Key Messages

Key characteristics of A&D industry makes it vulnerable to economic crimes

Globally, economic crime in the Aerospace and Defence sector is one of least reported in comparison to other sectors

Government has continuously focussed on making procurement transparent, but challenges remain

Onus on Companies to adopt zero tolerance policies and anti-fraud programmes and controls
Indian A&D sector – An overview
India’s defence capital budget has grown to INR 86k cr and we are the largest importer of armaments

Key Insights:

- The Indian government typically spends around 2.0% of GDP on defence related expenditure (~35% is capital outlay)
- Defence budget for 2018-19 has seen a marginal increase of 5.8% over the last year and accounts for 10.74% of the total allocation
- Capital expenditure has been increases by ~8.7% over the last year's revised estimates, that significantly exceeds that of revenue
- New defence production policy and two defence industrial production corridors were announced
- Allocation of INR 9,734 crores towards Research and Development (R&D) is an y-o-y increase of 29%
- INR 130 crores allocated for assistance in prototype development under the make procedure for Indian Army projects

Source: PwC Research, Union Budget 2017
Indian Defence industry supply side segmentation

DEFENCE PUBLIC SECTOR UNDERTAKINGS (DPSUs) & ORDNANCE FACTORIES BOARD (OFBs)
• Grown tremendously through protection
• Responsible for strategic requirements of armed forces
• Have developed and acquired new technologies
• Large backlog of orders
• Increased outsourcing from DPSUs & OFBs

IT/ENGINEERING COMPANIES
• Active in the field of aerospace engineering and design
• Big players have separate aerospace vertical: Wipro, Infosys, HCL
• Offer complete solutions ranging from Product Design and Development, Embedded Systems and Avionics to Product Lifecycle Management services
• Have capability to undertake, sustain and verify activities in several aircraft subsystems

OEMs & LARGE/MID SIZED INDIAN COMPANIES
• OEMs and Tier-1s looking towards lower cost destinations - India in an attractive destination for all majors
• Aggressive capability building by big houses like Tata, L&T, M&M, Kalyani; Reliance new entrant
• Mid sized and small players like Dynamatic, Aequus, Technologies, Maini Group, TAAL, Samtel, India Forge, Axis Aerospace building capabilities/diversifying products to cater to a larger value chain

MSMEs
• Auto ancillary companies looking to enter
• Key pain points – access and cost of capital, building capability, accreditation
• Special focus by the government on 5,000 companies operating in niche areas, supplying primarily to DPSUs
Government is working to build a facilitative environment in the A&D sector...

**Strategic Partner (SP) model**
- SP policy promulgated on 31 May 17.
- Government will shortlist Indian companies to be SPs to associate with OEMs
- Eligibility criteria includes, interalia, cap of 49% on FDI & ownership and control with resident Indian citizens
- One private sector SP will be chosen for each of the 04 platforms - fighter jets, helicopters, armoured vehicles and submarines
- MoD will also select the foreign OEMs separately and simultaneously
- Will involve transfer of the requisite scope, range and depth of technology

**Abolition of Foreign Investment Promotion Board (FIPB) and FDI policy**
- Union Cabinet approved abolition of FIPB on 24 May’17
- Processing of applications for FDI will now be handled by Department of Defence Production (DDP) for defence equipment and by MHA for small arms in consultation with Department of Industrial Policy & Promotion (DIPP)
- DIPP issued Standard Operating Procedure (SOP) for processing of applications
- Liberalization of FDI cap - Foreign investment up to 49% will be under automatic route
- Proposals for FDI beyond 49% will be considered by MoD /MHA on a case-to-case basis

**Impact on A&D sector**
- Will encourage investments by assuring selected domestic companies of future orders
- Will give impetus to building a domestic supply chain
- OEMs allowed to interact with all shortlisted SPs

**Changes in FDI policy bring defence at par with other sectors by allowing portfolio investments up to the sectoral caps**
- Delays in MoD & MHA might vitiate achieving the objective
Section 1 – Overview of the Indian A&D sector

...to build a domestic industrial base and promote indigenisation...

**DPP 2016**

DPP 2016 released with following changes
- Introduction of a new category of acquisition ‘Buy Indian (IDDM)’
- Definition of acquisition categories elaborated and decision flow-charts provided for the acquisition process
- Simplified ‘Make’ procedure with focus on MSMEs
- Weightage for enhanced performance features
- Increase in Indigenous content (IC)
- Reduction in procedural delays and ease of doing business
- Consolidated offset policy (amendments to DPP 2013 incorporated)
  - Offset threshold increased
  - Standard operating procedures laid out for change of IOP/ products
  - Exchange rate variation benefit to the private sector
  - ‘Services’ partially reintroduced as an eligible offset avenue
  - Reduced requirement of indigenous content to 30% in ‘Buy (global)’ bids where Indian firm/JV is bidding

**Recent developments**

- OEMs will need to re-think India strategy- increase collaboration
- Encourages Indian companies to begin design & development within the country
- OEMs need to address the issue of life cycle support costs
- Level playing field for domestic firms with DPSUs
- Ease in discharging offset obligations

**Acquisition categories**
- Buy (Indian – IDDM)
- Buy (Indian)
- Buy and Make (Indian)
- Make (Indian)
- Buy and Make
- Buy (Global)
...to achieve self reliance in defence

**Foreign Trade Policy**

- Revised list of Special Chemicals, Organisms, Materials, Equipment and Technologies (SCOMET), which either prohibits or permits under a license the export of dual use items
- Wassenaar Arrangement’s munitions list and the dual-use list items have been added in Category 6 of SCOMET list
- Changes reflect India’s efforts to gain membership to international export regimes - Nuclear Suppliers Group, Australia Group, and Wassenaar Arrangement

**Industrial Licensing**

- Prior to July 2016, an Industrial License (IL) was required to manufacture defence items under the Industries (Development and Regulation) Act, 1951 and was issued by DIPP
- In July 2016, MHA notified Arms Rules, 2016, which provided that MHA will issue the license to manufacture items configured for military use
- Vide Notification S.O. 1636 (E) dated 19.05.2017, MHA has again delegated powers and functions to grant manufacturing license for defence items to Secretary, DIPP

**Impact**

- Indian export controls now in line with the Wassenaar Arrangement
- Will facilitate Indian companies entry into global supply chains
- Will develop an export market for Indian equipment

- Positive decision. applications for grant of manufacturing licenses in defence sector, will now be processed faster
- However, Arms Act and Arms Rules need to be aligned with FDI and IL policies
Corporate fraud – an overview
**Introduction**

**Fraud is defined as:**

- Act, omission, concealment of fact or abuse of position by any person;
- With an intention to deceive or injure the interests of the Company, its shareholders, Creditors or any other person

**Corporate Fraud**

- Corporate fraud consists of activities undertaken by an individual or company that are done in a dishonest or illegal manner, and are designed to give an advantage to the perpetrating individual or company.
- Corporate fraud schemes go beyond the scope of an employee’s stated position, and are marked by their complexity and economic impact on the business, other employees and outside parties.
Regulatory legislations covering fraud

- Indian Penal Code 1860.
- Information Technology Act 2008.
- Prohibition of Insider Trading.
Fraud repercussions: individual punishment...(i)

• As Per Section 447 of Companies Act 2013, imprisonment for a **term not less than 6 months and up to 10 years and fine**, which shall **not be less than the amount involved in the fraud** and may extend to **thrice of such amount**.

• If the fraud involves public interest, the minimum imprisonment to be awarded shall be **3 years**.

• As per Prevention of Money laundering Act 2012 if any person convicted offence in this act, there can be punishment of imprisonment **up to 3-7 years with fine up to 5 lakh rupees**.

• As per Indian Penal Code 1860, punishment of offences, every person shall be liable to punishment under this Code and not otherwise for every act or omission contrary to the provisions thereof, of which he shall be guilty within India.

• As per Section 66F (Acts of cyber terrorism) of Information Technology Act 2002, If a person denies access to authorized personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyber terrorism and **he is liable for Imprisonment up to life**.
Fraud repercussions: Impact on reputation ...(ii)

- **Blacklisting**

- **Financial loss**
  Fines assessed for misleading investors, civil suits to recoup investor and creditor losses and the unwillingness of companies to extend credit to the business in the future all add up to a severe financial loss for the company.

- **Loss in external confidence**
  Once a fraud has been uncovered, the company faces an ongoing problem of public trust in the organization

- **Negative impact on company morale**
  The effect of fraud on a company's culture and morale can be shattering.

- **Reputational loss**
Frauds in the A&D industry
**Asset misappropriation, consumer fraud and cybercrime were the most frequently reported frauds across industries**

<table>
<thead>
<tr>
<th>Industry</th>
<th>Asset misappropriation</th>
<th>Business misconduct</th>
<th>Cybercrime</th>
<th>Bribery and Corruption</th>
<th>Consumer fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer</td>
<td>48%</td>
<td>31%</td>
<td>30%</td>
<td>28%</td>
<td>25%</td>
</tr>
<tr>
<td>Professional Services</td>
<td>46%</td>
<td>32%</td>
<td>30%</td>
<td>26%</td>
<td>26%</td>
</tr>
<tr>
<td>Financial Services</td>
<td>56%</td>
<td>41%</td>
<td>41%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology</td>
<td>43%</td>
<td>39%</td>
<td>31%</td>
<td>26%</td>
<td>23%</td>
</tr>
<tr>
<td>Industrial Products</td>
<td>48%</td>
<td>29%</td>
<td>29%</td>
<td>26%</td>
<td>26%</td>
</tr>
</tbody>
</table>

**Key insights**

- Fighting fraud has become a core business issue
- 49% of organisations globally said they’ve been a victim of fraud and economic crime – up from 36%
- 52% of all frauds are perpetrated by people inside the organisation
- 31% of respondents that suffered fraud indicated they experienced cybercrime
- Aerospace and defence companies have unique risks due to the large scale and value of contracts, fierce competition and the complexity of the regulatory and compliance environment.

*Source: PwC's Global Economic Crime and Fraud Survey 2018*
**Strong correlation between economic development and fraud**

- Our survey reveals some interesting nuances about global approaches to fraud, which could offer valuable pointers for nation states as they continue on the path of economic development.

- In developing countries, 58% of companies involved in money movement (and/or any of the following lines of business: financial institutions, mutual funds, money service businesses, broker dealers, insurance companies, or dealers in precious metals, stones or jewels) told us they had experienced anti-money laundering (AML) regulatory enforcement or inspection in the last two years. The equivalent figure in developed countries was just 48%.

- In developing countries, 15% of companies told us they expect to significantly increase funding for anti-fraud investments in the next 24 months. The equivalent figure in developed countries was just 9%.

- In developing countries, respondents told us that economic crime is more often committed by internal actors (59%). The equivalent figure in developed countries was just 39%.

*Source: PwC’s Global Economic Crime and Fraud Survey 2018*
**Defence sector does not have perfect competition:** Inherent distortions make it susceptible to economic crime

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highly regulated</td>
<td>Large number of sanctions/approvals required</td>
</tr>
<tr>
<td>• Manufacture</td>
<td>Raises entry barriers – restricts number of players</td>
</tr>
<tr>
<td>• ToT</td>
<td></td>
</tr>
<tr>
<td>• Sales – domestic &amp; export</td>
<td></td>
</tr>
<tr>
<td>Information asymmetry</td>
<td>Suppliers – Specifications, true price</td>
</tr>
<tr>
<td></td>
<td>Buyers – Long term demand</td>
</tr>
<tr>
<td>Monopsony- single buyer and L1 basis</td>
<td>Win-lose situation</td>
</tr>
<tr>
<td>Close knit buyer group</td>
<td>Fewer people to influence, scope for middlemen</td>
</tr>
<tr>
<td>Cutting edge technology – complex specs</td>
<td>Difficult to comprehend</td>
</tr>
<tr>
<td>Shrinking budgets</td>
<td>Intense competition</td>
</tr>
<tr>
<td>Limited suppliers and frequent complaints</td>
<td>Limited buyer options</td>
</tr>
<tr>
<td>High transaction costs</td>
<td>Greater risks</td>
</tr>
<tr>
<td>Large deal size</td>
<td>Increases financial stake for suppliers</td>
</tr>
<tr>
<td>Grey market – very lucrative</td>
<td>Increased temptation to violate laws</td>
</tr>
<tr>
<td>Lack of transparency in procurement</td>
<td>Greater scope</td>
</tr>
<tr>
<td>Conviction difficult</td>
<td>Encourage agents</td>
</tr>
<tr>
<td>Very high capex in R&amp;D and Production</td>
<td>Very high stakes for suppliers</td>
</tr>
</tbody>
</table>

**Economic crimes**

- **Unauthorised receipts and expenditures**
  - Bribery – Government officials; Commercial vendors and suppliers
  - TINA violations
  - Fabrication of records
  - Improper cost allocations

- **Speed Money**: US allows (after disclosure)

- **Financial statement manipulation**
  - Improper revenue/expenditure booking
  - Fictitious transactions

- **Misappropriation of assets**
  - Theft of intellectual property
  - Espionage
  - Cyber Crime

- **Money Laundering**

- **Smuggling**

- **Disclosure fraud**

- **Aiding and abetting**

- **Fraud by senior management**
India has had its fair share of controversial deals in defence

<table>
<thead>
<tr>
<th>Acquisition Programme</th>
<th>Year</th>
<th>Deal amount</th>
<th>Alleged Kickback amount</th>
<th>Status</th>
<th>Blacklisted companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jeeps for Army</td>
<td>1948</td>
<td>INR 80 L</td>
<td>Not available</td>
<td>Case closed</td>
<td></td>
</tr>
<tr>
<td>HDW submarines</td>
<td>1981</td>
<td>$ 330 mn</td>
<td>$ 23 mn</td>
<td>Case closed</td>
<td></td>
</tr>
<tr>
<td>Bofors 155 mm howitzers</td>
<td>1986</td>
<td>$ 285 mn</td>
<td>$ 12 mn</td>
<td>Case closed</td>
<td></td>
</tr>
<tr>
<td>Denel rifles</td>
<td>1999</td>
<td>$ 386 mn</td>
<td>$ 49.2 mn</td>
<td>Case closed</td>
<td>Denel</td>
</tr>
<tr>
<td>Barak missile</td>
<td>2000</td>
<td>INR 1150 crores</td>
<td>INR 175 crores</td>
<td>Trial ongoing</td>
<td></td>
</tr>
<tr>
<td>Scorpene submarine</td>
<td>2005</td>
<td>INR 18,798 crores</td>
<td>INR 500 crores</td>
<td>Trial ongoing</td>
<td></td>
</tr>
<tr>
<td>Ordnance Factories Board</td>
<td>2009</td>
<td>INR 10,000 crore</td>
<td>INR 600 crore</td>
<td>Conviction</td>
<td>IMI; Rheinmetall Air Defence; Corporation Defence</td>
</tr>
<tr>
<td>AgustaWestland VVIP helicopters</td>
<td>2010</td>
<td>INR 3600 crores</td>
<td>INR 362 crores</td>
<td>Investigation ongoing</td>
<td>Finmeccanica; AgustaWestland</td>
</tr>
<tr>
<td>Tatra –BEML</td>
<td>2012</td>
<td>INR 3000 crores</td>
<td>Not available</td>
<td>Investigation ongoing</td>
<td></td>
</tr>
</tbody>
</table>

Source: PwC research Media Reports, International Journal, Article by Surojit Chakraborty
India’s blacklisting policy

Policy

• Blacklisting has been a hurdle in procurements in the past and led to long delays

• MoD, in Nov 2016, issued guidelines for penalties in business dealings with entities

• New policy provides for levy of financial penalties and/or suspension/banning of business dealings with entities, seeking to enter into contract with/having entered into a contract for the procurement of goods and services by the MoD

• Aimed to move from a blanket approach to a process driven approach

• Now, a company can be blacklisted for a maximum of 10 years

• Provision to do business with a blacklisted firm for support of critical spares and maintenance in view of national security

PwC comments

• Crime is committed by an individual and not by a body corporate

• Individuals must be punished while companies may be fined

• National Interest for defence procurements should prevail

• Blacklisting the firms limit the options for defence procurements
## Onus on companies to take preventive measures

### CEOs AND BOARDS OF DIRECTORS
- Ensuring a robust ethics and anti-corruption programme. Encouraging periodic independent review
- Disclosing the programme fully on your company’s website
- Speak up strongly against corruption inside the company and in public fora
- Conduct a fraud risk assessment

### INVESTOR ENGAGEMENT TEAMS, PORTFOLIO MANAGERS, AND ANALYSTS
- Explaining the ethics and anti-corruption programme
- Showing the results of independent reviews

### PROCUREMENT CHIEFS IN ARMS IMPORTING COUNTRIES
- Formulating effective ethics and anti-corruption programmes and making them public
- Explaining Ministry of Defence (MoD) regulations on the subject to all concerned
- Standardize processes for incident investigation and remediation

### GOVERNMENT OFFICIALS RESPONSIBLE FOR OFFSETS
- Encouraging bidding companies to publish their detailed offset obligations
- Encouraging publishing of annual performance assessments of their offset obligations

### ARMS EXPORTING GOVERNMENTS
- Formulating robust ethics and anti-corruption programs
- Export Controls
Measures to develop and implement an effective antifraud program

- Establish a base line
- Conduct a fraud risk assessment
- Evaluate design and validate operating effectiveness
- Address residual financial reporting fraud risks
- Standardize processes for incident investigation and remediation
- Harness the protective power of technology
- Invest in people, not just machines
Antifraud Program and controls

**STEP 1:** Risk Identification and assessment
- Determine areas of operations at risk
- Identify areas of company where schemes most likely to occur
- Identify potential fraud schemes
- Identify red flags and indications associated with schemes
- Build periodic monitoring and reporting to search for indicators
- Conduct further inquiry if red flag is detected or suspected

**STEP 2:** Preventive measures

**STEP 3:** Fraud Discovery/Expectation

**STEP 4:** Investigation

**STEP 5:** Action

**ZERO TOLERANCE**
Recommendations
Recommendations for reducing economic crime and fraud in A&D sector in India

- Create specialist procurement agency – multi-disciplinary specialists
- Encouragement/protection to honest officers – abolish Section 13(1)(d) of the PCA, 1988
- Improve and speed up prosecution
- Institutionalize out of court settlements
- Focus on prosecuting individuals - Blacklisting of entire group company counter productive and should be resorted to as the last resort and for grave and serious offenses
- Conducting due diligence of third party before engaging – work with reliable partners
- Stricter corporate governance: zero tolerance policies; mandatory implementation of anti-fraud programmes and controls
- Whistleblower protection
Thank you

Dhiraj Mathur (IAS, retd.)
Partner, Leader, A&D Practice
PricewaterhouseCoopers Pvt. Ltd.

Email: dhiraj.mathur@in.pwc.com