Strategic Goal 1: Prevent Terrorism and Promote the Nation's Security Consistent with the Rule of Law

Terrorism is the most significant national security threat the country faces. Accordingly, the Department's top priority is, and will continue to be, protecting this Nation's citizens against acts of terrorism. The Administration has recognized that terrorism cannot be defeated by military means alone and DOJ is at the forefront of the fight against terrorism by providing a broad spectrum of tools and skills to combat terrorists. Specifically, DOJ's agents, analysts, and prosecutors will use every available resource and appropriate tool to detect, deter, and disrupt terrorist plots, investigate and prosecute terrorists, and provide global leadership in developing and implementing rule of law programs in other countries and partner nations to help prevent terrorism abroad. This will include renewed efforts to support where appropriate the prosecution of international terrorists in other countries through enhanced international cooperation. The Department will aggressively pursue emerging threats around the world and at home; enhance its ability to collect, analyze, and disseminate actionable intelligence; and engage in outreach efforts to all communities to prevent terrorism before it occurs.

Goal 1 outlines the work that DOJ will perform to strengthen the ability of the Federal Government to protect the American people from terrorism, within the letter and spirit of the Constitution. Adherence to the rule of law strengthens security by depriving terrorist organizations of their prime recruiting and fundraising tools.

The Department has established four objectives to guide work in this area:

Objective 1.1: Prevent, disrupt, and defeat terrorist operations before they occur by integrating intelligence and law enforcement efforts to achieve a coordinated response to terrorist threats

Objective 1.2: Prosecute those involved in terrorist acts

Objective 1.3 Investigate and prosecute espionage activity against the United States, strengthen partnerships with potential targets of intelligence intrusions, and proactively prevent insider threats

Objective 1.4 Combat cyber-based threats and attacks through the use of all available tools, strong public-private partnerships, and the investigation and prosecution of cyber threat actors

Numerous components within the Department will continue to protect the Nation's security by counteracting new and significant national security challenges, including cyber threats, weapons of mass destruction, espionage, and transnational organized crime with ties to foreign governments that seek to do harm to America.

Among the DOJ components that share responsibility for this goal are: Federal Bureau of Investigation (FBI), National Security Division (NSD), U.S. Attorneys, Criminal Division (CRM), Drug Enforcement Administration (DEA), Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the United States Marshals Service (USMS), and INTERPOL Washington. These components will work with federal, state, and local partners as well as international counterparts to combat terrorism. Additionally, following the objectives of the National Intelligence

Strategy, as determined by the Office of the Director of National Intelligence, the components of DOJ that are members of the Intelligence Community (FBI and DEA) will work with their partners to ensure that intelligence is collected, analyzed, disseminated, and acted upon across all members of the Intelligence Community and throughout the U.S. Government.

Objective 1.1: Prevent, disrupt, and defeat terrorist operations before they occur by integrating intelligence and law enforcement efforts to achieve a coordinated response to terrorist threats

Combating terrorism is DOJ's top priority. The Attorney General, acting primarily through the FBI, has principal investigative responsibility for all criminal acts of terrorism (18 U.S.C. § 2332b(f)). A key tenet of this objective is to ensure that intelligence and law enforcement agencies are able to use all available tools to investigate vigorously and prevent acts of terrorism in a manner consistent with law.

Strategies to Achieve the Objective

Integrate federal law enforcement and domestic/international intelligence efforts to dismantle terrorist networks and diminish their support worldwide

The Department's successes in a wide range of counterterrorism and counterespionage matters has solidified the idea that a highly sophisticated fusion of intelligence and criminal authorities is extraordinarily effective in thwarting attacks on U.S. soil. The Department will continue to combat each new threat by reinforcing, refining, and institutionalizing the fusion of intelligence and law enforcement operations in a cohesive manner to achieve a coordinated response to terrorist threats.

The Department will collect, analyze, and disseminate critical information related to terrorist activity directed against U.S. interests abroad and at home. The Department will ensure that the human and technological assets necessary to facilitate the collection of raw intelligence data will be in place and that the intelligence information produced will be relevant and timely in its delivery. DOJ will continue to share intelligence products with the U.S. Intelligence Community, state, local, and tribal Law Enforcement Community partners, and foreign governments, where appropriate. Additionally, DOJ will continue to ensure that the Intelligence Community is able to make efficient use of foreign intelligence information collection tools, particularly the Foreign Intelligence Surveillance Act (FISA), in a manner consistent with law through its representation of the United States before the Foreign Intelligence Surveillance Court.

The Department will detect, penetrate, and disrupt terrorist threats, cut off material support to terrorists, and ensure effective crisis response to attacks when necessary. The Department will prioritize investigative and operational efforts toward the collection of intelligence, and ensure, when applicable, that law enforcement tools to mitigate threats to the public are appropriately used. The Department will coordinate domestically among prosecutors, agents, and state, local, and tribal law enforcement. Additionally, the Department will support foreign government efforts to investigate and prosecute in their own courts terrorists who threaten U.S. national security, both by engaging and sharing information with foreign law enforcement and by building the capacity of foreign governments to investigate and prosecute terrorism cases.

Strengthen partnerships with federal, state, local, and tribal government agencies and foreign partners to prevent, deter, and respond to terrorist incidents

The Department recognizes that the most efficient and effective means of fighting terrorism is to communicate, coordinate, and cooperate with its partners. Those partners include the intelligence and law enforcement communities, the Department of State (DOS), the Department of Homeland Security (DHS), the Department of Defense, and allied foreign governments. In addition to working with other federal agencies, the Department also oversees more than 100 Joint Terrorism Task Forces (JTTFs) that bring together thousands of federal, state, and local law enforcement partners in order to ensure efficient coordination.

In order to increase and more strategically focus the Department's international counterterrorism efforts, DOJ will continue to develop strong working relationships with foreign counterparts to coordinate multi-national investigations, evidence gathering and sharing, and tracking and apprehending international fugitives. DOJ will also continue to share intelligence and develop counterterrorism strategies with its international partners. As part of this effort, the Department will work with foreign partners to effectively use our network of bilateral extradition treaties, mutual legal assistance treaties, multilateral conventions, and other international agreements and networks to share intelligence and to collaborate on criminal investigations. In particular, extradition and mutual legal assistance requests are critical tools for law enforcement and prosecutors in bringing criminals, including terrorists, to justice. Where appropriate, and in partnership with the Department of State, DOJ will pursue new treaty relationships that strengthen its ability to deter terrorism, share evidence, and secure the return of fugitives. In addition, DOJ will continue to provide assistance to foreign counterparts to improve the skills of foreign prosecutors, law enforcement, and judges; encourage legislative and justice sector reform in countries with inadequate laws; promote the rule of law and defense of human rights; and explore the possibility of posting additional Justice Department attorneys abroad to increase cooperation and capacity building engagements with foreign governments. Such assistance will enhance the ability of foreign governments to prevent and disrupt terrorism before it extends beyond their borders to threaten the United States and will help to establish a framework for effective international law enforcement cooperation.

Build and maintain a Security Sector Assistance (SSA) workforce aimed at strengthening the ability of the United States to promote national security by assisting allies and partner nations to build their own security capacity

Per the Presidential Policy Directive (PPD) 23: Security Sector Assistance (SSA), the Department of Justice has been identified as a key player in strengthening the ability of the United States to help allies and partner nations build their own security and capacity, consistent with the principles of good governance and the rule of law. The PPD reinforces the Department's important and ever-expanding role in working with foreign partners and multilateral organizations to promote national security and combat terrorism and transnational organized crime. In accordance with PPD-23, the Department of Justice will develop an implementation plan for building and maintaining SSA workforce capacity and the expertise necessary to implement effectively

all facets of the PPD. The Department also has a central role in supporting the President's *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security*, signed on July 25, 2011. Priority 6 of the Strategy directs DOJ to promote the development of criminal justice capacities on a worldwide basis, to the point where international law enforcement capabilities and cooperation among states are self-sustaining.

Objective 1.2: Prosecute those involved in terrorist acts

Vigorously investigating and prosecuting terrorism offenses is a critical tool in the effort to incapacitate terrorists, gather valuable intelligence, and deter future acts of terrorism. Since September 11, 2001, DOJ's counterterrorism successes include achieving numerous criminal convictions of high-profile terrorists, defeating would-be terrorists, and protecting the Nation through prevention efforts. The investigation, disruption, and prosecution of terrorism will continue to be the top priority for the Department.

Strategies to Achieve the Objective

Build strong cases for prosecution

The top priority for the Department is to protect the Nation from terrorist attacks while ensuring that the civil liberties of our people are protected. In addition to providing coordination and expertise to prosecutors, law enforcement agencies, intelligence analysts, and the Intelligence Community, the Department ensures that national security investigations are conducted in a manner consistent with the Nation's laws, regulations, and policies, including those designed to protect the privacy interests and civil liberties of the American people. The Department's organizational structure ensures coordination and unity of purpose between prosecutors and law enforcement agencies, on the one hand, and intelligence attorneys and the Intelligence Community, on the other, thus strengthening the effectiveness of the DOJ's national security efforts.

The Department has been especially concerned with two relatively new threats: "lone wolf" terrorists who self-radicalize, and terrorist use of the Internet and other media to incite others to violence. In addressing both of these threats, the Department has adopted aggressive, but lawful, strategies. For instance, to address the possibility of lone-wolf terrorists the Department has prioritized the efforts of the Anti-Terrorism Advisory Council (ATAC) —a nationwide counterterrorism program that ensures experienced and trained Assistant United States Attorneys are prepared in every federal district in the country. The ATAC program has helped lead to the successful disposition of counterterrorism cases in a variety of locales, including many that are outside the large metropolitan areas, which have been traditional targets of terrorism.

Additionally, a specific prosecution strategy that the Department continues to develop is to focus Racketeer Influenced and Corrupt Organization (RICO) methods and charges on U.S.-based terrorist infrastructure. The RICO statute is typically used to hold organized crime, gang members, and others accountable for the full extent of their criminal activity conducted as part of an enterprise over a period of time and can include a wide variety of criminal activity. RICO allows prosecutors to include both state and federal violations as underlying racketeering acts within a single

RICO charge. Regarding terrorism, RICO has and will continue to be used to charge those involved in terrorist activities as well as those providing material support to terrorist organizations. The Department is proposing to amend the RICO statute to include a limited number of foreign crimes, thereby extending RICO extraterritorially in a non-money laundering context, and to clarify that RICO has extraterritorial application when predicate acts occur or part of the enterprise operates in the United States.

Objective 1.3: Investigate and prosecute espionage activity against the United States, strengthen partnerships with potential targets of intelligence intrusions, and proactively prevent insider threats

Foreign espionage strikes at the heart of U.S. national security, impacting political, military and economic arenas. The foreign intelligence threat to the United States is expanding, becoming more complex and less predictable. While traditional threats to national defense, military operations and policy, and intelligence, and science and technology remain, many intelligence threats are expanding their targets to include the burgeoning population of cleared defense contractors and other sectors affecting U.S. security, most notably sensitive economic information and emerging proprietary technology. Concurrently, foreign threats now have sophisticated networks of governmental and non-governmental entities using a wide array of intelligence collection platforms and engaging in long-term efforts to obtain sensitive information and threaten the security of the United States.

The Department will combat espionage by, among other things, vigorously investigating and prosecuting violations of espionage statutes and regulations. Additionally, DOJ will investigate and prosecute violations of export control and embargo statutes and regulations by combining intelligence and law enforcement to target individuals and networks involved in the illicit trafficking of controlled technologies and the proliferation of weapons of mass destruction and will expand its export control initiative to ensure nationwide coverage.

Strategies to Achieve the Objective

Protect U.S. national security against espionage and illegal foreign acquisition of U.S. technology

The Department will strive to combat espionage by becoming more proactive and preventive in approach, identifying early indications and warnings of traditional espionage and other less traditional espionage-related activities, such as the illicit transfer of technology, export control, theft of Intellectual Property (IP), and trade secret compromise. The Department will focus on developing strategic partnerships with and across the spectrum of military, industrial, and research stakeholders, owners, and developers. In addition, the program will identify specific targets of, and vulnerabilities to, foreign intelligence service intrusion and will identify priority threat country objectives and operations via sophisticated human intelligence and technical counterintelligence operations, including offensive and defensive cyber techniques.

The U.S. Government promotes foreign investment in the United States because such investment helps to keep the economy strong, vibrant, and integrated with the global economy. In certain situations, however, foreign investment can pose national security risks, result in unacceptable

transfers of sensitive United States technologies, or expose the critical infrastructure of the United States to hostile intelligence services and terrorist organizations. To address this concern, DOJ will continue to work with other agencies to review proposed acquisitions of certain American companies by foreign companies to balance the interest in promoting foreign investment with the need to protect national security.

Strengthen the Department's intelligence base and analytical capability to assess and respond to intelligence threats

Foreign intelligence information, including physical and electronic surveillance, is a critical tool for protecting the nation from terrorism, espionage, and other national security threats. Many of the Department's significant national security prosecutions – and countless intelligence actions that do not result in prosecution – would not be possible without the government making full use of the authorities available to it under a variety of federal laws, including the Foreign Intelligence Surveillance Act. The Department will continue its important work of representing the government before the Foreign Intelligence Surveillance Court. In addition, DOJ will expand its oversight operations, promoting ongoing communication and cooperation with the Intelligence Community, and advise relevant entities within the Executive Branch and Congress on the use of intelligence authorities.

Proactively prevent insider threats

As the Department leads the way in prosecuting those who wish to threaten our national security, it must also balance this effort with protecting civil liberties and maintaining the security of classified information. The Department must protect against the dissemination of classified material that would harm national security by investigating and, when possible, prosecuting individuals who disseminate classified information without authorization in order to deter future disclosures. This includes preventing information security breaches by the significant number of government employees and contractors with high levels of access to sensitive information. To address the evolving insider threat, the Department has become more proactive to prevent losses of information and technology. The Department continues to expand outreach and liaison alliances to government agencies, the defense industry, academic institutions, and to the general public.

Objective 1.4: Combat cyber-based threats and attacks through the use of all available tools, strong private-public partnerships, and the investigation and prosecution of cyber threat actors

A range of cyber activities can diminish our security and siphon off valuable economic assets. A growing number of sophisticated state and non-state actors have both the desire and the capability to steal sensitive data, trade secrets, and intellectual property for military and competitive advantage. The other major national security threat in cyberspace is cyber-enabled terrorism. The Department believes that it is a question of when, not if, there will be attempts to do so.

The cyber threat demands ready and fluid means of sharing information and coordinating actions. To successfully investigate and disrupt cyber threats, the Department must be creative and forward-looking in its approach, considering what kinds of tools, investigations, and outreach can be launched now to lay the groundwork

for future cyber efforts. As an example, the Department has partnered with nations worldwide in the INTERPOL Global Complex for Innovation, which will enhance its operational and investigative cyber capabilities through international cooperation and innovative technical solutions and systems. Collaboration with the private sector is also crucial to prevent breaches and protect confidential and proprietary information.

Strategies to Achieve the Objective

Protect the Nation from cyber attacks

Terrorists and other hostile adversaries plan and commit national security related crimes against the United States using the Internet and seeking a veil of anonymity. These illicit activities are not limited to using cyberspace to plan and execute classic espionage and terrorism, but can also include novel forms of national security threats to American assets and infrastructure. Consequently, the U.S. Government's national security operations increasingly focus on online conduct and communications.

The Department's cyber strategy involves an all-tools approach, inclusive of investigation and prosecution, and with a focus on the disruption of the threat, regardless of the particular tool used. For example, cyber threats could be disrupted using civil enforcement, regulatory enforcement, supply chain efforts, or other operations, and the offenses charged may not be limited to cybercrimes.

The Department has significant and growing national security responsibilities in the area of cyber security. Department attorneys regularly collaborate with agencies within the intelligence and defense communities with respect to both defensive and offensive cyber security operations. In addition, the Department retains primary authority over the investigation and prosecution of cyber-crimes, including those that have national security implications. These investigations most frequently arise in instances where an agent of a foreign government seeks to infiltrate or harm a sensitive or important piece of U.S. cyber infrastructure. The Department also works to disrupt cyber-attacks as a method of addressing ongoing intrusions, thefts of sensitive data, and attacks on the integrity and availability of systems. Finally, the Department has increasing legal and policy duties assisting interagency and legislative cyber initiatives to protect American critical infrastructure, networks, businesses, and computer users in a manner consistent with the law.

Develop and implement national cyber policies

To keep pace with the unique challenges of the evolving cyber threat, the Department will need to: hire, recruit, and train additional cyber-skilled professionals; prioritize disruption of cyber threats to the national security through the use of the U.S. Government's full range of tools, both law enforcement and intelligence; promote legislative priorities that adequately safeguard national security interests; invest in information technology that will address cyber vulnerabilities while also keeping the Department at the cutting edge of technology; and work with international partners to ensure a coordinated effort to counter the cyber threat.