Counterintelligence Policy Board will oversee the implementation of the objectives through an integrated counterintelligence community effort to capitalize on the comparative advantages of its constituent organizations.