Homeland Security 2017

Roadmap for Public Procurement of Smart Internal Security in India



1927-2017 FICCI @90

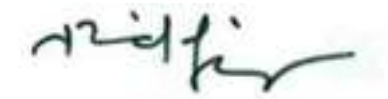
EY Building a better working world

Foreword



Dr. A. Didar Singh

Secretary General
FICCI



India is witnessing increasing threats to its internal security due to various internal and external factors. Internal security covers several dimensions of national interest and identifies with ensuring the internal environment of the country from turbulent activities that can potentially result in disorderly situation, loss of civilians' lives and destruction of the public or private assets. The expansion in smart internal security initiatives has been necessitated by the changing nature of crimes and criminals, the rapidly shifting technological landscape and the changing expectations of the citizens from the internal security agencies. To ensure that procurement in smart internal security projects is conducted in an efficient and transparent manner, a comprehensive set of guidelines, principles and policies should be available. Additionally, the technological advancements should be utilized in changing the existing public procurement model in smart internal security.

The implementation of smart internal security initiatives is expected to increase further in coming times. Accordingly, the human and budgetary assets spent in the procurement and implementation of these initiatives is also expanding and is expected to form a significant part of the spending of most internal security agencies. However, to address the requirements of smart internal security projects, the present public procurement framework adopted for generic public sector projects may not be adequate. It is therefore essential to examine the procurement framework for smart internal security projects and suggest ways to circumvent the challenges faced in the procurement and execution.

This paper proposed a four pronged framework to analyze and assess the public procurement framework for smart internal security projects on certain parameters and explores its various elements.

I am confident that this report will be of considerable value to all stakeholders in understanding the key parameters and suggest the way forward to transform the smart internal security procurement system in India.



Rahul Rishi

Partner and
Digital Government Leader
Ernst & Young LLP



We take pride in the fact that our knowledge papers on internal security, published in partnership with FICCI over the past 6 years, have been very well received by the public and private sector alike. We would like to extend this initiative and present this paper titled "Roadmap for public procurement of smart internal security in India" to explore the disruptive influence of digital technologies on the internal security sector, understand the intricacies and challenges in the procurement of "smart internal security" and sensitize the stakeholders on the need to transform it.

Douglas Engelbart, a revolutionary inventor, has said, "The digital revolution is far more significant than the invention of writing or even of printing." This digital revolution has disrupted every sector in the working world, and the internal security sector finds itself right in the middle of this disruption. Across the globe, digital technologies are being utilized to disrupt the conventional processes, methods and standards of internal security management. To counter the rapidly evolving crime scenario in India, the country's internal security agencies are driven to become smarter, providing a great growth impetus to smart internal security procurement.

However, the rapid growth in the procurement of smart internal security brings in several challenges for the procurement departments, which have to marry the traditional public procurement frameworks with the rapidly evolving and novel procurement models of smart internal security projects.

In this paper, we have analyzed the current state of smart internal security procurement, identified the key challenges faced and enumerated some of the leading practices adopted in India and across the globe. Based on this study, the paper strives to provide a joint roadmap for the Government, internal security agencies and private sector to transform the current procurement framework in tune with the needs of rapid advancements in smart internal security.

We sincerely hope you find this knowledge paper insightful and useful to understand the growth drivers and opportunities for improvement in the procurement framework of smart internal security. We would like to thank FICCI for giving us the opportunity to present some insights on internal security through this knowledge paper at the Homeland Security 2017 conference held in New Delhi.

Contents



01

Executive summary

page - 6



02

Introduction

page - 10

2.1 What is smart internal security
page - 10

2.2 Need for smart internal security initiatives
page - 11

2.3 Need to examine smart internal security procurement
page - 12



03

Assessment of smart internal security procurement in India

page - 16

3.1 Policy and regulations
page - 16

3.2 Processes
page - 19

3.3 Technology
page - 23

3.4 People
page - 25



04

The road ahead

page - 30

01

Executive summary

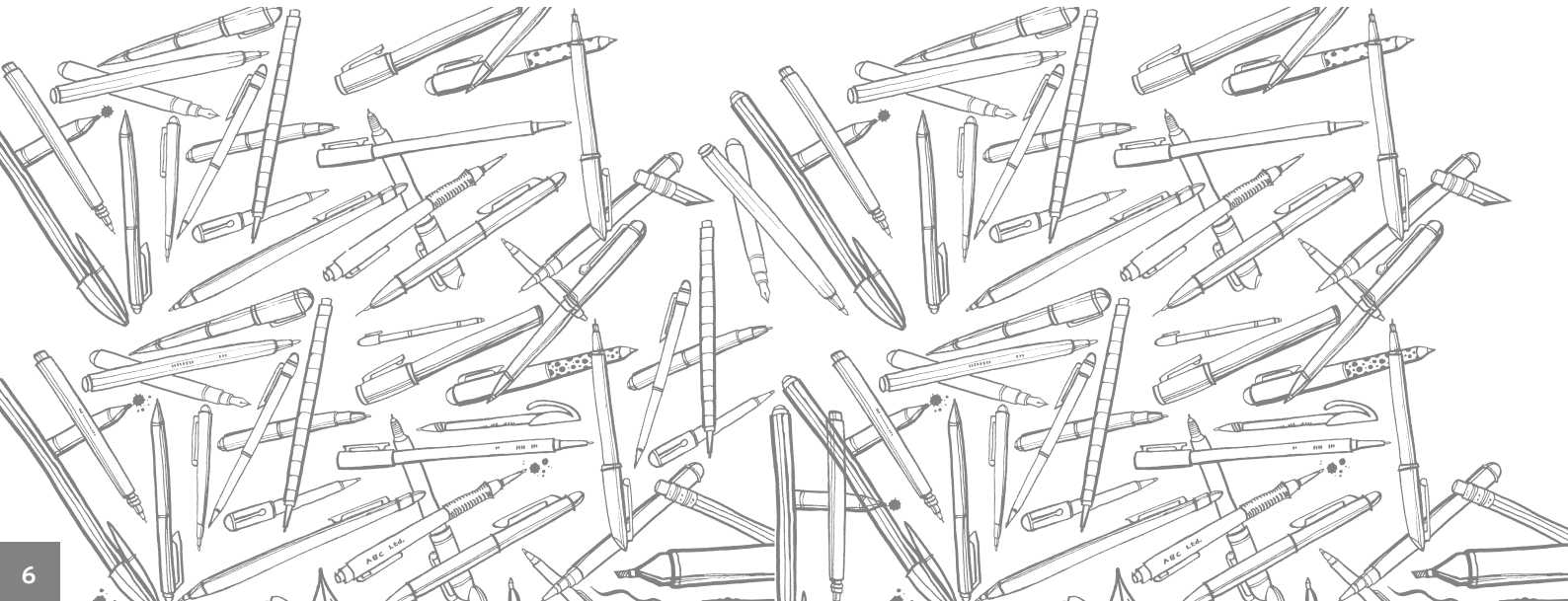
"The fourth generation warfare is more about being prepared to tackle internal security challenges by the police than facing external aggression by the Army"- Ajit Doval, National Security Adviser to the Prime Minister of India.

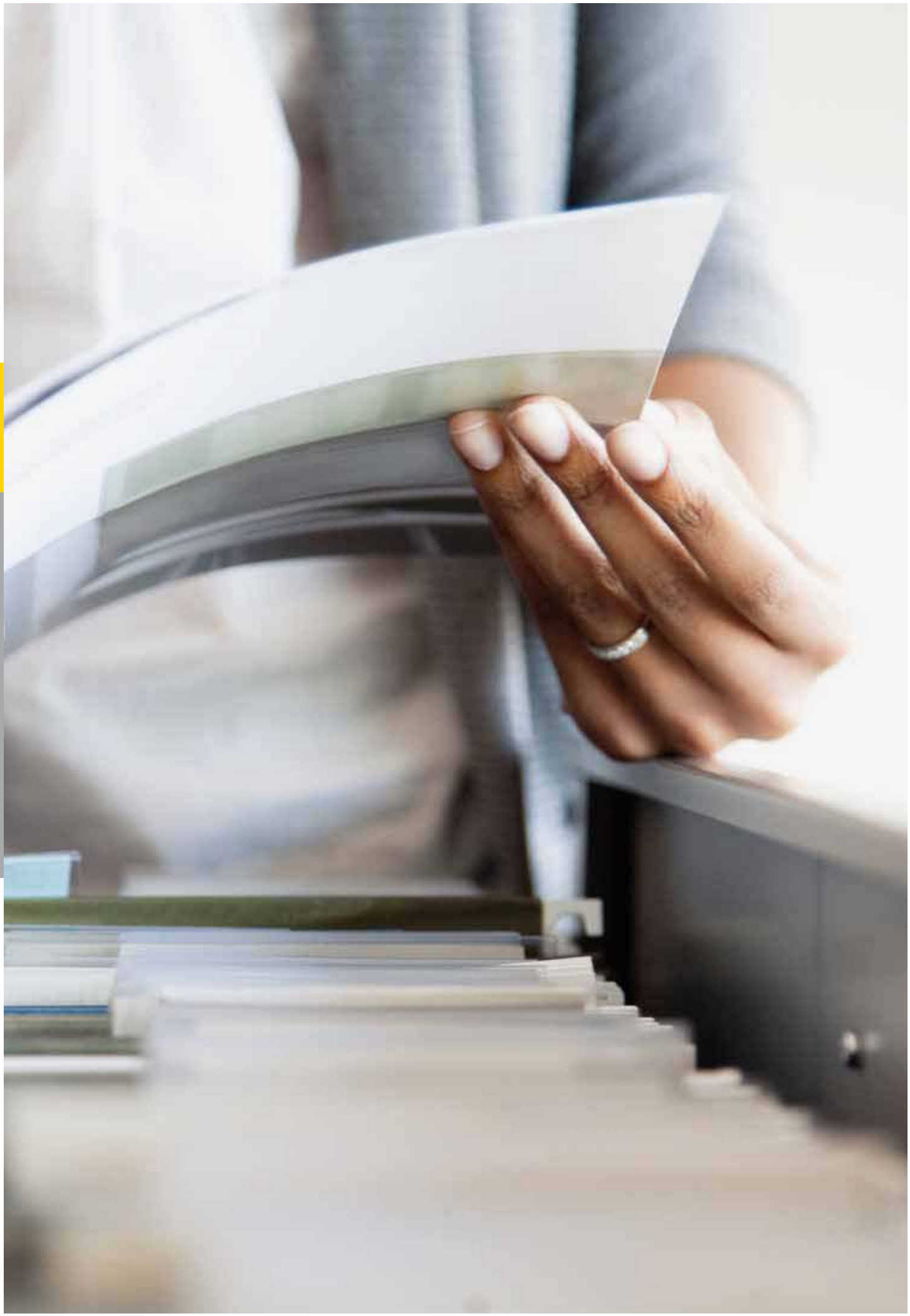
The crime scenario in India is undergoing rapid changes. In the past two decades, newer and more complex crimes such as cybercrimes, information fraud, organized crime, financial frauds and terrorist financing have risen at a much higher rate than the increase in average crime rate. Furthermore, higher standards of living of citizens, an active press and widespread use of social media have played an active role in raising the service level expectations of citizens from internal security agencies. This has underscored the need for enhancing smart internal security, which covers the use of information, communication and digital technologies by internal security forces. There is increasing pressure on the Government and the internal security agencies to rapidly implement smart internal security projects and instantly demonstrate their benefits. However, this has put tremendous pressure on the procurement framework and process for these projects.

This paper proposes a four-pronged framework to analyze and assess the public procurement framework for smart internal security projects on parameters such as policy and regulations, processes, technology and people. The paper explores the different elements of the public procurement framework on these four parameters. It identifies the reforms and initiatives taken by internal security agencies within India and draws parallels from developments in other countries.

Based on this assessment, the paper proposes a roadmap for sustainable improvement in the smart internal security procurement framework. The key recommendations are as follows:

- Centralized initiative for creating procurement standards, guidelines, discussion forums and repository of leading practices for smart internal security projects
- Long-term procurement planning by each internal security agency for their internal security projects in a standard format to be instituted at the Center
- Active engagement with the private sector to ensure that the smart internal security technologies and procurement models are customized to the Indian scenario
- Capacity building of procurement officers to enable them to marry the traditional models of public procurement with the emerging procurement models in smart internal security









02 Introduction

2.1 What is smart internal security
page - 10

2.2 Need for smart internal security initiatives
page - 11

2.3 Need to examine smart internal security procurement
page - 12

2 Introduction

Threats to India's internal security are increasing due to various internal and external factors. Incidents and threats such as the 26/11 Mumbai terror attacks, Kashmir insurgency, cross-border terrorism, increasing Maoist insurgency, cybercrimes, cultural conflicts and other real and alleged threats have reiterated the importance of protecting India's citizens from the potential maelstrom. In light of this situation, the Central and State Governments should consider modernization and upgrade of India's internal security sector as a matter of priority.

Internal security covers several dimensions of national interest and relates to protecting the internal environment of the country from turbulent activities that can potentially result in a disorderly situation, loss of civilians' lives and destruction of the public or private assets. Currently, internal security in India is handled by a host of government bodies with intricate functional and reporting structures. India's internal security agencies primarily comprise the state and UT police forces, central armed police forces, the intelligence and investigative agencies, and courts. The figure below provides an overview of the various internal security agencies in India.

This chapter introduces the concept of smart internal security, underlines the need for implementing smart internal security initiatives and explores the specific nature of smart internal security procurement due to which it needs to be seen in a different light than the other procurement activities undertaken by the Government.

Ministry of Home Affairs, Government of India

Central Armed Police Forces	Investigation & Intelligence	Naxal Management
CRPF	NATGRID	Bureau of Immigration
CISF	NCB	BPR&D
BSF	IB	Border Management
Assam Rifles	CBI	NCRB
SSB	GEQD	Disaster Management
NSG	NIA	
ITBP	CFSL	

State / UT Government

- State / UT Police
- Home Guard
- Civil Defense
- Prisons

Department of Justice, Government of India

- Courts

Figure 1: Internal security agencies under MHA

2.1 What is smart internal security

In the last two decades, India has undergone a dramatic shift in adoption of rapidly changing technologies including latest digital technologies, internet, mobile, social media, etc. While the adoption of new technologies has improved the standard of living of the citizens; it has also provided a sophisticated and innovative medium of committing crimes to the criminals. The advent of latest technologies has given rise to complex and globalised criminal networks, increasing cyber-crime, and the use of digital platforms as a distribution channel.

Realising the need for transformation of law enforcement forces, Hon'ble Prime Minister Shri Narendra Modi emphasised on transforming India's police into a 'SMART' police force. He defined 'SMART policing' as a set of five underlying principles – Strict and Sensitive, Modern and Mobile, Alert and Accountable, Reliable and Responsive, and Techno-savvy and Trained. For the purpose of this paper, smart internal security has been defined as the use of

information, communication and digital technologies by internal security agencies to improve their law enforcement activities. The ambit of smart internal security projects extends across the entire spectrum of internal security covering intelligence, policing, investigation, justice delivery, prison management etc. Some of the notable smart internal security initiatives currently implemented or being undertaken in India are as follows:

- Intelligence management: Open source intelligence (OSINT) projects of agencies such as BSF, NATGRID, state police forces
- Policing and crime management: Crime and Criminal Tracking Network System (CCTNS), Citizen-Police connect apps and analytics systems being implemented by state police forces
- Investigation: Intelligent case management system of CBI linked with forensics and analytics tools
- Criminal justice: e-Courts, Integrated Criminal Justice System (ICJS)
- Prisons management: e-Prisons
- Emergency response: States' centralised emergency response systems (e.g. Dial 100 and Dial 112)
- Safe city initiatives: City surveillance (fixed and aerial), intelligent traffic management, command and control centres

2.2 Need for smart internal security initiatives

The increase in smart internal security initiatives has been necessitated by the changing nature of crimes and criminals, the rapidly shifting technological landscape and the changing expectations of the citizens from the internal security agencies. Some of the key trends are explored below.

- **Emergence of new types and modes of crimes**

  It has been noticed that criminals are becoming early adopters of latest technologies and platforms. James Comey, former Director of FBI, stated, "An element of virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated."

  As per NCRB data, while crime in India increased steadily at a compounded annual growth rate (CAGR) of 6.6% from 2012 to 2015, the corresponding CAGR of cybercrime was 39.3%[1]. Similar trends can be seen for newer types and modes of crimes, especially the ones that involve digital technologies. Crimes such as terrorism, naxalism, money laundering, terrorism financing, financial frauds and organized crime are increasingly being propagated using mobile technology and social media.

- **Limited police presence**

  The total number of personnel count in Central and State security agencies is around 3 million (approximately 2 million State-level personnel and approximately 1 million at the Central level). India's police-to-population ratio is 145 personnel per 100,000 population, much below the UN-prescribed ratio of 222 personnel per 100,000 population[2] . This clearly indicates the probable challenge of providing a safe and secure environment to all citizens through conventional law-enforcement methods.

- **Changing expectations of citizens from law enforcement agencies**

  The citizens of India, who are the primary customers for all the internal security agencies, have also evolved with time. The living standards of citizens have improved and there is an increased urban agglomeration, which has led to increased crime rates in cities. As per the crime statistics published by NCRB in 2015, while the average crime rate (crime per 100,000 citizens) across India stood at 582 in 2015, most of the cities experienced much higher crime rates. For instance, the crime rate in Delhi was 1,067 and Jaipur was 856[1].

  Further, the citizens' expectations from internal security agencies regarding criminal intelligence, response time, investigative and forensic capabilities, and conviction rates have increased, primarily due to the increasing influence of Western developed economies.

The above trends underline an urgent need for the Indian internal security agencies to adapt to the ever-changing technological landscape and adopt smart internal security initiatives to effectively deal with the present and future challenges. It is imperative to adopt a strategic approach and incorporate the use of innovative technologies and systems to improve efficiency, accountability, cost-effectiveness and resource allocation.

[1]Crime in India, National Crime Record Bureau, 2012-2015
[2]Bureau of Police Research & Development, Government of India

2.3 Need to examine smart internal security procurement

The implementation of smart internal security initiatives is increasing and is expected to increase further in the coming years. Accordingly, the human and financial resources spent in the procurement and implementation of these initiatives are also increasing, and are expected to form a significant part of the spending of most internal security agencies. Further, with the Government of India's vision for smart city implementation, the procurement of safe city initiatives such as CCTV surveillance and intelligent traffic management is expected to rise significantly.

However, the current public procurement framework adopted for generic public sector projects may not be adequate to address the requirements of smart internal security projects. The key reasons are as follows:

- **Limited applicability of procurement guidelines**

  While public procurement rules and guidelines address procurement of goods, works and services as separate components, most smart internal security procurements involve an intricate combination of goods, works and services.

- **Lack of previous reference models**

  Most of the smart internal security projects are novel and exclusive in nature and have few or no previous reference implementations in India. In fact, several smart internal security projects currently being implemented in India have been successful in more developed economies in the West, and their application in Indian demographics is still being explored.

- **Innovative procurement models**

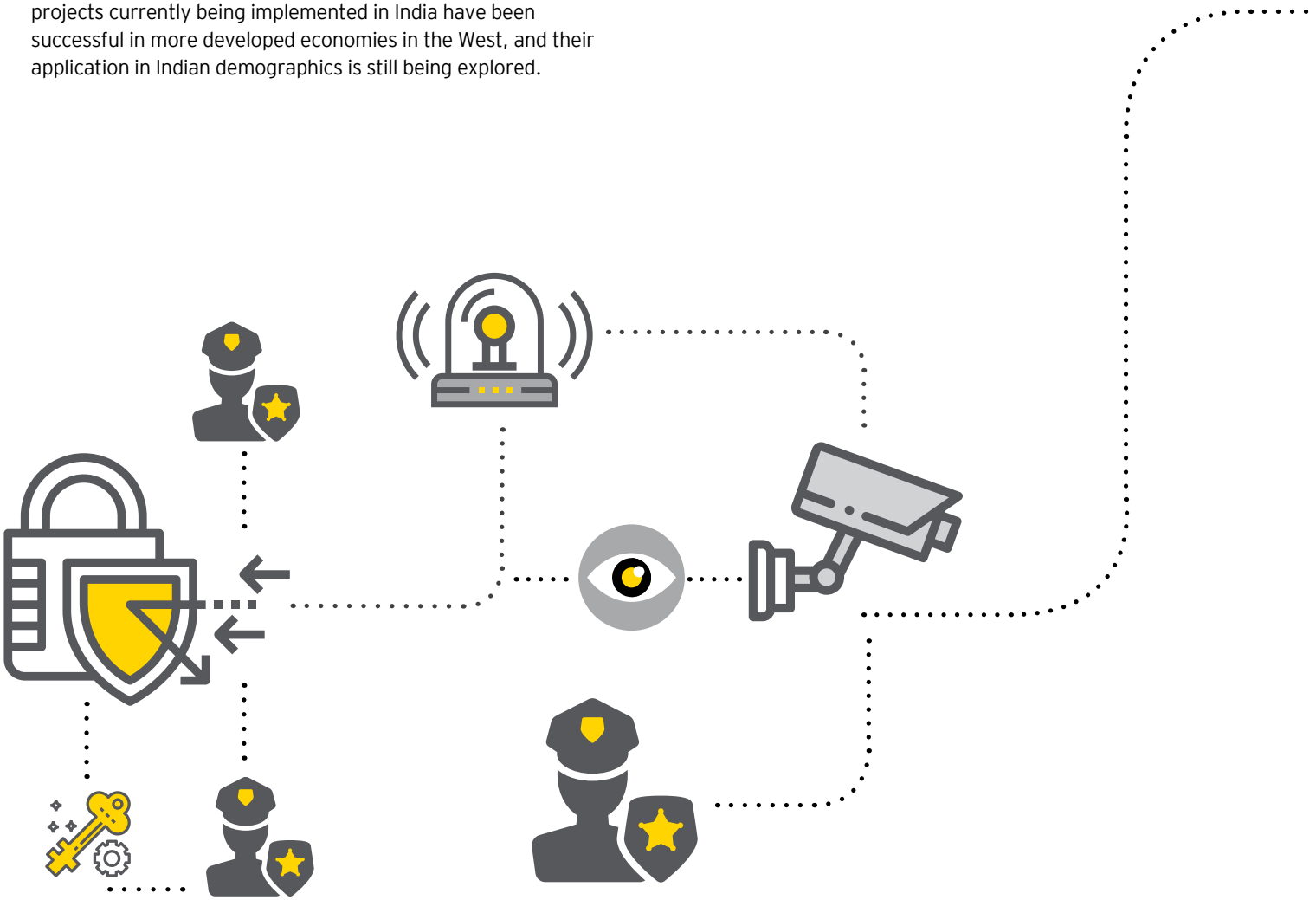
  Several smart internal security projects are being implemented under innovative procurement models, often in public private partnership (PPP) mode, which is different from traditional procurement models.

- **Limited experience of procuring entities**

  Given the limited experience of Indian internal security agencies in implementing smart internal security projects, it is difficult to identify a reliable set of vendors, technologies, products etc. Further, it is difficult to estimate the cost of such projects and the key risks involved in their execution. It is also difficult to clearly define the expected output and outcome of such projects.

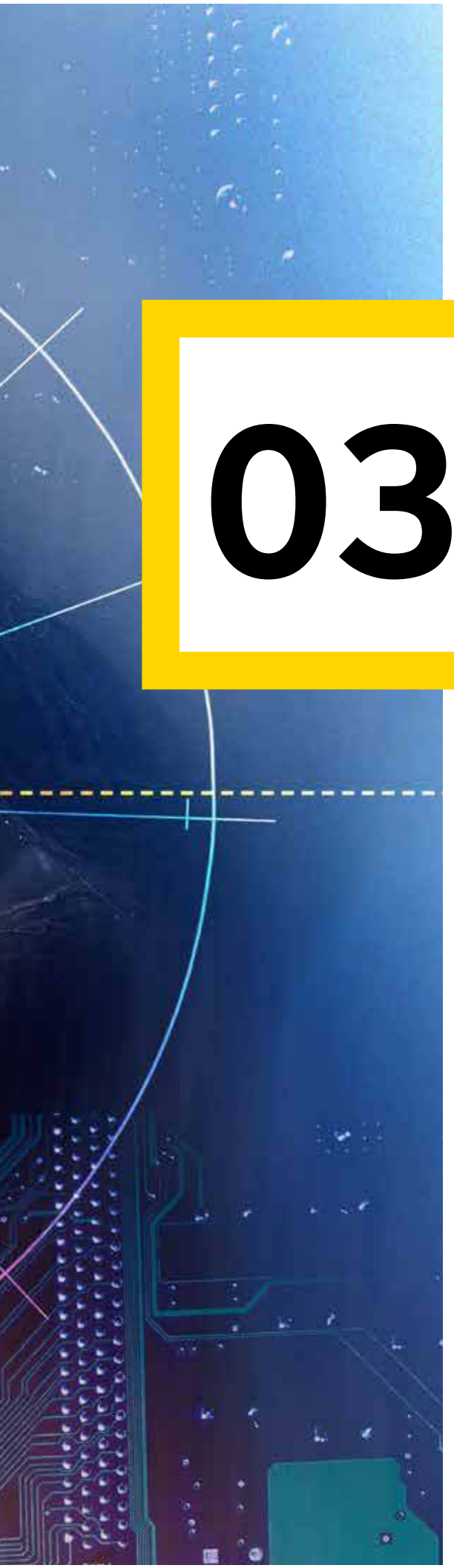
It is therefore essential to examine the procurement framework for smart internal security projects under a different lens, which is customized to its requirements.

In the next section, we introduce a four-pronged framework for analyzing and assessing smart internal security procurement in India.









03 Assessment of smart internal security procurement in India

3.1 Policy and regulations
page - 16

3.2 Processes
page - 19

3.3 Technology
page - 23

3.4 People
page - 25

3 Assessment of smart internal security procurement in India

A radical overhaul of the existing public procurement framework in smart internal security is needed to establish a system that can judiciously utilize the allocated public funds and maintain public trust. In this chapter, we present an analysis of the reforms and initiatives undertaken by internal security agencies on four pillars: Policy and regulations, process, technology and people.

Together, these four pillars will be explored to study the current status of public procurement in the smart internal security domain and the different initiatives taken by the internal security forces in India. This will help in charting the future roadmap for public procurement transformation in smart internal security projects:

- Policy and regulations: Bespoke guidelines and templates to guide the smart internal security procurement will ensure standardized and effective procurement by various procuring entities
- Process: Standardized processes for the entire procurement cycle, from procurement planning till contract management, will drive benefits for smart internal security procurement.
- Technology: Disruption in conventional procurement models and processes should be harnessed through digital technologies for strategy driven, innovative and collaborative procurement of smart internal security projects.
- People: In order to effectively execute the procurement plans of the internal security agencies, adequate engagement and capacity building of different stakeholders, i.e., government officers, private sector participants and citizens, are essential.

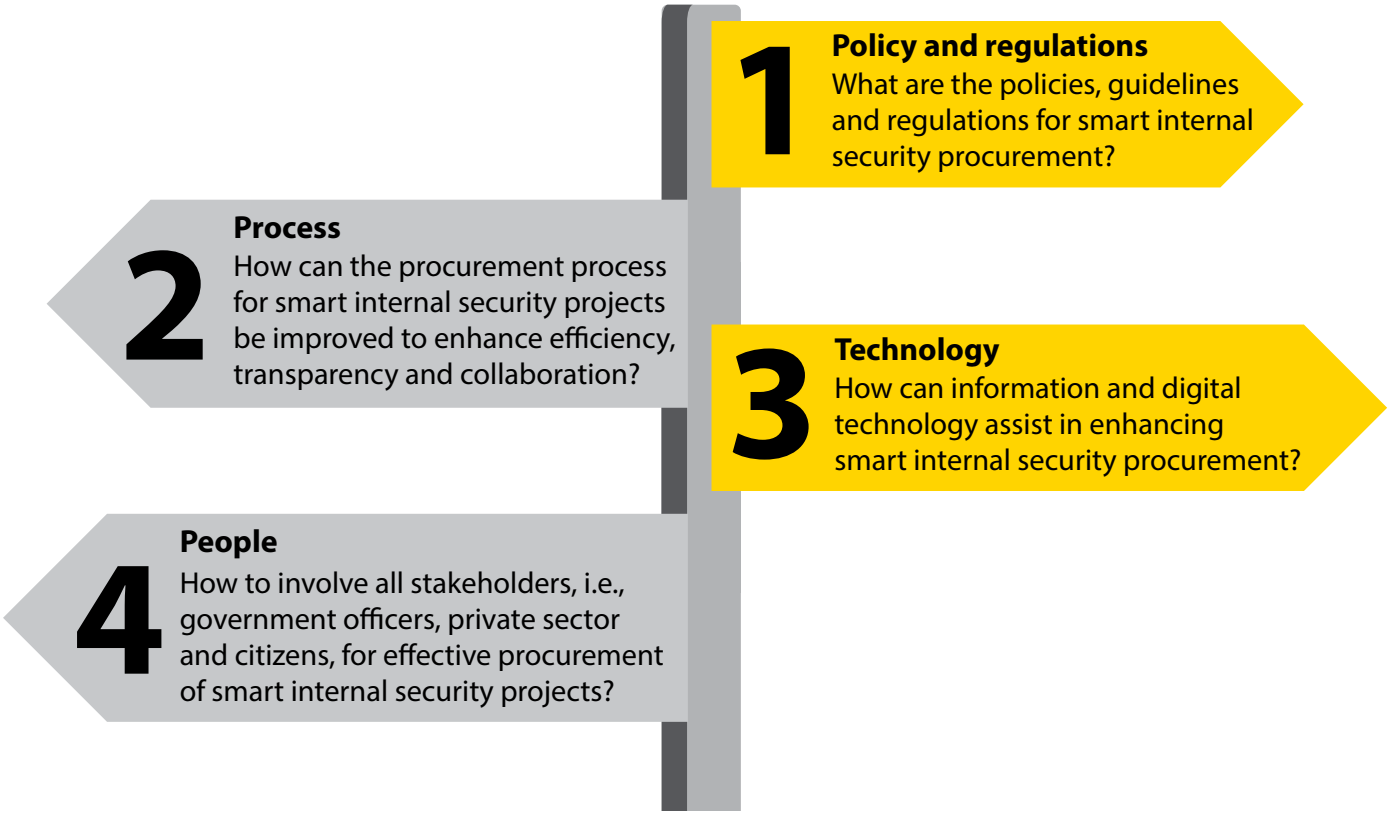


Figure 2: Pillars of reforms in the smart internal security procurement framework

3.1 Policy and regulations

"Malfeasance in public procurement can be contained by having a procurement law and institutional structure"- Shri Arun Jaitley, Hon'ble Finance Minister, Government of India

Research studies suggest that on average, public procurement constitutes 10%–15% of gross domestic product (GDP) worldwide but approximately 20% in India[3] . As discussed in the previous chapter, the procurement of smart internal security is expected to grow many folds in the coming years. Therefore, it is expected to come under the scanner of citizens, media and the Government. It is also difficult to find reference documents and templates when designing tender documents, as these models are still evolving.

Given the esoteric nature of these projects coupled with the increased scrutiny, it is essential that the officers responsible for the design and execution of smart internal security procurements are guided by sound policies and guidelines, and

[3]World Trade Organization estimates

find adequate support from the government. This section explores the Policy & Regulations applicable to smart internal security, on the following dimensions:

- Applicability of current procurement guidelines for smart internal security procurement
- Government support and guidance on smart internal security procurement

Applicability of current procurement guidelines for smart internal security procurement

Public procurement policy is the overarching principle guiding the government officials during the procurement process. Currently there is no national legislation on Public Procurement in India. The figure below represents the institutional and legal framework of public procurement in India.

It can be inferred that the multitude of guidelines and regulations do not provide a single consolidated view of the procurement policy applicable for smart internal security projects. There have been several initiatives taken in revising the public procurement legislation in the last few years, e.g., introduction of the Public Procurement Bill in 2012 (and subsequent revision in 2015), release of GFR 2017 and introduction of Government e-Marketplace (GeM) as an online platform for common use goods and services. Further, the state police forces also have their individual police manuals, which are based on the Model Police Manual issued by the Bureau of Police Research and Development (BPR&D). However, as per BPR&D's own research, most of the police departments are lagging behind in revising their manuals.

The current policies and regulations provide broad guidance for procuring goods, works and services but lack definite procurement guidelines specific to smart internal security projects. Further, due to the multiplicity of policies and regulations, there arises a problem of synchronization between different policies, thus creating confusion.

In 2010, NASSCOM published a study titled e-*Governance and IT services procurement: issues, challenges and recommendations*, which included views from several public and private sector players regarding challenges faced in the procurement and execution of information and digital technology projects in the government domain. One of the key challenges highlighted was the non-standard terms and conditions of the procurement contract. The industry participants recommended that model RFP documents be prepared for each type of ICT project, after industry consultation.

In 2010, the Ministry of Information Technology (MeitY; formerly known as DeitY) designed model RFP documents to act as a guiding light across all government departments for their information and communication technology related procurement, including consulting services, system integration, and hardware and software licenses. Unfortunately, several government organizations were unaware of the existence and legal standing of these model RFPs and therefore never utilized them for their procurements. In 2016, MeitY revised the model RFPs, incorporating the latest technologies, new implementation models and suggestions from the industry.

While the model RFPs of MeitY are not very specific to smart internal security projects, they provide a reasonable template that can be used for the procurement of ICT projects and incorporate the views of the industry. These model RFPs can be utilized by the internal security agencies to develop project-specific model RFPs for smart internal security procurement.

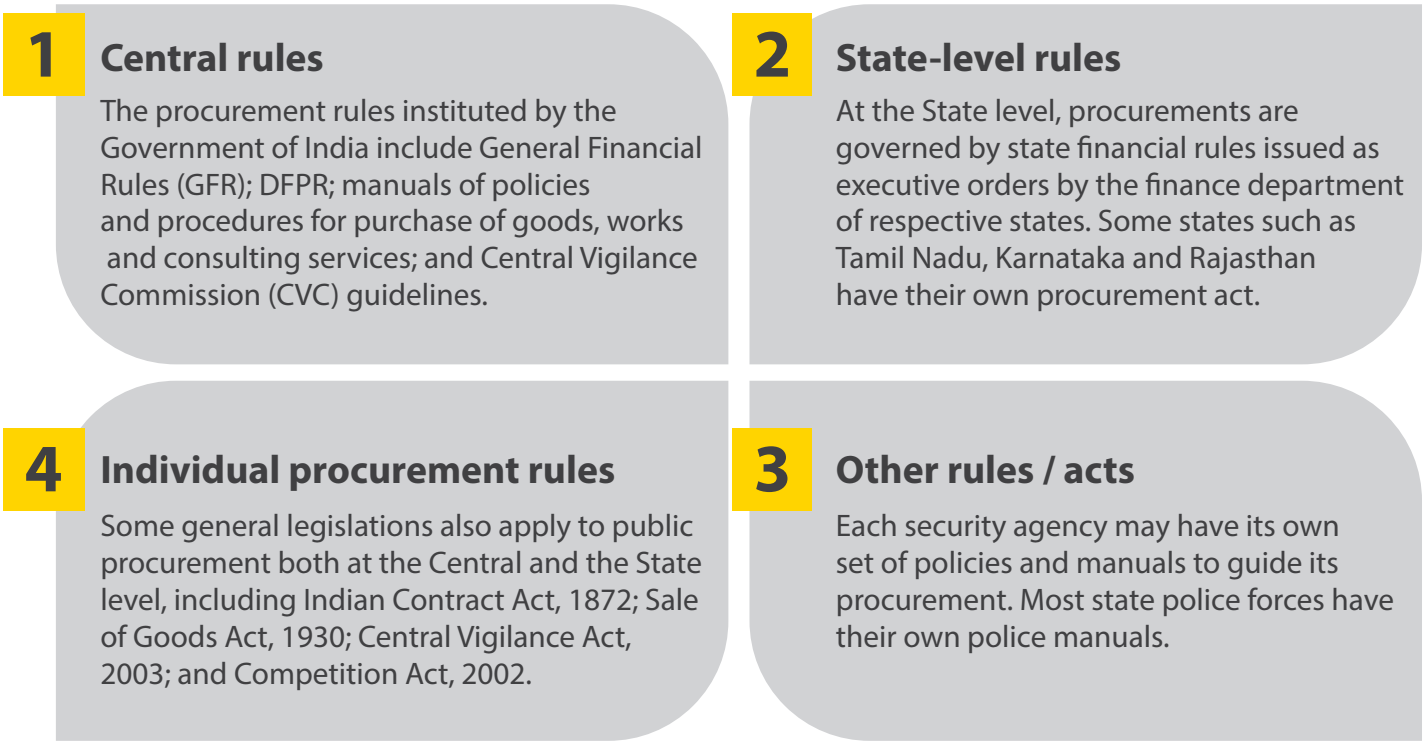


Figure 3: Institutional and legal framework of public procurement in India



US Department of Homeland Security (DHS)

The US Department of Homeland Security (DHS) has issued specific guidelines for procurement namely "Acquisition Policies & Regulations" which facilitate the mission of developing and supporting comprehensive, effective and timely acquisition policy guidance for enhancing the ability to award and administer contracts. Under Acquisition Policies & Regulations, two documents have been published Homeland Security Acquisition Regulation (HSAR) and Homeland Security Acquisition Manual (HSAM).

- HSAR is the regulation that establishes uniform DHS policies and procedures for all acquisition activities within the DHS
- HSAM establishes for the DHS uniform department-wide acquisition procedures, which implement or supplement the Federal Acquisition Regulation (FAR) and the Homeland Security Acquisition Regulation (HSAR), and other agency regulations and statutory requirements.

Source: DHS website



Smart City Mission – Ministry of Urban Development (MoUD), Government of India

For successful implementation of the smart city projects, MoUD Government of India has clearly defined the guidelines and toolkits for all participating cities. These toolkits contain model RFPs, model article of association for Special Purpose Vehicle (SPV), city tenders (collation of all the tenders floated for the SIs), presentations and forms to support the concerned procuring authorities. MoUD has specifically provided separate model RFPs for selection of consulting services and system integration services.

Source: MoUD Smart Cities Mission website

Government support and guidance on smart internal security procurement

Apart from the publishing of project-specific procurement rules, guidelines and templates, it is essential that the Government support the procuring entities in their smart internal security procurement process through other measures. These could include continuous guidance and handholding, brainstorming exercises, roundtable discussions and knowledge-building conferences to share leading practices, capacity-building measures for procuring officers of internal security agencies and regular project status reviews. It is important that MHA and its nodal agencies establish a mechanism for continuous engagement with internal security agencies where MHA can act as a sounding board for their ideas and plans, provide subject-matter expertise, share leading practices from other parts of the country and even alleviate their concerns regarding administrative issues. MHA (or its nodal agencies) can also provide a one-stop-shop for interacting with the vendor community for thought leadership initiatives and ideation on new projects.

One such example can be seen in the implementation of the CCTNS Mission Mode project. NCRB as the nodal agency has played a pivotal role in building the vision of the project, funding, brainstorming, selecting system integrator and consultant, setting guidelines, designing model RFPs, procuring, implementing, monitoring and capacity building, which includes training-related material for all the personnel pan-India. NCRB has provided continuous support to the states for successfully completing the project.

Summary of reform initiatives relating to policies and regulations

While there are some initiatives taken by MHA and other agencies towards establishing adequate policies, regulations and requisite government support for smart internal security procurement; a more concerted effort is required in this domain. A high level assessment of the parameters in the procurement policies and regulations framework is presented in the table below.

S.No.	Parameters	Progress
1	Applicability of current procurement guidelines	**Needs improvement**
2	Government support and guidance on smart internal security procurement	**Needs improvement**

Needs significant improvement | Needs improvement | On track

3.2 Processes

According to the OECD Principles for Integrity in Public Procurement (2009), the procurement cycle consists of three main phases:

- **Pre-tendering**

  Needs assessment, planning and budgeting, definition of requirements and choice of procedures

- **Tendering**

  Invitation to tender, evaluation and award

- **Post-award**

  Contract management, order and payment

The procurement lifecycle for a tender-based smart internal security project can have the following phases:

- Ideation and solution design
- Detailed project report and project planning
- RFP/tender notice and promotion
- Pre-bid meeting and vendor participation
- Bid submission and evaluation
- Award of contract
- Project implementation (project management and contract management)
- Post-implementation (impact evaluation)

Effective procurement would require each stage of the procurement lifecycle to be streamlined and improved to achieve the overall strategic objectives of the project. Each individual part of the lifecycle will also have to be evaluated independently to optimize the steps. The procurement process for smart internal security can become very complex due to the nature of the items that have to be procured, future implications and the large scale of the projects. Therefore, it is imperative to modernize the procurement processes, standardize frameworks and leverage technology to improve efficiency and public service delivery.

This section explores the processes applicable to smart internal security, on the following dimensions:

- Procurement planning and strategy
- Procurement management framework
- Collaboration between different procuring agencies
- Financing of smart internal security projects

Procurement planning and strategy for smart internal security projects

Procurement planning and strategy involves the process of translating the organizational vision and mission into tangible and specific activities, targets and projects. These are used to estimate demand, determine finances and timelines, and plan the end-to-end procurement lifecycle of a project. Robust procurement planning can also help in increasing the participation of external stakeholders in the procurement lifecycle for better solution design and market analysis. Ultimately, sound procurement planning and strategy helps in improving the public procurement output and increasing the value for money.

The uniqueness and complexity of smart internal security projects imply that they require greater amount of planning and preparation. The technologies and systems being deployed under

these projects are new to the Indian scenario in many cases and therefore need long-term planning by both the purchasers and the vendors. It is also important for different smart internal security projects to be integrated with each other for seamless functioning and increased efficiency. This has to be done during the planning and design phase itself, and the procuring entities need to be mindful of the specific integration and operational requirements.

BPR&D emphasized the importance of long-term procurement planning through its report titled *Impact Assessment of Modernization of Police Forces (MPF)*, which was published in 2010. The report states that "MHA could consider issuing a guideline under which all states would create detailed 5 year vision plans for modernization. Based on the vision plans, an approval for 5 year's budget could be granted by MHA." However, most of the state police forces have not prepared their long-term vision or modernization plan. The plans for implementing smart internal security projects are also being driven from MHA, and the states themselves have not carved out a singular view of all their current and future smart internal security projects.

A recent example of long-term planning was seen in the Smart Cities Challenge of Ministry of Urban Development, Government of India. The challenge was rolled out across all states and UTs in India, and 98 cities across India participated in it. Each city was expected to create a 5- to 10-year plan of the initiatives to be taken, including a governance plan, implementation plan, financing plan and risk management plan. This smart city plan was created through a triangulation of the strategic goals of the city, citizens' expectations and leading practices across the globe. The smart city plan of most cities also covered safe city components such as city surveillance, command and control center, and intelligent traffic management.

In February 2017, the Telangana Police called for the preparation of a 10-year "Vision Document" and roadmap. According to an official release, the Director General of Police, Telangana, envisaged a unified Telangana Police that worked seamlessly and delivered prompt, fair and efficient service to the citizens of Telangana. "This involves a smooth integration and interface between various districts/commissionerates, special units and the headquarters and a coordinated approach, with enhanced adoption of technology and advanced techniques in IT, communications and automation - in delivery of services, investigation and administration."



Source: News article published by DNA India on February 16, 2017

Procurement management framework

The procurement management framework covers the processes and practices followed for smart internal security projects. It involves the following stages:

- **Design**

  Requirement definition, demand estimation and supplier analysis

- **Pre-selection**

  Supplier engagement, preparation of RFP and draft contract, and bid collation

- **Select**

  Bid process management, risk assessment and award of contract

- **Execute**

  Contract management, project management and change management

- **Evaluate**

  Post-implementation evaluation of the project, knowledge management and change management

A robust procurement management framework, which includes efficient processes and tested rules and standards, backed by appropriate data, technology and people, is essential for all procuring entities. Proper procurement management frameworks will also help in increasing transparency and accountability of the system, which is extremely important in the context of public procurement in India.

However, given the novelty and complexity of smart internal security projects, the procurement management processes and standards are still evolving. Procuring entities face challenges during the requirement definition and cost estimation stage due to lack of reliable data and previous instances of implementation. Even the procurement data about suppliers, products and previous projects in different/same states is not codified and therefore unavailable for utilization by other procuring entities. Even though several vendors and suppliers have shown active interest in participating in smart internal security projects, their lack of similar experience in Indian markets presents a challenge for the procuring entities.

Contract management for smart internal security projects varies from that for conventional projects. Given the technical complexity

and novelty of such projects, it becomes difficult at their design stage to define their exact scope of work, work products, service-level expectations as well as outcomes. Often, their output is dependent upon inputs from other systems and actions of multiple stakeholders who may belong to different jurisdictions. For instance, smart surveillance projects are often deployed by the police department in a city, but they require buy-in and support of Urban Local Bodies, traffic department, IT department etc. Further, the completion of a project is highly dependent on prior availability of data center, fiber connectivity, GIS map layer etc. Often, these variables make it difficult to execute the projects within the traditional procurement framework, and may require the procuring entity and the implementation agency to devise innovative methods that were not envisaged as part of the original RFP document. In such cases, the conventional contract management framework for goods, works and services may prove too rigid for administering smart internal security projects. It is therefore important for the procuring entities and vendors to establish a flexible contract management and change request framework, based on mutual understanding and trust, so that the projects can be executed smoothly. It is also essential to institute a process for impact assessment of smart internal security initiatives to measure their impact against the originally planned outcomes.

Reiterating the example of the CCTNS project, a robust procurement management framework was instituted by NCRB at the Central level. Comprehensive data sets regarding project budgets, vendor information, contract values of different states/UTs, completion status etc. were centrally published for use by other procuring entities. This led to a more transparent and accountable procurement and also benefitted the procuring entities and the vendors alike.

Collaboration among procuring entities

Each state/UT is unique in terms of demographics, crime profile and therefore smart internal security project requirements. However, the common building blocks of a smart internal security project would remain similar across different implementations. Therefore, it is prudent for procuring entities to collaborate among themselves for procurement of smart internal security projects, to reap economic benefits through aggregation of demand and economies of scale. Collaboration can also help in identifying the leading practices in one state/UT and utilizing them to improve processes in a different state/UT.

The key issues faced in collaborative procurement of smart internal security projects are:

- Lack of planning by procuring entities for smart internal security procurement
- Absence of single national smart internal security database with classification and codification of goods, works and services, which could have helped in identifying areas of collaboration
- Limited impetus from Central agencies to encourage inter-state/UT collaboration

Different models of collaboration can be adopted for smart internal security procurement. Some of the common models are presented below:

- Combining procurement requirements of similar projects into one single project. The common procurement may be carried out for the entire project or some common components of the individual projects, e.g., combined procurement of common software licenses by different procuring entities across a state.
- Combined empanelment of rate contracts with vendors providing smart internal security components. This may be carried out by a few procuring entities on their own or by a central organization, representing all procuring entities, e.g., empanelment of vendors with DGS&D or through Government e-Marketplace (GEM).
- Development of a common scalable project framework for a smart internal security project, which can be customized and scaled for different entities with minimal effort, e.g., centralized development of Core Application Software (CAS) for the CCTNS project, which was then customized for each state/UT.

The police forces in England and Wales have reported a combined savings of over £200 million (2010-15)[4] by leveraging better procurement management techniques and collaboration between different departments.

Financing of smart internal security projects

Smart internal security projects are being financed through a wide range of funding options. As per the Constitution of India, policing is a state subject. Thus, most smart internal security projects at the State level are financed by the State Governments through their internal budget. However, the Central Government provides additional financing to states in order to implement certain projects of strategic importance. Currently, some of the smart internal security projects are directly being financed by the State Governments and some even by Urban Local Bodies (ULBs). Several other projects are being financed through the grants from the Central Government. For example, the CCTNS project is being financed as a Mission Mode Project (MMP) by the MHA, several Safe City initiatives are being financed by the MoUD under smart city scheme, and centralized emergency response projects are being partially funded by MHA.

The expected pace of implementation of smart internal security projects is, however, much greater than the availability of government funds to implement these projects. Further, it is also noteworthy that given the novelty of smart internal security projects in India, there is a limited number of vendors and technologies currently on offer. Several leading global vendors are

[4]Forensic and other services procurement cost comparison, Police.UK, 2015

still testing the waters of the Indian markets and therefore their price propositions are not yet customized to the Indian scenario. This makes it difficult for Indian purchasers to obtain the best value for money from such projects.

The above scenario requires that the vendor ecosystem for smart internal security be quickly ramped up. Also, it is imperative to identify new and innovative modes of financing smart internal security projects. Some of the innovative financing models emerging in digital projects include public private partnership (PPP), public private people partnership (4P), crowd funding and monetization of data and services in smart internal security projects. Sangrur Police initiated the "Surveillance System for Safe Society" (S4), where they installed 2,963 CCTV cameras[5] . The project was funded externally by NGOs, local unions and social organizations.

However, the inherent security considerations of smart internal security projects would prevent the procuring entities from exploring innovative funding models, which are often utilized by smart city projects.

San Francisco Citizens Initiative for Technology and Innovation (sf.citi)

Sf.citi is a novel initiative undertaken by the technology community of San Francisco to improve public safety, transportation, job creation and education. Sf.citi engaged the technology sector, citizens and city policy makers to work together to achieve the desired objectives.

Sf.citi has created a mobile application to help in streamlining the field reporting process and to enable real-time report sharing for the San Francisco Police Department (SFPD). The SFPD officers also receive direct access to the SFPD crime data warehouse in the field for quick and improved decision making. It was estimated that SFPD efficiency has increased by more than 40%.

This initiative was funded through a US$100,000 donation by sf.citi, laptops were donated by HP and the mobile app was created by sf.citi member company ArcTouch.

Source: Forbes.Com, July 2012

Summary of reform initiatives relating to procurement framework

It can be inferred that the traditional procurement management framework for public procurement needs to be revisited to ensure effective procurement of smart internal security projects. A high-level assessment of the parameters in the procurement framework is presented in the table below.

S.No.	Parameters	Progress
1	Procurement planning	Needs significant improvement
2	Procurement management framework	Needs improvement
3	Collaboration among procuring entities	Needs significant improvement
4	Financing of smart internal security projects	Needs improvement

Needs significant improvement

Needs improvement

On track



[5]CCTV cover without government funds: Sangrur police wins award, Hindustan Times, September 2015

3.3 Technology

Information and digital technologies have emerged as key enablers in improving the efficiency of public entities and bringing in transparency and accountability. With the use of digital technologies, procurement of smart internal security projects can shift from archaic transactional methods to a strategy-driven, innovative, collaborative and relationship-oriented process.

This section explores the following technology interventions and their impact on the procurement of smart internal security projects:

- e-Procurement
- MIS and analytics for procurement

e-Procurement

e-Procurement systems automate the end-to-end procurement process, including pre-tendering (procurement planning, approval and design), tendering (floating of RFP, interaction with bidders, receiving bids, bid evaluation and award of contract), and post-tendering (project monitoring, invoice submissions, payments and change request management). Use of e-Procurement systems not only leads to increased efficiency and transparency, but also allows for wider advertisement as well as standardization of procurement process from planning till contract management. Implementation of e-Procurement and e-Marketplace in Italy and Australia delivered annual cost saving of EUR250 million and AUS$73 million, respectively[6].

Apart from the usual benefits derived from the use of e-Procurement systems, smart internal security projects can derive the following specific benefits:

- Linking procurements with the strategic plan of the purchaser (e.g., completion of CCTNS and surveillance projects can trigger the procurement planning for a crime analytics solution)
- Availability of reference procurement documents of similar projects by other procuring entities, across the country
- Instant notification to a widespread range of vendors, across the globe
- Hassle-free involvement of foreign vendors in the procurement process
- Robust contract management solution allowing automated contract administration taking into account complex RFP terms and yet simultaneously providing flexibility for changes in contract terms, order splitting, change request management etc.
- Reduced chances of litigation as a result of increased transparency

Government e-Procurement was instituted as a Mission Mode Project in India, under the National e-Governance Plan (NeGP). However, given the federal structure, India has multiple e-Procurement systems each at the Center, State level, Municipality level and even separate e-Procurement systems of various procuring entities. Further, despite the mandate to procure all projects above a certain threshold value through e-Procurement, it has been observed that several smart internal security projects are still taking the route of manual procurement. Furthermore, the processes of pre-tendering and post-tendering (or contract management) are very rarely automated in most jurisdictions and organizations.

Digital contract management system – Indian Railways

The Indian Railways has announced the launch of digital contract, a system of digitization of its entire supply chain across all zones. This step is aimed at improving the ease of doing business and transparency. With 100% e-tenders and e-auctions already assimilated into the system, The Railways is further planning to build on these initiatives to achieve seamless flow of material, finances and information.

Digital contract management system of railways envisages involving stakeholders including industries, financial institutions, customers and inspecting agencies, to create an efficient, responsive and transparent system. The system includes digitization of processes such as bill submission, inspection, dispatches, receipt, bill passing and bill payments and enabling the use of analytics for increasing supply-chain efficiencies in real time.

Such digitization will enable the use of analytics for decision-making, reduce inventories and reduce procurement cycle time, leading to reduced cost of products/services.

Source: News article "Railways supply chain to go digital" published in the Hindu on April 10, 2017

[6] EY research

MIS and analytics for procurement

MIS and analytics are very important tools in public procurement to drive various strategic and operational benefits across the entire procurement supply chain.

Business Intelligence in Government of Singapore GeBIZ system

Government Electronic Business (GeBIZ) Portal is an integrated portal for use by all Singapore government agencies to conduct business electronically with their suppliers. The development of business intelligence (BI) in GeBIZ can be broadly divided into two areas: GeBIZ InSIGHT and GeBIZ Management Console (GMC).

GeBIZ InSIGHT allows users to:

- Research past tenders, quotations and period contracts of similar purchases across the entire public sector to determine prices
- Extract purchase references, documents, specifications and requirements of similar purchases. This information will help buyers plan and structure future purchases and source for reliable suppliers
- Appraise suppliers by retrieving supplier financial information and transactional history
- Evaluate current tenders and quotations by guiding buyers through the tender/quotation evaluation process in a step-by-step manner
- Extract information on similar historical purchases and suppliers for buyers to refer to
- Recommend appropriate procurement categories and suggest possible suppliers to invite during the tender notification process

Some key capabilities of GMC include:

- Providing overall spend visibility of government procurement
- Demand forecasting and identifying potential areas for demand aggregation (DA) across the public sector
- Facilitating the establishment of customized procurement KPIs for individual agencies and the entire government

Source: Singapore Government's e-procurement portal

While e-Procurement is being adopted slowly across smart internal projects across internal security agencies in India, a robust and standardized codification of procured items, which can enable procuring entities to understand what is being procured by other entities, is almost non-existent. Each e-Procurement system has its own categorization of items, and the procuring agencies using these systems are forced to choose among these codes. This prevents the creation of a consolidated procurement database, which could have been useful for creating MIS and analytics to assist with future procurements.

Further, given the novelty of smart internal security projects, it is important that key lessons learned from any implementation of these projects are comprehensively documented and shared with the other procuring entities. Information such as project objectives, project design considerations, procurement model, supplier study, price estimation, bidding documents, implementation plan and challenges, risk management plan and project KPIs can be contributed by procuring entities and should be available to other entities through a central knowledge repository. Currently, no such knowledge base exists, and the procuring entities have to rely on informal channels and personal acquaintances for gathering such knowledge. Therefore, several procuring entities have to reinvent the wheel for designing and implementing their smart internal security projects.

Summary of reform initiatives relating to technology

It can be inferred that technology initiatives can vastly improve the procurement framework for smart internal security projects. However, due to lack of standardized data and systems, the procuring entities are not able to derive these benefits. A high-level assessment of the parameters in the procurement framework is presented in the table below.

S.No.	Parameters	Progress
1	Procurement planning	**Needs improvement**
2	MIS and analytics for procurement	**Needs significant improvement**

Needs significant improvement | Needs improvement | On track

3.4 People

Smart internal security projects generally involve multiple stakeholders, often including the private sector and the citizens as well. Due to the strategic importance as well as novelty of smart internal security projects, it has become crucial for internal security agencies to involve all stakeholders from the planning stages of these projects and keep them engaged till the end to ensure that the intended outcomes are achieved.

This section explores the following people interventions and reforms, and their impact on the procurement of smart internal security projects:

- Engagement with the private sector
- Citizen engagement – pre- and post-procurement
- Change management of government officers

Engagement with the private sector

Several smart internal projects currently being implemented in India are largely inspired by the technologies and projects implemented in developed economies in the West, which have a very dissimilar demographic and crime profile as compared with India. The private sector has generally been the torchbearer for these newer technologies and has made considerable effort in demonstrating these technologies to the Indian internal security agencies and decision makers. However, it is important that the public sector should also put in commensurate effort in understanding these technologies and their applicability to the Indian scenario. The rapidly changing technical landscape has made it difficult for the officers in internal security agencies to keep up with the latest technologies. This underlines the need for their constant skill upgrade and technical training. At the same time, it is essential for internal security agencies to sensitize the private sector to the specific needs of Indian security sector. This will enable them to customize their technologies and solution offerings to the Indian context.

Apart from the rapidly evolving technical design of smart internal security projects, the conventional procurement models are also witnessing disruption. Internal security agencies are either inventing new procurement models or taking reference procurement models implemented outside India, which have not been implemented before in the Indian context. Therefore, upskilling of procurement officers of internal security agencies is required along with a dialogue with the private sector players to identify the most suited procurement models for each project.

MoUD, Government of India, has adopted a highly participative and collaborative model for its flagship Smart City Mission. Strategic alliances were fostered with vendors for knowledge sharing, including participation by vendors in brainstorming workshops, technology demonstrations and round table conferences with the participating city administration officers.

Ministry of Railways (Railway Board)

The Ministry of Railways plans to set up of a National Rail Transport University (NRTU). NRTU's mission is to host high-quality faculty and research centers for creating a resource pool for best-in-class professionals for the railways and transport sectors. It will deliver digitally enabled programs and act as a large-scale platform for technical skilling and continuous learning of government employees. NRTU will invite participation from private sector in design and delivery of technical courses.

The initiative will ensure setting up of a collaborative platform between the public and private sector. This will promote growth of both the stakeholders in understanding, developing and executing citizen-centric digital initiatives.

Source: RFP document released by Indian Railways for National Rail Transport University

Citizen engagement – pre- and post-procurement

Citizen engagement is an inseparable component of an efficient and accountable procurement process. Citizen engagement is important at the stage of planning and designing smart internal security projects, and it is also important to gauge citizen feedback after the implementation of these projects.

At the planning and design stage, citizen feedback can help the purchasers identify which smart internal security projects should be prioritized and the key expectations of the citizens that these projects need to fulfill. Engagement of citizens at this stage will also help build awareness about the project and develop a common understanding of the outcomes from the project. Citizen engagement and feedback after the implementation of a smart internal security project becomes even more important, as most of these projects have a citizen interface and can succeed only through active adoption by citizens. Currently, internal security agencies seldom engage citizens for planning of smart internal security projects. Post-project engagement is mostly limited to one-way communication regarding the implementation of the project.

One of the largest citizen engagement exercises was mandated by the MoUD for its smart city challenge wherein 98 cities competed by submitting their plans for transforming into smart cities. One of the key requirements was to engage citizens, and gather their requirements and expectations from the proposed smart city initiatives. Door-to-door surveys, social media and government websites were leveraged for the initiative. Smart City Plans saw participation from citizens at unprecedented levels. Approximately 1.5 million citizens contributed on the "My Gov" portal by uploading their views and suggestions[7] .

[7] Press Information Bureau article dated June 25, 2016

Bangladesh – Citizen engagement in public procurement under Procurement Reform Project (PPRP)-II

With the assistance of the World Bank Group, Bangladesh has set up Procurement Reform Project (PPRP)-II, which involves pre- and post-engagement of citizens in public procurement. A Citizen Committee was formed at the Upazila level, which included 12 to 15 members from a range of professionals, including school teachers, social workers, retired government officials, retired engineers, and health professionals. The committee members were trained on technical issues of procurement monitoring and modalities of group monitoring. This proved to be of help to increase citizen engagement for review of the projects being implemented.

Source: Report by BRAC Institute of Governance and Development, 2016

Philippines – End-to-end procurement process involving citizen participation

The Philippines Procurement Law mandates citizen participation in all stages of the procurement process, including pre-bid conference, opening of bids, bid evaluation, post-qualification and award of contract. Under this system, procuring entities are required to invite outside organizations to sit in on meetings of their Bid and Awards Committees (BACs). Observers may also observe contract implementation, and citizens are able to file complaints with the local ombudsman if they suspect irregularities.

Source: PhiliGems Policy

Change management for government officers

The implementation of smart internal security projects is disrupting the conventional models of internal security and law enforcement, including service-level expectations of citizens, standard operating procedures and governance structures. Successful implementations of these projects would require a great deal of effort and change from the internal security personnel, who are required to not only learn the new technologies and processes but also unlearn the conventional methods.

Procurement of smart internal security projects cannot be treated as a standalone process. The success of the procurement process is tied to effective capacity building and change management for successful implementation of these projects. It is critical to train the procurement personnel on planning and managing change.

An effective change management process should start from the planning and designing stage of the project, where a common project vision is shared with all the stakeholders. Phase-wise communication and training should be planned, so that the users can get accustomed to the modern technologies and paraphernalia. Tying up performance management framework of stakeholders with their adoption of newer technologies can also prove to be an effective measure for change management.



Summary of reform initiatives relating to people

It can be inferred that the "people" aspect of procurement is crucial to achieving the vision of smart internal security in India.

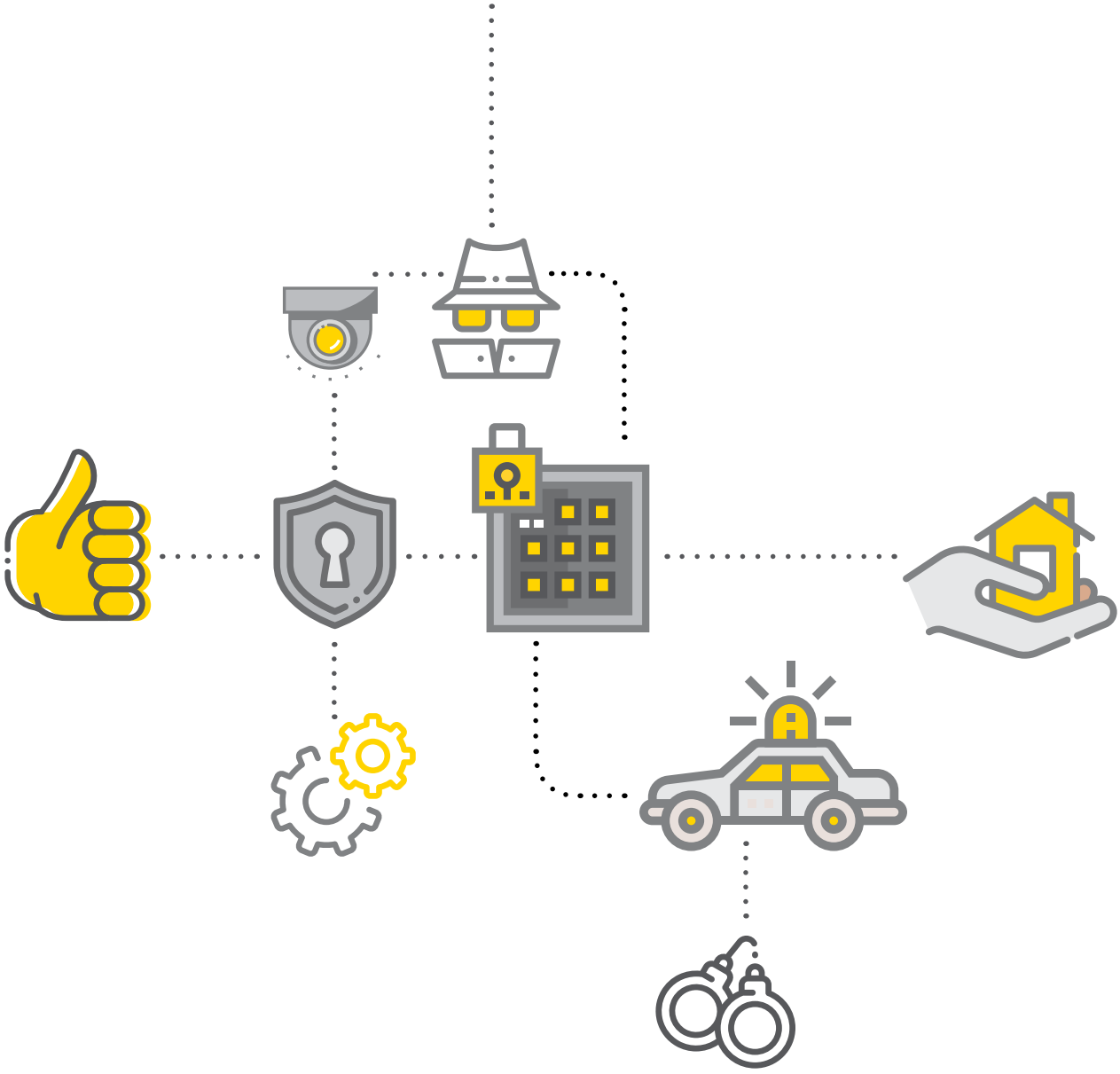
A high-level assessment of the parameters in the procurement framework is presented in the table below.

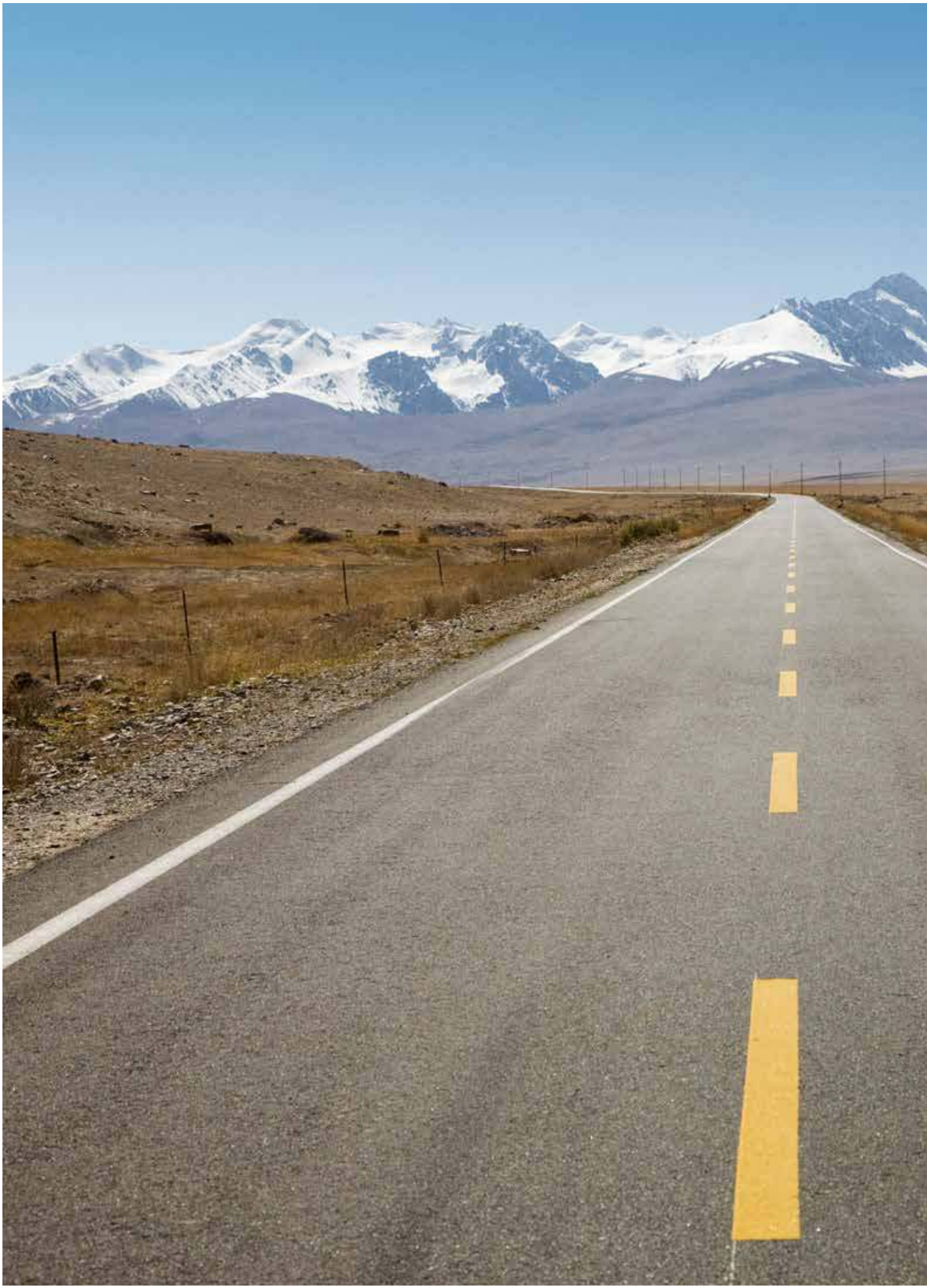
S.No.	Parameters	Progress
1	Engagement with the private sector	**Needs improvement**
2	Citizen engagement – pre- and post-procurement	**Needs significant improvement**
3	Change management of government officers	**Needs improvement**

Needs significant improvement

Needs improvement

On track







04 The road ahead

4 The road ahead

Despite significant investment in smart internal security initiatives in the past decade by the Central and State Governments in India, such initiatives are yet to succeed in meeting the desired outcomes envisaged by the Government. In the previous sections, we have established the disruptive impact of smart internal security projects and how they are essential for meeting the challenges being faced by Indian internal security agencies. We have also explored the various challenges being faced in the procurement of these projects under four different pillars, i.e., policy and regulations, process, technology and people. This is not only hampering the government's ability to deal with the complex procurement needs in smart internal security projects but also impeding the overall growth of the sector. To ensure that procurement in smart internal security projects is conducted in an efficient and transparent manner, a comprehensive set of guidelines, principles and policies should be available. Also, technological advancements should be leveraged in transforming the existing public procurement model in smart internal security. Continuous engagement of all stakeholders including internal security agency personnel, private sector and the citizens is essential as well.

Some of the steps that can be taken to transform the smart internal security procurement in India are enumerated below, under the four pillars of policy and regulations, process, technology and people.

Policy and regulations

1. Preparation of procurement guidelines and model RFPs

It is imperative that common procurement guidelines and standard procurement documents (or model RFPs) are created for similar types of smart internal security projects. Similar initiatives have already been taken for the CCTNS project by NCRB and for smart city projects by MoUD.

The model RFPs can be based on the applicable Central/State procurement rules and regulations, and can provide sufficient flexibility to the procuring entities to make changes as per the specific requirements of each project.

2. Central agency to guide smart internal security projects

There is a need to establish a central agency that is responsible for providing thought leadership and guidance to all internal security agencies regarding the design, procurement and implementation of smart internal security projects. Apart from establishing project standards, this central agency can also facilitate dialogue and sharing of leading practices and learnings between procuring entities across the country. This agency should also ensure continuous monitoring and periodic review of all smart internal security procurement related activities. In the current scenario, it is suggested that BPR&D could act as the central agency for smart internal security projects.

Process

3. Long-term plan for smart internal security procurement

It is recommended that all the smart internal security agencies be asked to prepare a 3- to 5-year procurement plan for their smart internal security initiatives. The plan should take into account the strategic priorities of the procuring entity, mandates from the MHA and leading practices from other geographies. Some of the elements that can be covered in the plan are list of smart internal security projects, financial estimates, implementation plan, integration plan with other projects, financing plan and risk management plan.

These long-term procurement plans and vision documents can help all the stakeholders involved in the process by increasing transparency and involving suppliers and vendors from the pre-procurement stage itself. This will allow for greater market engagement as the vendors can see what relevant opportunities are anticipated. They can also contact authorities for information and planning their product development and customization specific to the planned initiatives. This can also help in internal planning for internal security agencies and budget estimation.

4. Collaborative procurement model for smart internal security projects

Given the similar nature of various smart internal security projects being implemented across various jurisdictions in India, it would be prudent to promote collaborative procurement models. These could range from mass scale procurement by a central agency and further downstream distribution, to empanelment of vendors at negotiated prices to provide services across all jurisdictions. Another common model for implementation has emerged in smart internal security projects called the cafeteria model. Under this model, a standard scalable product can be developed centrally, after gathering common requirements from all jurisdictions. This central product can then be offered to all the participating entities, through a common IT infrastructure to save on costs and implementation effort. Individual procuring entities can ask the implementation agency to make small changes to the solution as per their specific requirements. This model leads to considerable cost savings as compared to separate implementation by each procuring entity.

Technology

5. Mandatory use of e-Procurement for smart internal security procurement

While most jurisdictions have made the use of e-Procurement portals mandatory for public procurement above a certain threshold value, this mandate is not being followed by several procuring entities. It is recommended that procurement of smart internal security projects only be done through an e-Procurement solution. This initiative will help in creating standardized data sets for all smart internal security procurements, which can then be utilized for the purpose of MIS and business intelligence.

6. Smart internal security procurement database

A standardized procurement database of smart internal security procurements needs to be created across all internal security agencies in India. It is recommended that a standard codification for procurement categories, types of items being procured and classification of vendors be created. The database can be populated by all internal security agencies and made available across India to any procuring entity planning to carry out procurement of a smart internal security project. Further, analytics can be applied on this database to derive useful insights and intelligence on suppliers, prices, procurement strategies, implementation challenges etc.

7. Knowledge management framework

It is recommended that a centralized knowledge management portal be implemented, specifically catering to smart internal security project planning, design, procurement and implementation. The portal can be made available to all internal security agencies, and can also have restricted participation from the vendors and citizens.

The knowledge portal will be a repository of guidelines, processes, leading practices, procurement models, standard operating procedures, RFPs, project approach and methodologies. Vendors will also provide domain-specific knowledge to be added to the database.

People

8. Engagement with industry and vendor community

Internal security agencies should proactively engage with the industry and vendor community to form a common opinion on the design of procurement models for smart internal security projects. Further, the industry should also be engaged to impart knowledge and leading practices of smart internal security projects implemented in other jurisdictions (in India or outside India). The public sector should also educate and sensitize the industry and vendors on the Government's procurement plans, mandates and objectives.

9. Citizen engagement

It is recommended that citizens be engaged in the planning and design phase of smart internal security projects to understand their sentiment toward the need and benefits of these projects. Further, it is extremely important to gather feedback and conduct a sentiment analysis of the citizens after the implementation of smart internal security projects, and then use the feedback to improve the project design and operations.

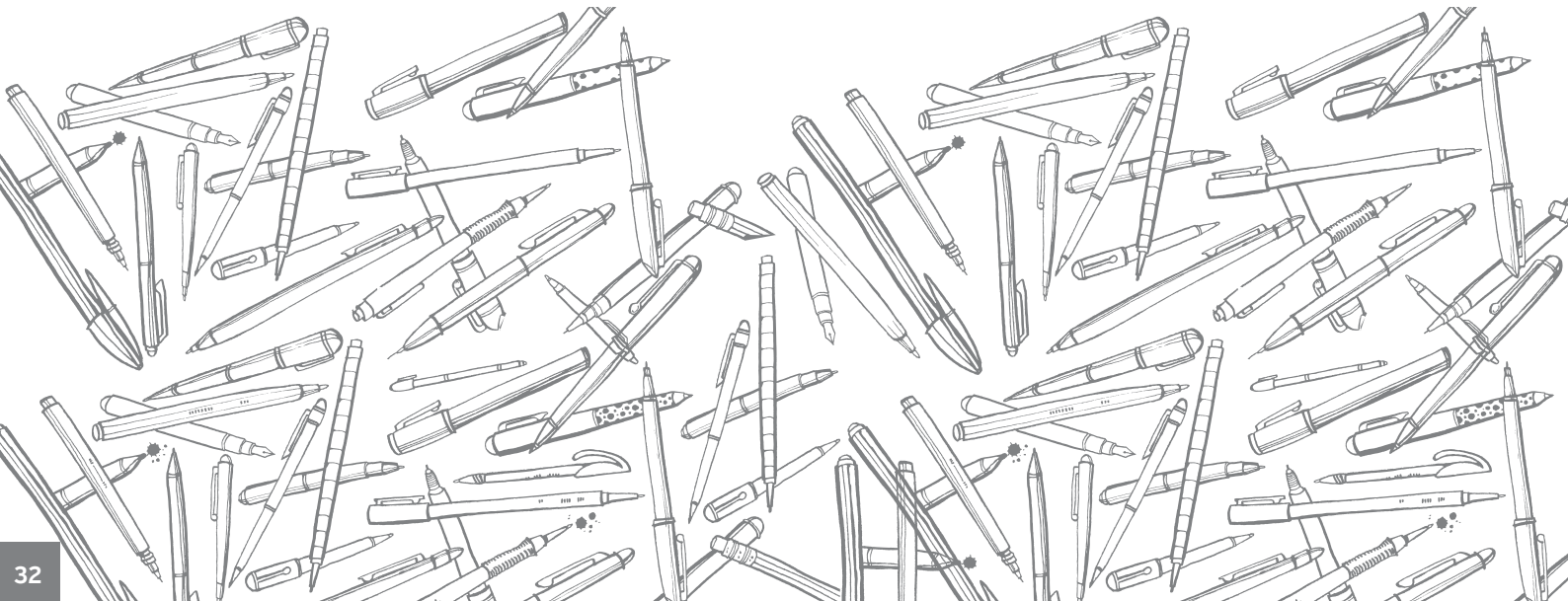
10. Change management

Change management is an extremely important component of all government projects and is especially important for successful implementation of smart internal security projects. It is recommended that pre-procurement and post-implementation training programs be mandatory for all relevant stakeholders of smart internal security projects. Performance appraisals of government officials involved in smart internal security projects should take into account their performance in implementing and adopting these projects.



Bibliography

- Acquisition Policies and Regulation, U.S. Department of Homeland Security
- CCTNS Project, Print release by Press Information Bureau, Government of India, February 2015
- CCTNS: RFP for selection of System Integrator, Delhi Police
- CCTV cover without government funds: Sangrur police wins award, Hindustan Times, September 2015
- Crime in India, National Crime Record Bureau, 2012-2015
- Data on police organizations, Bureau of Police Research and Development, Jan 2016
- Demand for Grants: 2017-18 Analysis (Home Affairs), PRS Legislative Research, March 2017
- e-Governance and IT services procurement: issues, challenges and recommendations, NASSCOM, 2010
- Extension of CCTNS Project, print release by Press Information Bureau, Government of India, November 2015
- Forensic and other services procurement cost comparison, Police.UK, 2015
- For India, internal security a greater challenge despite border skirmishes, Indian Express, January 2016
- Government procurement in India: domestic regulations and trade prospects, CUTS International, 2012
- Government procurement law and policy: India, Library of Congress, March 2010
- Impact assessment of Modernization of Police Forces, Bureau of Police Research and Development, 2010
- India's staggering wealth gap in five charts, The Hindu, December 2014
- Model Police Manual, Bureau of Police Research and Development
- National requirement of manpower for 8-hour shifts in police stations, Bureau of Police Research and Development, 2015
- Prime Minister Narendra Modi bats for SMART policing, The Hindu, November 2014
- Principles for Integrity in Public Procurement, OECD, 2009
- Public Procurement Bill, 2012 (as Introduced in Lok Sabha), Ministry of Finance, Government of India, 2012
- RFPs, Ministry of Urban Development: Smart Cities Mission, 2017
- RFP standardization: model RFPs and guidance notes, Ministry of Electronics and Information Technology, 2017
- Smart policing awards 2016: compendium of best practices in smart policing, FICCI, 2016
- Social accountability in public procurement: How citizen engagement can make a difference, BRAC Institute of Governance and Development, 2016
- Social accountability in public procurement: how citizen engagement can make a difference, BIGD Public Procurement Reform Project II, October 2016
- Social media penetration in rural India grows faster than urban, Business Standard, June 2015
- Telangana police chief calls for preparing 'Vision Document', Outlook India, February 2017
- Training program on public procurement, Ministry of Finance, Government of India, January 2015





About FICCI Security Department

FICCI has many specialised committees where key concerns of the industry are debated and discussed with the specific aim of presenting the recommendations to the Government for favourable decisions.

Considering internal security is the backbone of growth and overall development of a nation, FICCI has constituted two specialised committees to look into various aspects of security –

- Committee on Homeland Security (HLS) is chaired by Mr. G. K. Pillai, Former Union Home Secretary, Govt. of India, which is working towards bridging the gap between policing and technology.
- Committee on Private Security Industry (PSI) is chaired by Ms. Manjari Jaruhar, Former Special DG – CISF, Govt. of India. The committee has been advocating for key policy issues confronting the industry.

Some of the focus areas:

Police Modernisation: FICCI is working towards bridging the gap between policing and technology. We engage with various enforcement agencies and provide them a platform to interact with industry, to articulate their requirements and to understand new technologies for security. This initiative is under our umbrella theme of "Safe & Secure Nation".

Road Safety: United Nations has proclaimed 2011-20 as the Decade of Action on Road Safety. FICCI feels that the Indian Industry can play a significant role in addressing the issue of road safety and will be promoting potential private sector interventions in Road Safety through their core business activities.

Indian Unmanned Aerial Systems (UAS) Policy & Regulations: FICCI has initiated formulating Working Groups in areas of: (a) enabling regulations for developmental use of UAS, and prevention of rouge UAS; (b) framework for permission and licencing for manufacturing of UAS; and (c) technological structure for detection and neutralisation of unidentified UAS. FICCI will submit the suggestions and recommendation for Indian UAS Policy & Regulations to the Ministry of Home Affairs.

SMART Policing: FICCI has initiated the process of examining the details of initiatives in SMART Policing across the country and will share the same with the relevant ministries/departments to help Government and police departments in learning from the experiences of other states and also for possible adoption of some of the best practices. FICCI has also been advocating for the cause of SMART policing and its relevance for India's growth.

India Risk Survey: FICCI every year conducts survey of risk as perceived by corporates, which could affect business continuity. The objective of the report is to inform and sensitise all stakeholders about the emerging risks for a developing economy like India, so that well planned and strategic policy decisions can be made.

Security Standards and Guidelines: FICCI is working with the Bureau of Indian Standards (BIS) for creation of standards and guidelines for electronic security.

Capacity Building Programmes: FICCI has initiated capacity-building programmes and workshops as an attempt to increase awareness about Women Safety at Work Place, Forensics of Fraud Detection, White Collar Crimes, etc.

Public Procurement for Internal Security: FICCI is working towards advocacy for bringing well-defined procedures for fair and transparent procurement of security products and solutions, so as to provide level playing field to the industry.

Enforcement of Private Security Agencies Regulation (PSAR) Act 2005: Major portion of the private security industry is unorganised. FICCI is advocating the proper enforcement of the Act.

Armed Security for Cash Logistics: FICCI is advocating for a well-articulated policy for deployment of armed private security guards for protection of cash vans, which carry crores of public money every day.

Private Security Workers' Categorisation as Skilled / Highly Skilled Workers: Re-categorisation notified vide a Gazette notification S.O.191(E). Security guards without arms have been categorised as 'Skilled Workers' and Security guards with arms have been categorised as 'Highly Skilled Workers'.

Minimum Standards/Guidelines for Cash Logistics Companies: FICCI is advocating for establishment of standards and operating guidelines for cash logistics companies.

FICCI Contacts

Sumeet Gupta
Director
sumeet.gupta@ficci.com

Ankit Gupta
Senior Assistant Director
ankit.gupta@ficci.com

FICCI
Federation House, Tansen Marg, New Delhi - 110 001
T: +91-11- 23487515, 23487212, F: +91-11- 23765333
www.ficci.com

EY Contacts

Rahul Rishi
Partner
Rahul.Rishi@in.ey.com

Akshya Singhal
Director
Akshya.Singhal@in.ey.com

Saurabh Bansal
Senior Manager
Saurabh.Bansal@in.ey.com

Ernst & Young Offices

Ahmedabad
2nd floor, Shivalik Ishaan
Near. C.N Vidhyalaya
Ambawadi
Ahmedabad-380015
Tel: +91 79 6608 3800
Fax: +91 79 6608 3900

Bengaluru
12th & 13th floor
"U B City" Canberra Block
No.24, Vittal Mallya Road
Bengaluru-560 001
Tel: +91 80 4027 5000
+91 80 6727 5000
Fax: +91 80 2210 6000 (12th floor)
Fax: +91 80 2224 0695 (13th floor)

1st Floor, Prestige Emerald
No.4, Madras Bank Road
Lavelle Road Junction
Bengaluru-560 001 India
Tel: +91 80 6727 5000
Fax: +91 80 2222 4112

Chandigarh
1st Floor
SCO: 166-167
Sector 9-C, Madhya Marg
Chandigarh-160 009
Tel: +91 172 671 7800
Fax: +91 172 671 7888

Chennai
Tidel Park
6th & 7th Floor
A Block (Module 601,701-702)
No.4, Rajiv Gandhi Salai
Taramani
Chennai-600113
Tel: +91 44 6654 8100
Fax: +91 44 2254 0120

Delhi NCR
Golf View Corporate
Tower - B
Sector 42, Sector Road
Gurgaon-122 002
Tel: +91 124 464 4000
Fax: +91 124 464 4050

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity New Delhi-110037,
India
Tel: +91 11 6671 8000
Fax +91 11 6671 9999

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
NOIDA-201 304
Gautam Budh Nagar, U.P. India
Tel: +91 120 671 7000
Fax: +91 120 671 7171

Hyderabad
Oval Office
18, iLabs Centre
Hitech City, Madhapur
Hyderabad - 500081
Tel: +91 40 6736 2000
Fax: +91 40 6736 2200

Kochi
9th Floor "ABAD Nucleus"
NH-49, Maradu PO
Kochi - 682 304
Tel: +91 484 304 4000
Fax: +91 484 270 5393

Mumbai
14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (west)
Mumbai-400 028, India
Tel: +91 22 6192 0000
Fax: +91 22 6192 1000

5th Floor Block B-2
Nirlon Knowledge Park
Off. Western
Express Highway
Goregaon (E)
Mumbai-400 063, India
Tel: +91 22 6192 0000
Fax: +91 22 6192 3000

Pune
C–401, 4th floor
Panchshil Tech Park
Yerwada
(Near Don Bosco School)
Pune-411 006
Tel: +91 20 6603 6000
Fax: +91 20 6601 5900



Ernst & Young LLP

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016

© 2017 Ernst & Young LLP. Published in India.
All Rights Reserved.

EYIN1705-053
ED None

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither Ernst & Young LLP nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

MK



EY refers to the global organization, and/or one or more of the independent member firms of Ernst & Young Global Limited

About FICCI

Established in 1927, FICCI is the largest and oldest apex business organisation in India. Its history is closely interwoven with India's struggle for independence, its industrialization, and its emergence as one of the most rapidly growing global economies

A non-government, not-for-profit organisation, FICCI is the voice of India's business and industry. From influencing policy to encouraging debate, engaging with policy makers and civil society, FICCI articulates the views and concerns of industry. It serves its members from the Indian private and public corporate sectors and multinational companies, drawing its strength from diverse regional chambers of commerce and industry across states, reaching out to over 2,50,000 companies.

FICCI provides a platform for networking and consensus building within and across sectors and is the first port of call for Indian industry, policy makers and the international business community.

ey.com/in

@EY_India EY|LinkedIn EY India EY India careers