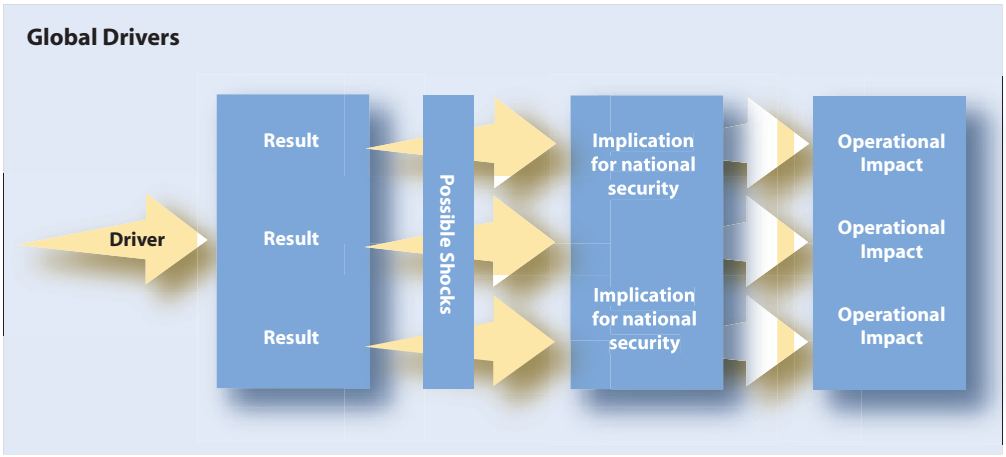
SECTION I

# FBI FORECAST

*The foundation of strategic planning is long-term forecasting. The FBI's enterprise-wide Intelligence Program provides robust forecasting capability, which integrates external and internal data to forecast global drivers and their operational impacts. Those impacts, in turn, are translated into organizational goals and objectives. The FBI identifies global "drivers" — broad factors that can directly or indirectly cause changes in the future threat environment. These "drivers" correlate in many ways to categories or "dimensions" used in a variety of U.S. and foreign forecasts. The FBI forecast process focuses on seven global drivers, outlined below and discussed in more detail in Appendix A. From those drivers, we identify probable results, as well as less probable results caused by "shocks" — high-impact, low probability events. The results are then assessed for their implications on the FBI mission and its strategic planning process. From those implications, a list of operational impacts, as well as organizational and recruiting consequences, is produced.*



The most notable operational impacts and organizational consequences related to each "driver" identified by the FBI are:

### (1) Global and domestic demographic changes

- global — more operations abroad; need increased intelligence from within immigrant communities; wider variety of linguists required
- domestic/internal — rapid FBI staff turnover presents opportunity for culture change, but loss of corporate memory

### (2) Communications revolution

- intelligence — encryption constrains Foreign Intelligence Surveillance Act (FISA) operations, will need to get closer to end-nodes
- investigations — identity theft will make perpetrator identification more difficult
- internal — easier FBI peer-to-peer communications; greater need for technically savvy staff; need for alternate communications in event of catastrophic outage

### (3) Global economic changes

- external — terrorism and organized crime converge; greater need for coordinating countermeasures with foreign countries and financial organizations
- internal — difficulty recruiting highly paid technical talent

### (4) Rising belief in non-material values abroad

- external — increasing danger to agents working abroad as anti-Americanism increases and actors disperse, FBI may become target
- internal — greater difficulty recruiting ethnic Arabs and Muslims, as well as any newly identified ethnic groups associated with threats

### (5) Technological revolutions

- external — reduced ability for threat groups or governments to hide undercover identity of agents; increase in espionage and cyber crime against U.S. corporations
- internal — need for increased technical recruiting; need for enhanced civil liberties training as technology outpaces policy

### (6) Revolutions in security technology and practice

- international — more "policing" actions abroad; more espionage against U.S. defense and contractors
- internal — need for continuity of operations following attack on FBI; mounting political pressure for technical solutions faster than they can be produced and implemented

### (7) Changing role of state and law

- external — need to cooperate with more entities; need more methods of cooperation beyond task forces and cases
- internal — need to reassess security procedures as number of non-FBI partners and participants grows

The FBI forecasts that sub-national and non-governmental entities will play an increasing role in world affairs for years to come, presenting new "asymmetric" threats to the United States. Although the United States will continue to occupy a position of economic and political leadership — and although other governments will also continue to be important actors on the world stage — terrorist groups, criminal enterprises, and other non-state actors will assume an increasing role in international affairs. Nation states and their governments will exercise decreasing control over the flow of information, resources, technology, services, and people.

Globalization and the trend of an increasingly networked world economy will become more pronounced within the next five years. The global economy will stabilize some regions, but widening economic divides are likely to make areas, groups, and nations that are left behind breeding grounds for unrest, violence, and terrorism. As corporate, financial, and nationality definitions and structures become more complex and global, the distinction between foreign and domestic entities will increasingly blur. This will lead to further globalization and networking of criminal elements, directly threatening the security of the United States.

Most experts believe that technological innovation will have the most profound impact on the collective ability of the federal, state, and local governments to protect the United States. Advances in information technology, as well as other scientific and technical areas, have created the most significant global transformation since the Industrial Revolution. These advances allow terrorists, disaffected states, weapons proliferators, criminal enterprises, drug traffickers, and other threat enterprises easier and cheaper access to weapons technology. Technological advances will also provide terrorists and others with the potential to stay ahead of law enforcement countermeasures. For example, it will be easier and cheaper for small groups or individuals to acquire designer chemical or biological warfare agents, and correspondingly more difficult for forensic experts to trace an agent to a specific country, company, or group.

In the 21st Century, with the ready availability of international travel and telecommunications, neither crime nor terrorism confines itself territorially. Nor do criminals or terrorists restrict themselves, in conformance with the structure of our laws, wholly to one bad act or the other. Instead, they enter into alliances of opportunity as they arise; terrorists commit crimes and, for the right price or reason, criminals assist terrorists. Today's threats cross geographic and political boundaries with impunity; and do not fall solely into a single category of our law. To meet these threats, we need an even more tightly integrated intelligence cycle. We must have extraordinary receptors for changes in threats and the ability to make immediate corrections in our priorities and focus to address those changes. And, we must recognize that alliances with others in law enforcement, at home and abroad, are absolutely essential.

**Counterterrorism Forecast:** Terrorism is the most significant threat to our national security. In the international terrorism arena, over the next five years, we believe the number of state-sponsored terrorist organizations will continue to decline, but privately-sponsored terrorist groups will increase in number. However, the terrorist groups will increasingly cooperate with one another to achieve desired ends against common enemies. These alliances will be of limited duration, but such "loose associations" will challenge our ability to identify specific threats. Al-Qaeda and its affiliates will remain the most significant threat over the next five years.

The global Weapons of Mass Destruction (WMD) threat to the United States and its interests is expected to increase significantly in the near term. We expect terrorists to exploit criminal organizations to develop and procure WMD capabilities. Globalization will make it easier to transfer both WMD materiel and expertise throughout the world. The basic science and technologies necessary to produce WMD will be increasingly well understood. Similarly, raw materials will be more available and easier to obtain.

Violence by domestic terrorists will continue to present a threat to the United States over the next five years. The number of traditional left wing terrorist groups, typically advocating the overthrow of the U.S. Government because of the perceived growth of capitalism and imperialism, have diminished in recent years. However, new groups have emerged that may pose an increasing threat. Right wing extremists, espousing anti-government or racist sentiment, will pose a threat because of their continuing collection of weapons and explosives coupled with their propensity for violence. The most significant domestic terrorism threat over the next five years will be the lone actor, or "lone wolf" terrorist. They typically draw ideological inspiration from formal terrorist organizations, but operate on the fringes of those movements. Despite their ad hoc nature and generally limited resources,

they can mount high-profile, extremely destructive attacks, and their operational planning is often difficult to detect.

**Counterintelligence Forecast:** The threat from countries which consider the United States their primary intelligence target, adversary or threat either will continue at present levels or likely increase. The most desirable U.S. targets will be political and military plans and intentions; technology; and economic institutions, both governmental and non-governmental. Foreign intelligence services increasingly will target and recruit U.S. travelers abroad and will use non-official collection platforms, including increasing numbers of students, visitors, delegations, and emigres within the United States. Foreign intelligence activities are likely to be increasingly characterized by the use of sophisticated and secure communication technology to handle recruited agents and to be more likely than in the past to occur almost anywhere in the United States.

**Cyber Forecast:** Cyber threats confronting the United States emerge from two distinct areas: (1) traditional criminal activity that has migrated to the Internet, such as fraud, identity theft, child pornography, and trade secret theft; and (2) Internet-facilitated activity, such as terrorist attacks, foreign intelligence threats, and criminal intrusions into public and private networks for disruption or theft. The vulnerability of the United States to such activity is rapidly escalating as its economy and critical infrastructures become increasingly reliant on interdependent computer networks and the World Wide Web. The cyber threat to our national security stems from two groups: (1) non-state actors such as terrorist groups and hackers; and (2) foreign governments that have developed cyber espionage or information warfare programs to target U.S. networks. The number of foreign governments and non-state actors exploiting computer networks and developing their cyber capabilities is on the rise.

**Public Corruption Forecast:** The corruption of local, state, and federally elected, appointed, or contracted officials undermines our democratic institutions and sometimes threatens public safety and national security. The root of corruption is greed, and over the next five years there will be increased government spending and increased opportunities for government officials to violate the public trust. As our nation tightens security at our land borders and our air and sea ports to prevent terrorism — terrorists, international drug enterprises, and alien smuggling rings will increasingly seek to recruit U.S. law enforcement officials to further their operations, thereby undermining our security at the borders. Likewise, as additional controls are established to minimize identity fraud, there will be an increase in demand by criminal enterprises to corrupt government officials who issue identification documents.

**Civil Rights Forecast:** Most hate crimes statistics have remained relatively constant, but there have been specific areas of increased activity. From 1996 to 1998, there was a spike in arson against religious properties. Since 9/11, there has been an unprecedented number of hate crimes directed against Muslim, Sikh, and Arab-American individuals and institutions. In the event of another terrorist attack on U.S. soil or against U.S. interests abroad, we anticipate similar spikes of activity directed against persons who share actual or perceived ethnicity, religion, or national origin with the terrorists. In addition, the number of crimes under "Color of Law" statutes is expected to increase in direct proportion to the increase in the number of law enforcement and correctional officers over the next decade.

**Transnational/National Crime Forecast:** Drug trafficking poses a continuing threat, responsible for an estimated 50,000 drug-related deaths and $110 billion in social costs per year. In producer countries, the trade funnels both money and power to criminal elements and illegally armed groups, and provides a breeding ground for corruption, violence, environmental degradation, and political and economic instability. Gang-related violence will continue as long as the demand for illicit drugs remains or increases, and drives gangs to battle for retail drug distribution markets, especially in large user-based metropolitan areas. Human trafficking organizations have increased dramatically in recent years, and will likely continue to do so over the next five years. Worldwide human smuggling is estimated to be a $7 billion industry, bringing hundreds of thousands of illegal immigrants to the United States each year. Increasingly, terrorists and their supporters will use alien smuggling networks to circumvent increased border security measures implemented since 9/11. International criminal groups will grow and form new partnerships and alliances due largely to globalization. It is likely that criminal groups will expand their intelligence capabilities to thwart law enforcement investigations.

**White Collar Crime Forecast:** Major white collar crime will impact the U.S. economy over the next five years. Corporate fraud has undermined the public's confidence in American business institutions, and the aggressive investigation and prosecution of major corporate fraud will be a key factor in restoring long-term confidence in our business leaders. Money laundering poses a growing threat to national security. Advances in technology and the globalization of financial institutions will allow terrorist and criminal organizations to more easily influence economic, social, and political institutions. Money launderers and those engaging in financial institution fraud will increasingly use sophisticated computer technology, offshore banking, and complex financial mechanisms to facilitate their criminal activity and hide illicit proceeds. An increase in government procurement from industry over the next five years will create opportunities for major fraud. Health care fraud is expected to increase dramatically over the next decade as the aging of the U.S. population drives increases in private health care and Medicare spending.

**Violent Crimes Forecast:** General violent crime rates have significantly decreased over the last five years (1997-2002); however, murders have increased over the last three years (1999-2002). Additionally, within the first six months of 2003, murder rates in the northeast United States continued to rise. New York, Newark, Philadelphia, and Baltimore all had significantly more murders compared to the same period in 2002. Major violent incident crimes, such as sniper murders and child abductions will continue. These crimes paralyze whole communities and stretch local law enforcement resources often for long periods of time. The widespread publicity associated with sniper murders may produce imitators. The problem of organized child prostitution will continue to increase as criminal enterprises victimize juveniles to meet increasing demands.