TRANSPARENCY INTERNATIONAL
the global coalition against corruption

Defence Integrity Pacts
Identifying the corruption risks in defence and security
Enlisting the defence contractors
Integrity self-assessment by nations
Developing counter-corruption pl

BUILDING INTEGRITY AND COUNTERING CORRUPTION IN DEFENCE & SECURITY

20 PRACTICAL REFORMS

Using metrics and surveys
Involving civil society
Leading Change
Reducing corruption risks in contracts in operations
Educating change leaders
Independent Monitoring
Codes of Conducts, values and behaviours
Military-owned businesses
Build leadership understanding
Diagnosis of Corruption Risks
Strategic and planning considerations for conflict environments
Asset disposal

www.transparency.org

1. IDENTIFYING THE CORRUPTION RISKS IN DEFENCE AND SECURITY

Corruption is a broad term. This Handbook breaks it down into 29 specific defence corruption issues that provide a basis for a country-specific analysis.

There is no generic diagnosis, and therefore no generic plan that will work in every situation. However there are key risk areas and recurring problems across the world. To help diagnose the risks, TI has devised a framework for understanding defence and security corruption that can guide you around the range of possible corruption issues and provide a starting point for your own analysis.

This framework has been used during dialogue with the senior leadership in many nations: with defence ministers, the most senior officials and high-ranking military officers, as well as at public meetings and with civil society.

While neither definitive nor exhaustive, the framework is robust enough to serve as the starting point for most nations. It breaks the generality of defence and security corruption down into five broad headings encompassing different types of corruption. Those areas of defence where corruption is most significant and causes the greatest problems have a subsequent chapter of this handbook devoted to them.

This framework is a good tool to open the debate within a ministry or department or across the armed services. It can identify which issues are relevant and which need to take priority. It can be used to talk to colleagues and identify which issues are significant.

FIGURE 1: FRAMEWORK FOR DEFENCE AND SECURITY CORRUPTION

POLITICAL	PERSONNEL	PROCUREMENT
DEFENCE & SECURITY POLICY	LEADERSHIP BEHAVIOUR	TECHNICAL REQUIREMENTS / SPECIFICATIONS
DEFENCE BUDGETS	PAYROLL, PROMOTIONS, APPOINTMENTS, REWARDS	SINGLE SOURCING
NEXUS OF DEFENCE & NATIONAL ASSETS	CONSCRIPTION	AGENTS/BROKERS
ORGANISED CRIME	SALARY CHAIN	COLLUSIVE BIDDERS
CONTROL OF INTELLIGENCE SERVICES	VALUES AND STANDARDS	FINANCING PACKAGE
EXPORT CONTROLS	SMALL BRIBES	OFFSETS
		CONTRACT AWARD, DELIVERY
FINANCE	**OPERATIONS**	SUBCONTRACTORS
ASSET DISPOSALS	DISREGARD OF CORRUPTION IN COUNTRY	SELLER INFLUENCE
SECRET BUDGETS	CORRUPTION WITHIN MISSION	
MILITARY-OWNED BUSINESSES	CONTRACTING	
ILLEGAL PRIVATE ENTERPRISES	PRIVATE SECURITY COMPANIES	

POLITICAL

If a corrupt individual or group is able to influence defence and security policy (for example, to create a requirement for procurement of fast jets when no such need truly exists), this is high-level corruption. The subsequent procurement process can be largely clean, yet fundamentally flawed.

A **defence** process can be manipulated or overcomplicated in order to hide corrupt decisions and illicit enrichment, for example, if a policy approval procedure is lacking or policy decisions are not published. In the most extreme cases, defence corruption at the highest level might represent 'state capture', if an elite is able to shape state decisions across a much wider area.

Where countries are rich in natural assets, such as oil, timber, minerals or fish, the military or security forces can become closely or improperly connected with their exploitation. This **nexus of defence/security and natural assets** is common in conflict environments (for example, in Sierra Leone with diamonds, Angola with oil), but it also occurs in peacetime circumstances, as in Nigeria or Indonesia. Such linkages can be prime drivers of subsequent conflict.

Organised crime is present in every country and is a growing transnational security threat. Increasingly technology-enabled, it does not respect national or international boundaries and prospers in ungoverned spaces such as fragile states. Motivated by the acquisition of wealth, it is arguably beyond the power of any one agency or nation to contain effectively, and may have penetrated the defence, security and intelligence establishment. In these circumstances counter-corruption strategies will have little chance unless organised crime is prioritised and addressed at the same time.

Corruption within the **intelligence services** has been a significant problem in some countries, notably in post-communist and post-conflict societies. Intelligence services gather information that has potential economic and political leverage. This makes them an attractive target for corrupt behaviour.[1]

Arms export controls are susceptible to the risk of corruption as a vehicle for illegal arms transfers with negative consequences for international humanitarian law, human rights, and sustainable development. Corruption also hinders efforts to combat violent organised crime and terrorism as it undermines the ability of states to control the diversion of weapons from their intended end-users.

FINANCE

Misuse of defence and security budgets is one of the most common problem areas. In the defence sector a culture of secrecy can create an environment in which good financial practices such as auditing by an external division are not employed on the grounds of national security. Yet much public trust is gained by being more transparent. In any organisation or department, sound management of assets, with timely and efficient accounting systems, is one of the most powerful devices for maintaining integrity. The better the systems in place, the less opportunity there will be for corruption. As well as providing opportunity for fraud, a poor and disconnected accounting system makes it easy to conceal irregularities. Even if irregularities are found, poor accounting makes it impossible to identify those responsible, and hold them to account.

Asset disposals are a common category for corrupt management. This can occur through the misappropriation or sale of property portfolios and surplus equipment, particularly where the military is downsizing. Even large assets can be poorly controlled and easy to sell off corruptly or undervalued.

Secret defence and security budgets are a perennially difficult issue. There are valid reasons for secrecy, but these are open to abuse. Several countries have developed innovative ways of addressing the risks. A broader risk is when there are budgets outside defence that are also used by the military or security forces, but not identified as.

In many countries, defence and security establishments maintain income sources separate to their state revenue streams. These include **military-owned businesses**, either civilian businesses or defence companies which are directly or indirectly owned by the defence establishment. These pose obvious integrity risks.

Misuse of assets also extends to **illegal private enterprises**, with individuals gaining an income from state-owned assets. This may be through the payment of exorbitant fees to cronies for consultancy or other services, or the use of service personnel for private work. It can also include bankrolling of the military by private enterprises in return for military protection of their business interests. The development of a system of patronage between the military and private business is highly detrimental; the more profitable it becomes, the more difficult it is to counter.

PERSONNEL

Personnel and recruitment processes are particularly susceptible to corruption, especially if it is endemic throughout a defence establishment.

Corruption to avoid **conscription**, for example, had already been recognised as a problem in Napoleonic times.[2] Box 1 (below) shows how, in the case of conscription in Russia, personnel management in the modern era can be affected by corruption.

This is just one example of how corrupt practices in the personnel sphere can occur. Other examples are given in Figure 3. They range from having non-existent 'ghost soldiers' on the payroll to extorting favours from subordinates.

The most common effect of corruption in personnel is that it undermines the confidence of staff, making them increasingly prone to participating in or condoning corrupt practices.

For top officials and officers themselves, **leadership behaviour** requires committed and visible engagement by strong role models. They, in turn, need feedback through honest and objective assessment, for example, through third parties and opinion surveys.

Many citizens' experience of corruption is likely to be in the payment of **small bribes** in daily life. These might include payments for speeding up administrative procedures, bribes at checkpoints or payments to avoid predatory police. While this Handbook concentrates on large-scale bribery and corruption, policy-makers should note that anti-corruption plans must

BOX 1: CONSCRIPTION IN RUSSIA

Compulsory military service, also known as conscription or draft, can be a cause of pervasive corruption within the armed forces. Such is the case in Russia. In order to avoid conscription, would-be soldiers pay bribes to the military authorities, medical personnel in charge of assessment and officials in draft boards. Such practices are widespread and publicly acknowledged. In July 2010, Russia's nationalist Liberal Democratic Party, led by Vladimir Zhirinovsky, tabled draft legislation which would allow potential conscripts to pay a sum equivalent to US $32,500 to avoid military service. The resulting funds would be channelled toward the costs of the Ministry of Defence (MoD). This measure, aimed at Russia's military commissions, signifies both the great extent of draft corruption in the country and a clear recognition of this reality.

Serious attempts to deal with this issue have been made in recent years by the Russian government. The length of conscript service was shortened by six months in April 2008 to one year, while the list of exemptions from conscriptions has also been made more restrictive.[3] However, the 2004-7 federal government programme designed to trial a transition to fully professional armed forces was largely ineffective, due to poor design and pervasive corruption which prevents full remuneration from reaching the contracted soldiers.[4]

equally address small bribes and petty corruption. A plan that focuses only on high-value corruption is unlikely to succeed; the general public needs to see benefit at a local level.

Leadership of a reform process requires several other competences: presenting persuasive arguments for why change is necessary (Chapter 4), developing a common direction and energy for change across the top leadership (Chapter 5), building a reform plan (Chapter 6), training more leaders of change across the organisation (Chapter 7) and involving third parties (Chapters 9 and 10).

Significant progress can be made by working on an organisation's values (Chapter 8).

The central issues of integrity in personnel are **payroll, promotions, appointments and rewards**. Examples are shown below:

The **salary chain** is the long link from the national treasury right down to payment to an individual soldier. In many corrupt environments those funds are stolen or diverted en route, so that far less of the due amount finally reaches the soldier. This problem is often extreme in conflict environments, but is also common in peacetime.

More broadly, tackling corruption issues requires attention to the **values** and ethical behaviour of troops, officers and officials. Building **a strong ethical culture** of adherence to policies, rules and guidelines minimises corruption risk. This is particularly relevant in defence and security establishments, which traditionally have a strong custom of compliance to written regulations.

FIGURE 3: **CORRUPTIONS RISKS IN PERSONNEL**

PAYROLL	Extracting percentages from total cash for payroll
	Ghost soldiers on payroll
	Cronies on secret payroll
	Skimming from soldiers' salaries
APPOINTMENTS/RECRUITMENT	Nepotism, favouritism and clientelism: preferred postings and pre-term rank promotion
	Sabotaging personnel/other reforms to preserve power and authority in a given sphere
	Conscription: fees to avoid military service Fees to gain participation in peacekeeping forces
	Favours and fraud during the entry process for respected military educational institutions
	Favours or payment in the selection process for peace support operations or international missions
REWARD AND DISCIPLINE	Extorting favours from subordinates
	Payments to avoid disciplinary process or for reinstatement of position
	Use of disciplinary process to remove threats to power
	Use of reward process to endorse supporters

OPERATIONS

The military's image during operations at home and abroad is vital in promoting and retaining public confidence and respect. Operations are the context in which the general population has most face-to-face daily contact with the military and officials. Therefore their conduct is of paramount importance. This applies both to military personnel and to personnel of **private security companies**.

Where international forces intervene in a conflict country, their approach to corruption once in theatre is critical to the success of their mission. **Disregard of corruption in-country** runs a high risk of being seen as complicity in it. In the past, it was sufficient for military doctrine to regard corruption as a purely civilian/governance issue. But recent experience from Afghanistan to Bosnia to Colombia has shown the need for nations to recognise corruption as a major contextual factor in operations.

Sadly, there are too many cases where intervention or peacekeeping forces have themselves been a source of corrupt behaviour, and **corruption within a mission** has occurred. In many countries the military is used to provide internal security, often in circumstances where the police are unable to operate. Border forces and domestic intelligence and security agencies are also often structured as part of the defence ministry and classed as military forces. This increases the importance of considering counter-corruption in operations as a key element of building integrity in defence.

In a conflict environment, the flow of money into a country represented by local **contracting** and logistics – whether aid money or military support – is an important part of helping to develop that country. With all the problems in a conflict situation, it is easy for corrupt contracts to be awarded, and for non-performance to be tolerated.

PROCUREMENT

Of all defence processes, procurement is usually the highest area of corruption risk, with vulnerabilities at every stage.

These are listed opposite according to the procurement phase: both those from the framework above and a number of others are shown. This Handbook does not attempt a comprehensive review of ways to tackle procurement risks. Instead it devotes four chapters (14-17) to new ideas and reforms for addressing the most serious risks in that area.

FIGURE 2: **CORRUPTION RISKS IN THE PROCUREMENT CYCLE**

1. GOVERNMENT POLICY	Privileged defence relations; defence budgets; external financing; manufacturing government pressure on importers
2. CAPABILITY GAP DEFINITION	Military, political & commercial influence
3. REQUIREMENT/CONTRACT DEFINITION	Inadequate/corrupt military/official expertise, anonymous agents; 'justified opacity', excessive use of national secrecy
4. SUPPORT REQUIREMENTS DEFINITION	Costly & complex
5. OUTLINE PROJECT COSTING	Unreliable data
6. TENDER	Single sourcing; bidder collusion; lack of transparency; offset requirements; inadequate timescales
7. BID ASSESSMENT & CONTRACT AWARD	Evaluation manipulation; favoured bidders; offsets bias outcome; lack of transparency; failure to consider value for money
8. MANUFACTURE & DELIVERY	Variation order; lack of official control; incorrect equipment performance and lack of remedial contract measures
9. IN-SERVICE PHASE	Call-off contracts; lack of expertise; lack of long-term oversight (especially for service contracts)

9. ENLISTING DEFENCE CONTRACTORS

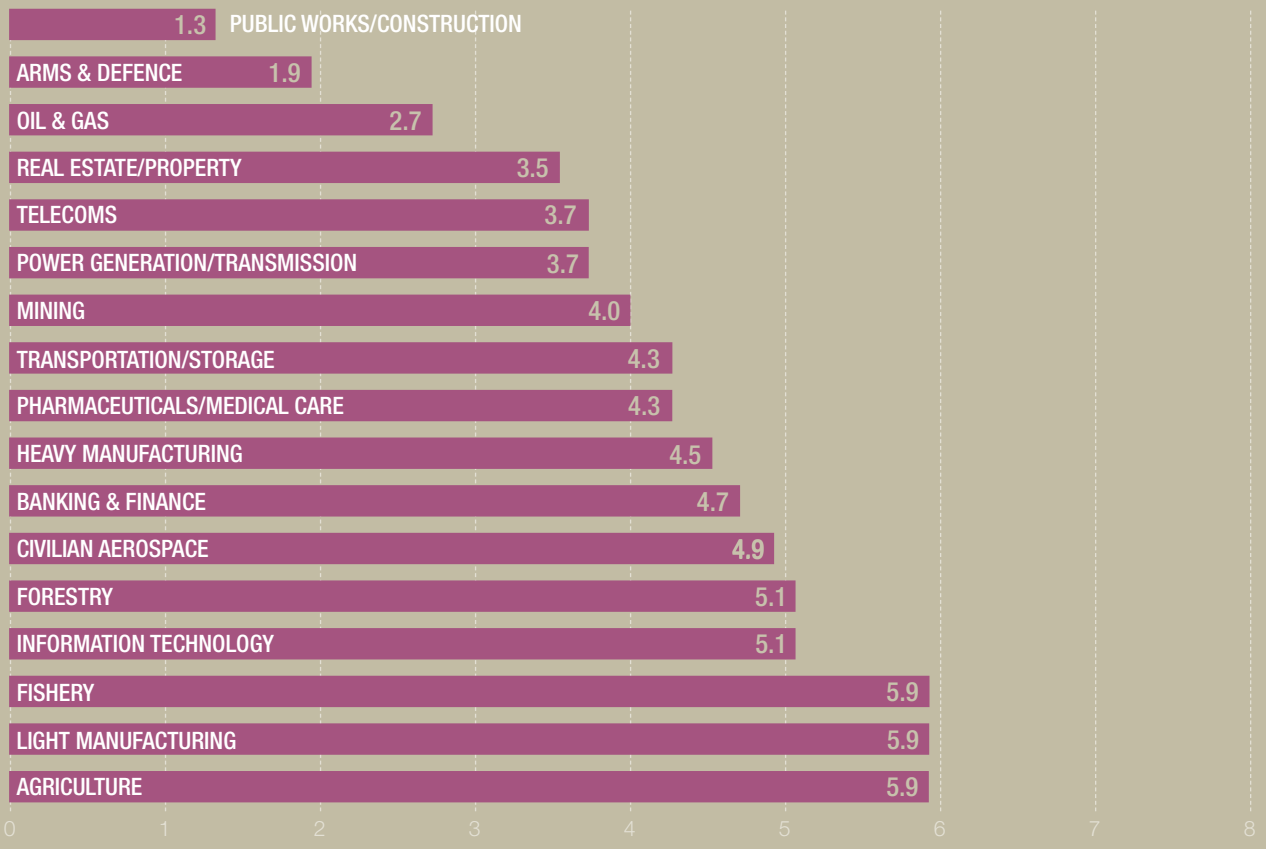
The defence industry has become more willing to engage in counter-corruption reform in the last five years – governments can use this willingness to accelerate their own reforms

This chapter illustrates how governments and companies can feed into each others' efforts to improve defence sector integrity. Governments can do so through supporting a sound business environment and by demanding high standards of integrity from companies they do business with, for example, through prosecution and debarment of corrupt behaviour. Companies can raise standards through better compliance programmes and through collective action, demonstrating that they want to operate in a bribery-free environment.

Several indices suggest the international defence sector is one of the most prone to corruption worldwide. One such index is TI's *Bribe Payer's Index*. In 2002, it ranked Arms and Defence as the industry sector perceived to be the second most corrupt.

In 2006 Control Risks released a survey of international businesses in which a third of defence sector respondents felt they had lost out on a contract in the year before due to bribery by a competitor, and stated this as the number one reason against bidding (Figure 9). As a result, defence companies are avoiding countries which they regard as high-risk, and corruption is given as the foremost reason for such action. This demonstrates that it is in the defence industry's interest to tackle the issue, and offers an opportunity for a defence ministry to collaborate with companies.

FIGURE 8: **TRANSPARENCY INTERNATIONAL'S BRIBE PAYER'S INDEX, 2002**



The scores are average all the responses on a 0 to 10 basis where 0 represents very high levels of corruption, and 10 represents zero perceived level of corruption.

COLLABORATION WITH DEFENCE COMPANIES

Once a defence establishment has the will and the knowledge to tackle corruption, and suitable policies have been put in place, its personnel need to build partnerships in order to control corruption across the entire sector. These relationships are crucial in opening up areas in which corruption traditionally operates discretely.

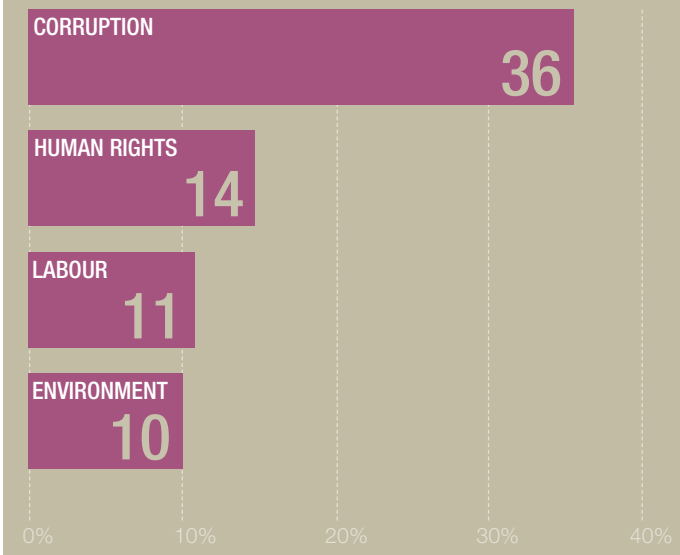
Anti-corruption programmes cannot be effective if designed and implemented in isolation from the contractor community. Active collaboration between governmental defence institutions and the defence industry can help isolate defence sector corruption. Each side can offer mutual cooperation and encouragement in integrity-building measures, and can refuse to do business with an entity perceived as corrupt, whether it is a company or a procuring government agency. One of the biggest concerns for defence establishments is how to attract high-quality suppliers. Clean companies will avoid environments where corruption is endemic, and will have stringent controls to minimise opportunities for corruption originating from their organisations or their agents. This can be a major driver for a ministry's reform.

COLLABORATION AMONG DEFENCE CONTRACTORS

There is much scope for private sector engagement at any stage of the programme to build integrity and reduce corruption risks. Companies can signal clearly to governments that they will not engage in bribery or corrupt practices, and so exert a positive influence over officials and organisations. In sectors such as mineral extraction, water, banking and construction, the private sector's role in raising standards has been crucial. For companies to raise standards within defence establishments, they must also raise standards among themselves. One way the industry can raise standards is by forming an anti-corruption forum and by setting a code of standards.

For example, Europe's defence industry has come together on corruption, coordinated by the AeroSpace and Defence Associations of Europe. Following meetings of major defence firms facilitated by TI, the Associations formed a group to develop a set of Common Industry Standards (CIS) for its member associations and their member firms to follow.

FIGURE 9: **REASONS FOR COMPANIES NOT TO BID IN A TENDER, 2006**
(CONTROL RISKS)



The Common Industry Standards released in 2008 cover:

1. Compliance with laws and regulations
2. Applicability to principal entities, agents and consultants
3. Prohibition of corrupt practices
4. Gifts and hospitality
5. Political donations and contributions
6. Agents, consultants and intermediaries – due diligence, legal provisions, fees, auditing/verification, etc.
7. Integrity programmes
8. Sanctions

Since the CIS were developed in 2007, the French and UK national associations have been engaged in efforts to develop national anti-corruption forums to implement them. There is also a much larger US forum, the 'Defense Industry Initiative' – see box 12 overleaf. Additionally, the UK's Society of British Aerospace Companies and Defence Manufacturer's Association have produced a short handbook containing guidance for implementing the CIS.[22]

Other industry sectors have taken similar actions (Box 11).

Another type of defence industry cooperation is the sharing of good practices. For example, in the United States, following high-profile problems in ethical conduct in several large defence contractors, the Defense Industry Initiative on Business Ethics and Conduct (DII) was established in 1986 to create a common ethos of ethics and integrity across the defence sector in the USA (see box 12). The DII organises an annual best practices forum and provides substantial training and guidance in ethics and business conduct to its members. For more information, see **www.dii.org**.

BOX 11: **EXAMPLES OF SUCCESSFUL COLLECTIVE ACTION ACROSS INDUSTRIES**

OIL, GAS AND MINING

The Extractive Industries Transparency Initiative (EITI) is a multi-stakeholder coalition of civil society, governments, industry, investors and international organisations, which sets a global standard for companies and governments to disclose payments and receipts in the extractive industries. Established in 2002, the EITI arose from the realisation of the 'natural resource curse', i.e. the paradox that countries rich in natural resources also tended to have high levels of poverty, corruption and conflict, fuelled by competition for riches. Many of these problems are the result of poor governance. The EITI aims to strengthen governance in participating countries by improving transparency and accountability in extractive industries. Both governments and natural resource companies are actively engaged.

For more information, see ***www.eiti.org***

SANCTIONS ON COMPANIES

Ultimately, such efforts aimed at building confidence between the public and private sectors require recourse to sanction should anti-corruption laws and regulations be breached. Defence establishments owe it to companies who comply with ethical norms to take action against those who fail to uphold the same standards. Efforts by companies to gain advantage through corrupt means should be given a high priority in terms of prosecutions through the criminal justice system. The defence establishment can reinforce can reinforce incentives to refute corruption by instituting debarment procedures for companies which are found guilty of corrupt practices, whether at trial or by plea. Box 13 describes the use of debarment within the context of wider regulation of defence companies in the USA.

GOVERNMENTS

Those at the top of defence and security establishments have an important role in bringing both national and international contractors into the reform plan. This can include some or all of the following:

- meeting with contractors as a body and encouraging them to develop an industry initiative
- meeting regularly with industry bodies to discuss progress
- emphasising to international companies that they have obligations under the CIS and that the government expects strict adherence to these standards
- speaking frequently at industry and other events on the importance of high standards of behaviour by defence contractors
- Carrying out a detailed review of where governments need to crack down on their own practices so as to better enable industry reform.

BOX 12: DEFENSE INDUSTRY INITIATIVE ON BUSINESS ETHICS AND CONDUCT

In the United States, following high-profile problems in ethical conduct in several large defence contractors, the Defense Industry Initiative on Business Ethics and Conduct (DII) was established in 1986 to create a common ethos of ethics and integrity across the defence sector. The DII supports the US federal legal framework by establishing six principles around which to organise companies and associations. The current principles are as follows:

1. Each Signatory shall have and adhere to a written code of business conduct. The code establishes the high ethical values expected for all within the signatory's organisation.
2. Each Signatory shall train all within the organisation in their personal responsibilities under the code.
3. Signatories shall encourage internal reporting of violations of the code, with the promise of no retaliation for such reporting.
4. Signatories have the obligation to self-govern by implementing controls to monitor compliance with federal procurement laws and by adopting procedures for voluntary disclosure of violations of federal procurement laws to appropriate authorities.
5. Each Signatory shall have responsibility to one another to share its best practices in implementing the DII principles; each Signatory shall participate in an annual Best Practices Forum.
6. Each signatory shall be accountable to the public.

For more information, see ***www.dii.org***

BOX 13: US AIR FORCE DEBARMENT PROCEDURE

The US Air Force has had much experience in dealing with defence contractors and has developed a structure whereby federal law can be used to punish and deter corruption, and to encourage compliance and ethical conduct.

US agencies have suspension and debarment officials, whose role is to debar or suspend contractors who contravene accepted rules of conduct. They update a public website of all debarred companies, which contracting officials are required to check prior to awarding new contracts. A decision to debar or suspend by an agency makes the person or organisation ineligible for new contracts by all agencies throughout the US federal government.

Companies and individuals become eligible for debarment if they engage in any crime that relates to business honesty, including fraud and corruption. The possibility of debarment is a substantial disincentive to participate in such activities. Debarment can also be employed should a party perform poorly on a contract, as well as for any other serious cause, at the discretion of the debarring official.

The US Air Force debarring official also oversees the US Government's investigation and prosecution of Air Force contractors suspected of committing procurement fraud. The legal basis for many of these actions is the False Claims Act (31 U.S.C. §3729-3733). This act provides incentives for people not affiliated with the government to file actions against federal contractors, by allowing them a share of the damages recovered. The US also requires the disclosure of misconduct by industry and imposes debarment as a sanction for failure to do so.

Incentives for strong ethical conduct by American firms are provided in the country's sentencing guidelines, which allow the strength of a company's compliance programme to be taken into account during sentencing for firms convicted of misconduct. Punishment for wrong-doing is further proportional to the extent the company has acted to prevent misconduct. The US Air Force also tends to favour contracting with companies which have good ethical reputations.[23]