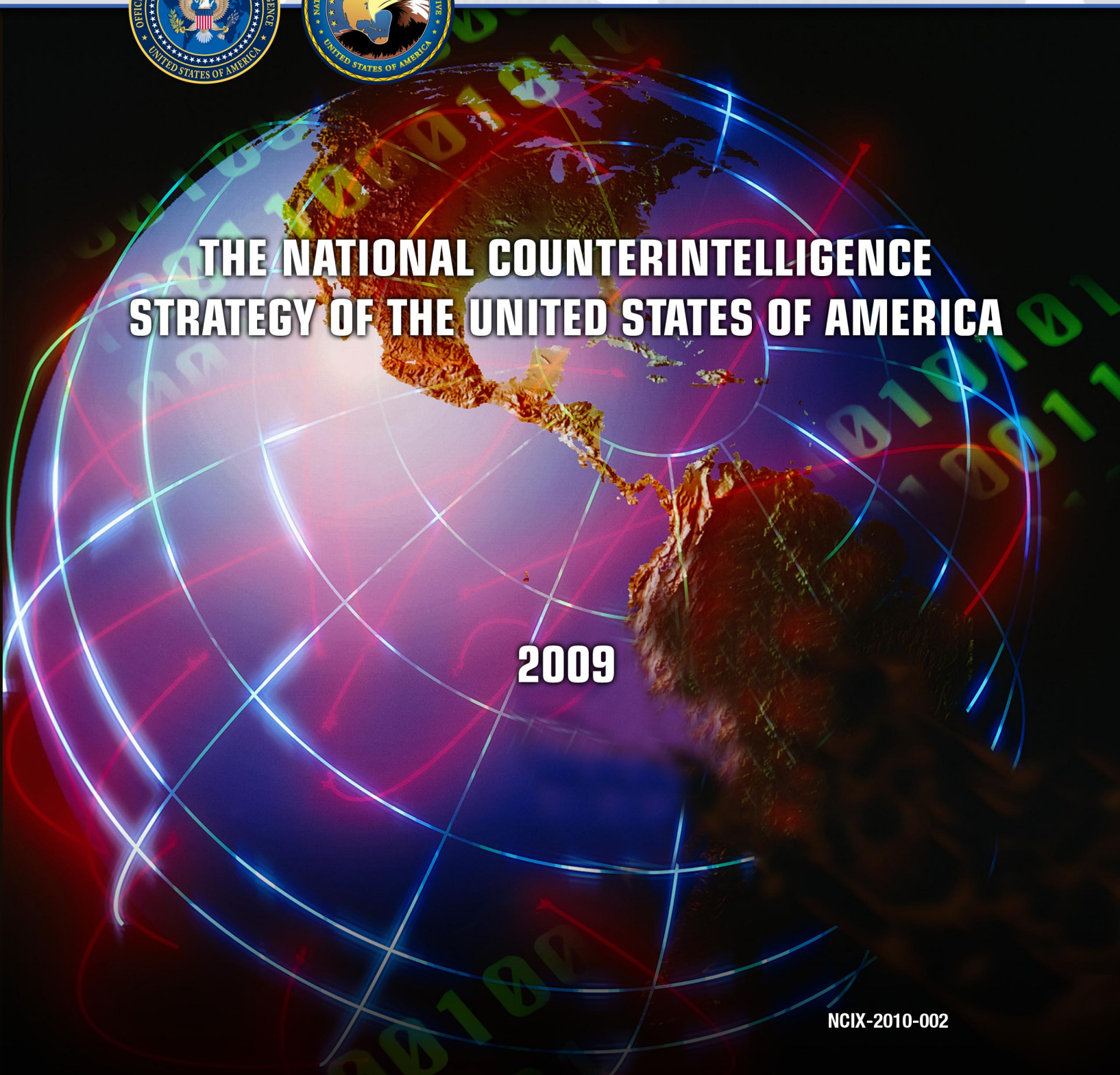
OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE



THE NATIONAL COUNTERINTELLIGENCE STRATEGY OF THE UNITED STATES OF AMERICA

2009

NCIX-2010-002

The National Counterintelligence Strategy of the United States of America (2009) was revised 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 State;
the Department of Defense,
including the Joint Chiefs of Staff;
the Department of Justice,
including the Federal Bureau of Investigation;
the Department of Energy;
the Department of Homeland Security;
the Central Intelligence Agency.

PREFACE

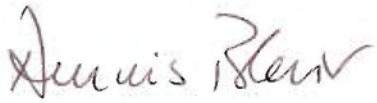
Approved by the President, as required by Section 402a of Title 50 of the United States Code, the *National Counterintelligence Strategy of the United States of America (Strategy)* serves as the United States Government's seminal planning document for government-wide counterintelligence efforts. This *Strategy* has been produced by the Office of the National Counterintelligence Executive (ONCIX), coordinated across the counterintelligence elements of the U.S. government, and endorsed by the National Counterintelligence Policy Board.

This *Strategy* is consistent with the *2009 National Intelligence Strategy (*NIS*)*, which for the first time elevated counterintelligence to a primary mission objective. The mission objective "Integrate Counterintelligence" is critical to accomplishing the NIS goals of enabling wise national security policies and supporting effective national security actions.

As a core intelligence mission, counterintelligence will be more fully integrated into the intelligence process. To achieve these goals, I have recently made several significant changes. I have appointed our nation's foremost counterintelligence professionals to the position of National Counterintelligence Executive (NCIX) and Deputy NCIX. The NCIX will lead the community efforts to identify and counter critical intelligence threats.

In an age of globalization and information sharing, greater openness has made us more vulnerable. Our information is being stolen at an alarming pace. In order to meet this challenge, our government's counterintelligence human and technical capabilities must function in a more integrated and coordinated manner than ever before. The NCIX has implemented a comprehensive counterintelligence effort, employing offensive and defensive measures that inform both policy and operations. We must understand not simply what foreign intelligence activities are being directed against the United States and its interests, but why, how and what our adversaries have learned about us.

Our nation expects us to lead the world in the intelligence arena. Our partners and allies expect the same. We are committed to keeping our national interests secure while building on the Intelligence Community's legacy of excellence.



Dennis C. Blair
Director of National Intelligence

FOREWORD

Strategy development is an ever-evolving and active process that ensures countries, institutions, and private industry look toward the future, provides direction, and sets appropriate goals and objectives. As the National Counterintelligence Executive (NCIX), I am charged with producing the *National Counterintelligence Strategy of the United States of America (Strategy)* on an annual basis. This *Strategy* provides strategic direction and guidance for counterintelligence activities of the United States Government to include the Intelligence Community.

Upon review of the *Strategy*, I have determined that the current mission and enterprise objectives are consistent with the 2009 *National Intelligence Strategy* (NIS), which for the first time, includes a mission objective for counterintelligence. The inclusion of the counterintelligence mission objective in the NIS reinforces the Director of National Intelligence's position that counterintelligence is a critical mission of the Intelligence Enterprise. The NIS mission objective states:

> *NIS Mission Objective 4: Integrate Counterintelligence. Provide a counterintelligence capability that is integrated with all aspects of the intelligence process to inform policy and operations. The Counterintelligence Community must build on its current efforts and focus on four areas:*
>
> - ***Detect insider threats.*** *Detect insiders who seek to exploit their authorized access in order to harm U.S. interests.*
> - ***Penetrate foreign services.*** *Penetrate hostile foreign intelligence services to determine their intentions, capabilities, and activities.*
> - ***Integrate CI with cyber.*** *Employ CI across the cyber domain to protect critical infrastructure.*
> - ***Assure the supply chain.*** *Assure the national security community's supply chain from foreign intelligence exploitation.*

The 2009 *National Counterintelligence Strategy* aligns to and supports the mission and enterprise objectives in 2009 *National Intelligence Strategy* and in particular addresses the four counterintelligence focus areas emphasized in NIS Mission Objective 4.

Detect insider threats. Insiders have caused grave, long-term damage to national security. History has demonstrated the intent of foreign intelligence services and entities to penetrate the Intelligence Community and extract information through the use of a trusted insider – recruited or volunteer. The Intelligence Community must be positioned to detect, respond to, and deter this threat. Currently, the Intelligence Community is creating a unified approach to combating insider threats. The Insider Threat Advisory Group (ITAG) leverages information assurance, security, and counterintelligence to detect, deter, and mitigate the

insider threat. The ITAG has identified fundamental insider threat elements, will define their "best practices," and will recommend standards and policy for a uniform Insider Threat Program.

Penetrate foreign services. The US faces numerous threats posed by state and non-state intelligence organizations. While the US must guard against those adversarial threats, we must also have a proactive approach to countering those threats. Effective penetrations substantially enhance our ability to counter, disrupt, and defeat operations inimical to US interests.

Integrate CI with cyber. The Intelligence Community must integrate counterintelligence into all aspects of computer network operations, workforce development, education, and awareness programs. We must identify, monitor, exploit and defeat hostile cyber activities through both offensive and defensive measures. Implementing such strategic activities will demand closer collaboration between offensive and defensive network operations to create the necessary synergies required to develop defenses against enemy tradecraft. To this end, we must strengthen collaboration among policy makers, law enforcement, counterintelligence elements, security, and other key players across the US Government on cyber operations. Collaboration must also be improved among the defense industrial base, think tanks, academic institutions, critical infrastructure sectors, and private industry partners as they all contribute to the national security mission.

Assure the supply chain. As US companies increasingly globalize their business structures and practices, foreign intelligence services may discover new avenues for penetration and exploitation of the United States government through its acquisition processes. Many Intelligence Community organizations and their counterintelligence elements are acting to address the unique threats and vulnerabilities in their own particular supply chains.

The DNI designated me as the Director of National Counterintelligence to clarify my roles and responsibilities within the Intelligence Community. As both the National Counterintelligence Executive and the Director of National Counterintelligence, in the coming year, I will work closely with the DNI, the counterintelligence community, other United States Government agencies, and the private sector to review and modify, as needed, the mission and enterprise objectives in the next counterintelligence strategy.

Continuity and agility in strategy, planning, and execution are important as we face threats that evolve slowly or change radically, year to year. As the Director of National Counterintelligence, I will lead the counterintelligence community's continuing efforts towards a unified and integrated enterprise, to execute this strategy.

Robert M. Bryant
National Counterintelligence Executive

THE STRATEGY

The nation's counterintelligence elements will operate as a unified, coherent community and will jointly conduct their offensive and defensive activities consistent with their respective capabilities and authorities and accomplish their objectives in accordance with 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 U.S. 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 U.S. 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 U.S. 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. A strong and well-protected U.S. information infrastructure is critical to virtually every aspect of maintaining our nation's security. Trusted insiders as well as external adversaries are targeting the U.S. information infrastructure for exploitation, disruption, and potential destruction. 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 U.S. INTELLIGENCE SYSTEM.

The U.S. intelligence system must provide reliable information to the U.S. 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 U.S. 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 U.S. intelligence system and of our critical national assets and critical infrastructure.

Threats and vulnerabilities are inherent in the human and technological dimensions of our culture, practices, standards, tradecraft, methods, and resources. Assessing these threats and vulnerabilities is an integral part of the essential and continual task of risk management. Recommendations to address these risks will include threat and 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 U.S. 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. Adversaries' knowledge can also be enhanced by accessing our information systems and networks, our supply chain and procurement processes, and our many scientific and research and development projects where foreign collaboration is valued and pursued. 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, the counterintelligence community will examine collection, analysis, dissemination practices, and other intelligence activities and will recommend and implement improvements, best practices, and common standards.

Intelligence is vulnerable not only to external but also to 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 U.S. 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, more sophisticated audit and analytical tools 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 counter-intelligence 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." 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 to counter foreign intelligence services and other adversaries who are using cyberspace to conduct intelligence activities directed against the U.S. 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 that 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.

In coordination with the National Counterterrorism Center, the counterintelligence community will produce actionable analysis to support the disruption of terrorist operations and safeguard U.S. 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 U.S. 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 U.S. 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 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 U.S. 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 U.S. ECONOMIC ADVANTAGE, TRADE SECRETS AND KNOW-HOW.

In collaboration with our colleagues throughout the government, the counterintelligence community will protect our critical national assets and critical infrastructure which include 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. The supply chain of the Intelligence Community is also at risk of exploitation in a globalized marketplace. Foreign companies or U.S. companies engaged in overseas partnerships may become targets for exploitation by adversaries seeking to gain unauthorized or unintended access to sensitive U.S. systems and technologies. These activities are 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 critical assets and infrastructure, which reside in myriad elements of the U.S. 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 critical national asset and critical infrastructure owners, including those outside the U.S. government.

SUPPORT U.S. 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, as amended, directs the nation's counterintelligence elements to protect against espionage. 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 ONCIX will develop a plan to assess current program development and performance, identify redundancy, and advise the DNI's CFO of 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. Consistent with the *Intelligence Community's Five Year Strategic Human Capital Plan* and other U.S. government efforts, we will 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 U.S. 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 U.S. national security structures. The private sector, other elements of government, 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 federal, state, and local governments, 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 federal state, and local governments, 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 continue to 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. The ONCIX will also continue to monitor the counterintelligence community's progress against these strategic objectives and provide our leaders with candid and accurate assessments on the state of the counterintelligence community.