# 8th Foundation Course for MES Officers

**Srinivas Bhoosarapu**

**Information and Cyber Security Researcher ,**

**Former CISO and Chief FinTech and Innovation Officer**

# Information and Cyber Security

**Srinivas Bhoosarapu**

**Information and Cyber Security Researcher ,**

**Former CISO and Chief FinTech and Innovation Officer**

# Agenda

- Information and Cyber Security
- Threats and Vulnerabilities
- Cyber Crimes – Honey Trap
- MES Future Integration Challenges and Opportunities
- Conclusion

# Information and Cyber Security

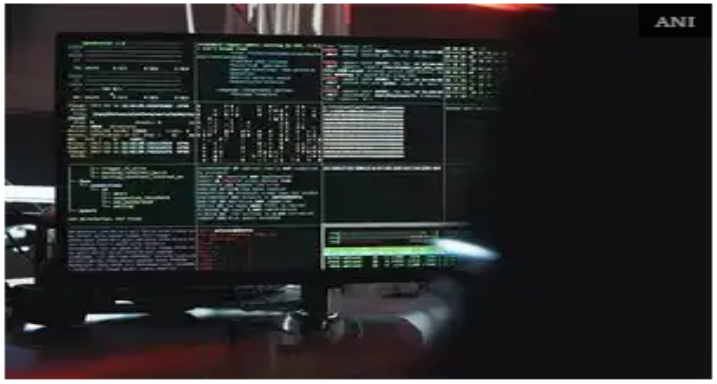
- **Cybersecurity is the practice of protecting computer systems, networks, devices, and data from digital attacks, damage, or unauthorized access,**

**Using a combination of**

- **Technology**
- **Processes**
- **Human awareness (People)**

# ICS in MES

**Synopsis**
Pakistan Cyber Force claims to have breached sensitive data from Indian Military Engineering Service and Manohar Parrikar Institute, potentially compromising defence personnel information. They also attempted to deface the Armoured Vehicle Nigam Limited website, prompting its shutdown for security audit. Cybersecurity experts are monitoring for further attacks, and measures are being taken to strengthen India's digital defences.




Cyber attack alert: Pakistan cyber force claims breach of Indian Defence Institutions websites

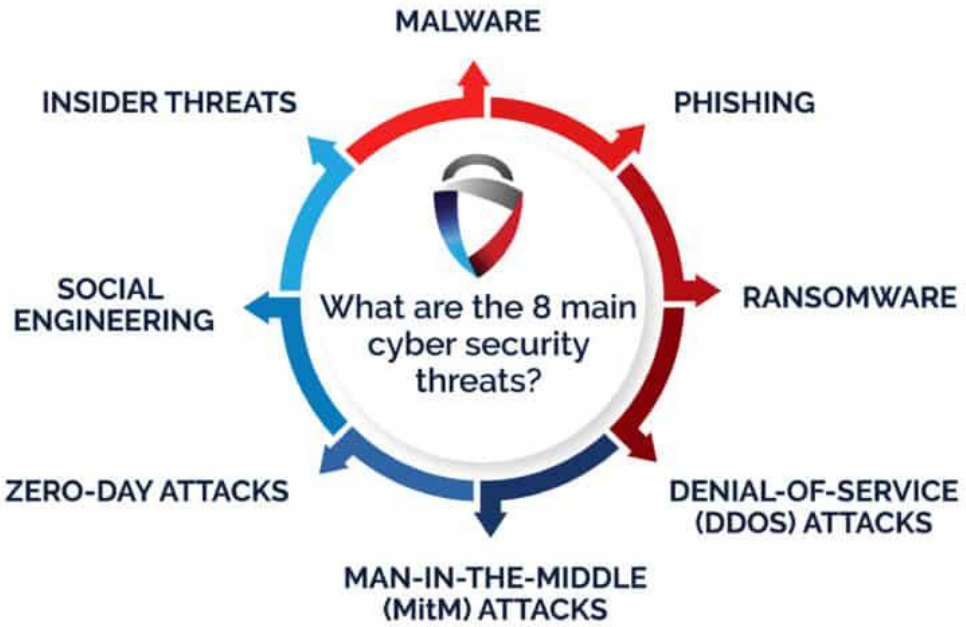
In a continued wave of cyber offensives, the account on X "**Pakistan Cyber Force**" has revealed that the group has allegedly gained access to sensitive data from the **Indian Military Engineering Service** and **Manohar Parrikar Institute** of Defence Studies and Analysis.

According to the sources, the claim suggests that the attackers may have compromised personal information related to defence personnel, including the login credentials.

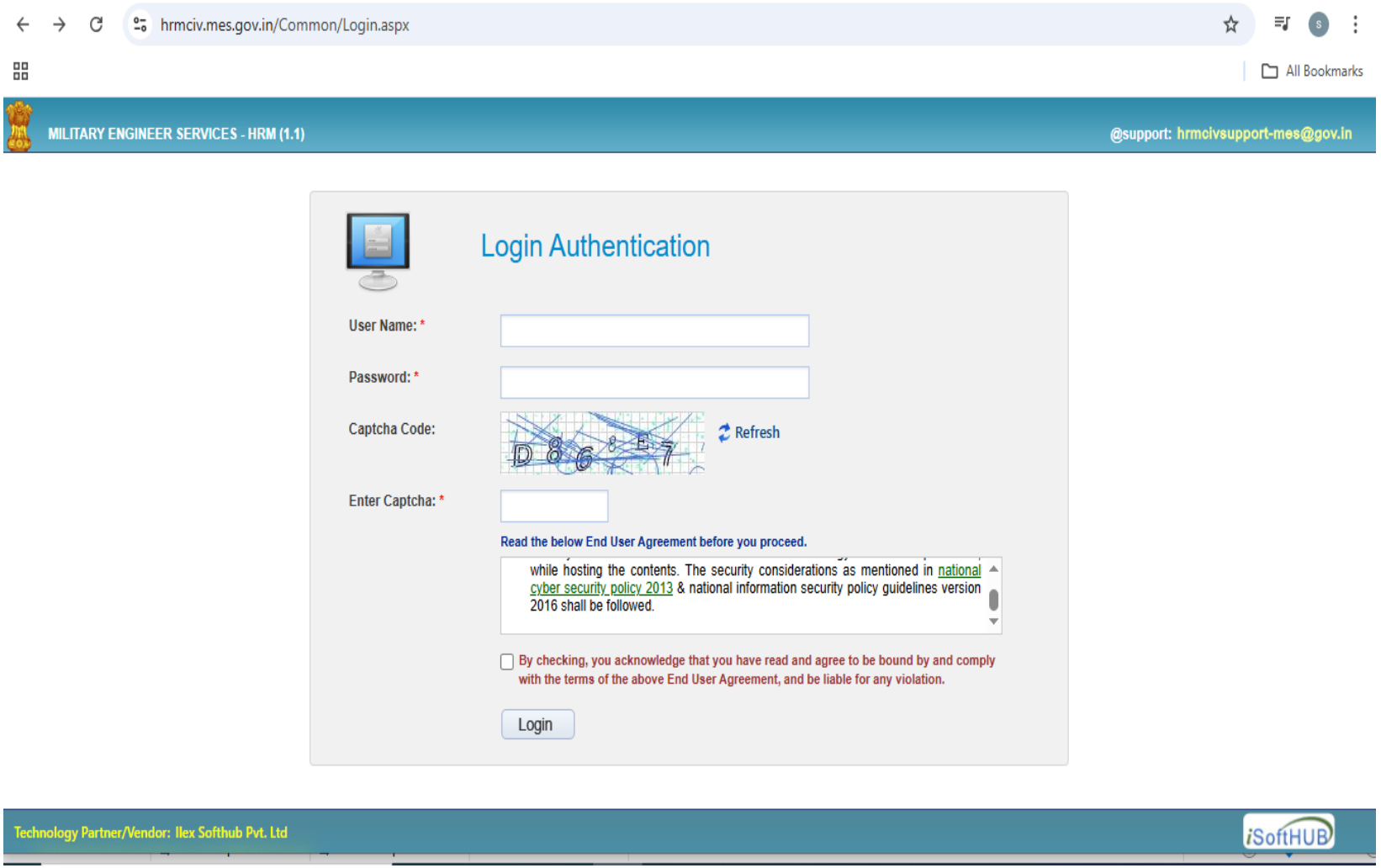
Source: Times of India

# Information and Cyber Security

- **Confidentiality (preventing unauthorized access)**
- **Integrity (protecting data from modification)**
- **Availability (ensuring access for authorized users)**



# HRMS – NCSP 2013 - Authentication



# Digital Transformation – eGov in MES

WEB BASED PROJECT MONITORING PORTAL

PRODUCT APPROVAL PORTAL

INAUGURATION OF WBPMP

BUDGET MANAGEMENT PORTAL

LAUNCH OF e-MB & MIMAMSA

- FOSTER TRANSPARENCY
- BUILD EFFICIENCY
- UNLOCK LATENT PRODUCTIVITY
- EFFECTIVE MONITORING BY STAKEHOLDERS
- ENABLE REPOSITORY OF INFORMATION AT THE CLICK OF THE BUTTON

INAUGURATION OF DWAP

CONTRACTOR AND CONSULTANT ENLISTMENT PORTAL

ELECTRONIC MEASUREMENT BOOK (e-MB)

MES INTEGRATED MONITORING AND MGT SOFTWARE FOR ARBITRATION (MIMAMSA)

190 E-TRAINING MODULES – DD DIGISHALA

**Automation Cell** - For uploading on MES website with open access.

# Digital Transformation – eGovernance

To manage infrastructure, construction, and engineering support for the armed forces, covering civil, electrical, mechanical, and IT domains

- Budget Management Portal
- Contractor & Consultant Enlistment Portal
- Electronic CashBook
- Electronic Measurement Book
- Product Approval Portal
- Project Monitoring Portal
- Work Estimation Application
- e-Governance Portal
- Defence Works Assets Portal
- MIMAMSA

# Cyber Security in MES

**Broadband Connectivity:** Ensuring high-speed internet access to all citizens, including those in rural and underserved areas, to bridge the digital divide and promote digital inclusion.

**Digital Identity:** Establishing secure and reliable systems for digital identity verification, authentication, and authorization, which are essential for accessing online services and conducting digital transactions securely.

**Open Data Initiatives:** Making government data and information freely available to the public in digital formats, promoting transparency, accountability, and innovation.

**Cybersecurity Measures:** Implementing robust cybersecurity protocols and frameworks to protect digital infrastructure, data, and privacy from cyber threats and attacks.

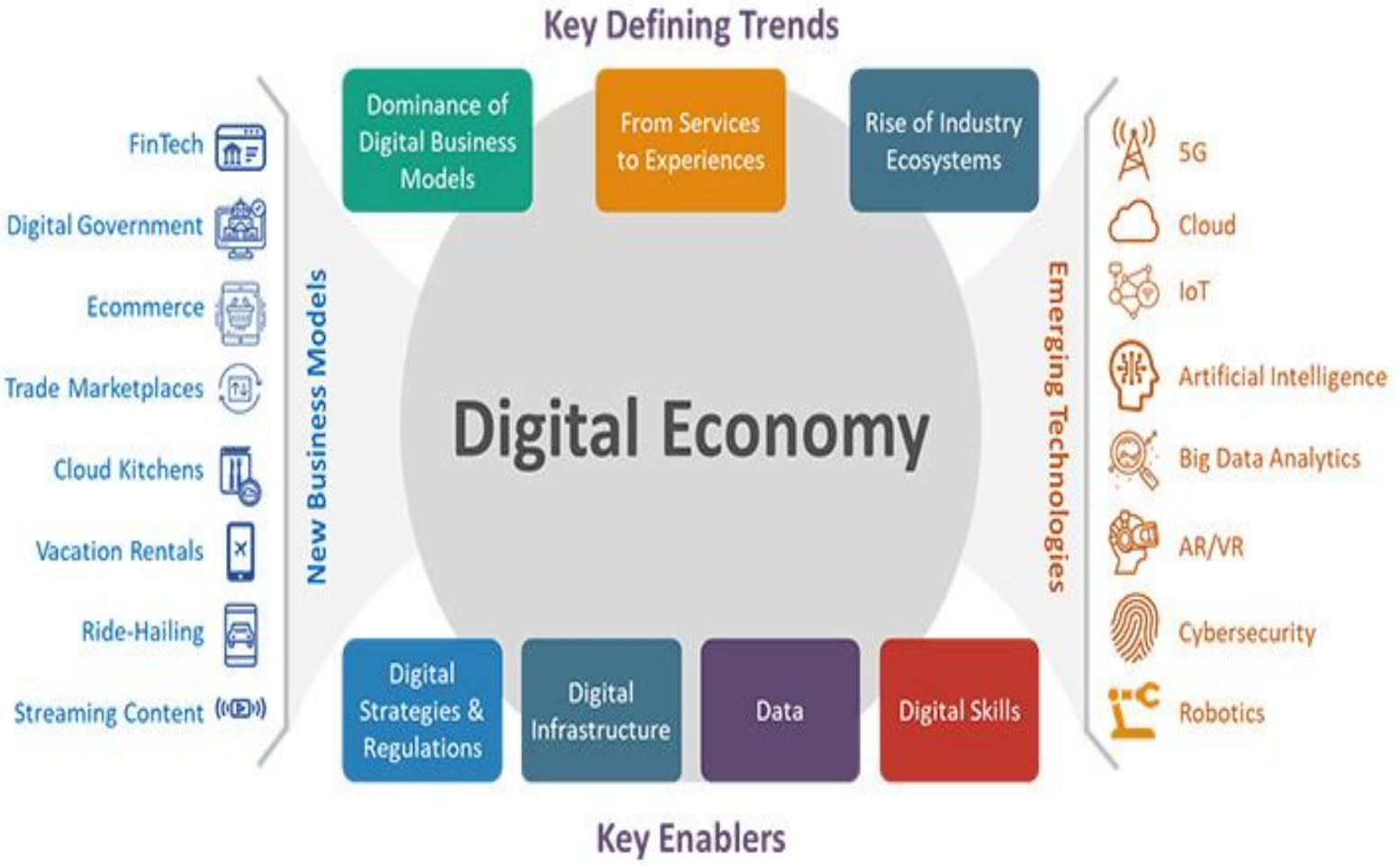
# Cyber Security Skill and Platforms

**Digital Service Delivery Platforms:** Developing user-friendly online platforms and portals for delivering government services and engaging with citizens digitally, enhancing efficiency and accessibility.

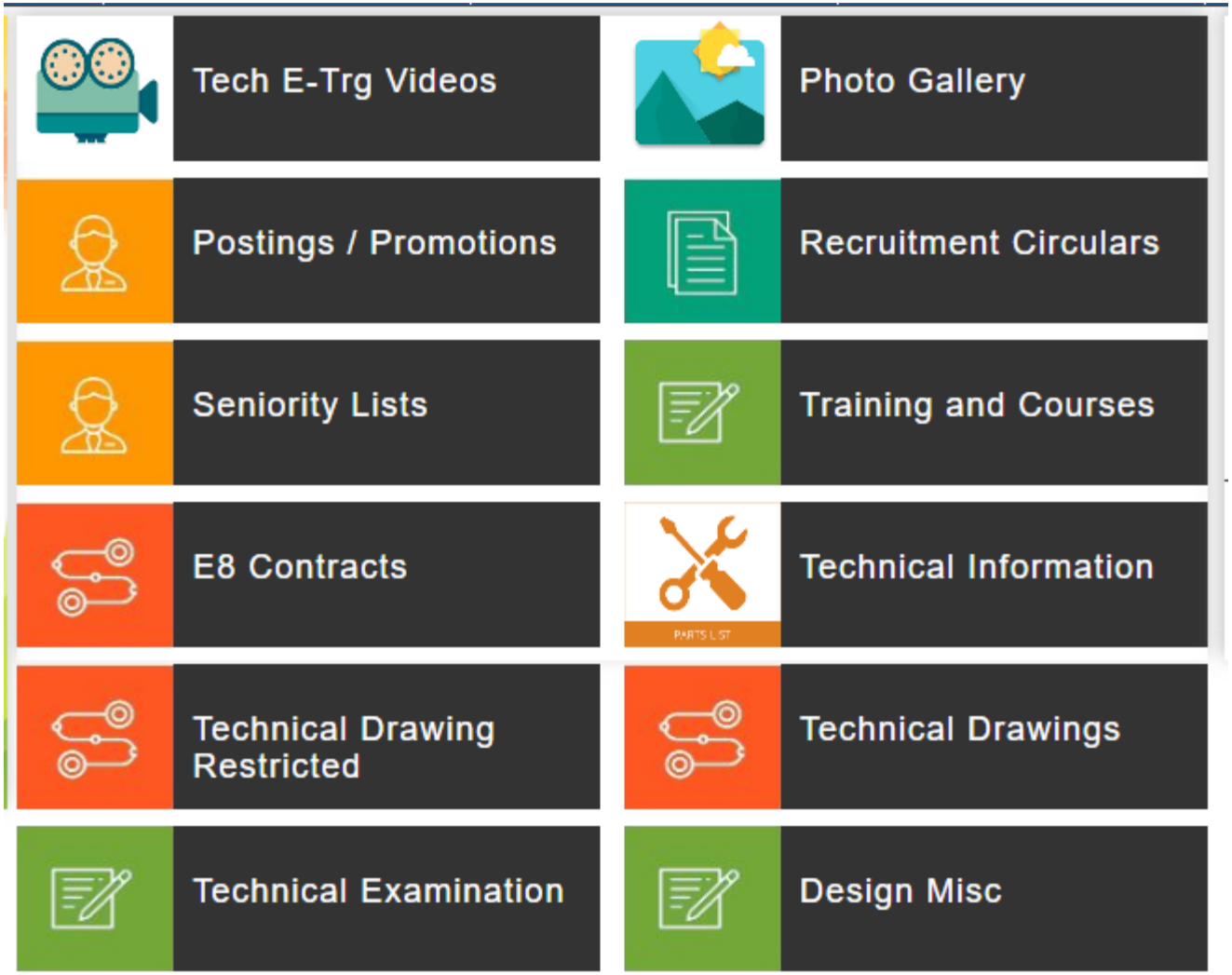
**Interoperability Standards:** Establishing standards and protocols to ensure compatibility and seamless integration between different digital systems and services, enabling data sharing and interoperability.

**Digital Literacy and Skills Development:** Promoting digital literacy and skills development initiatives to empower citizens to effectively use digital technologies and participate in the digital economy.

# Cyber and Emerging Technologies

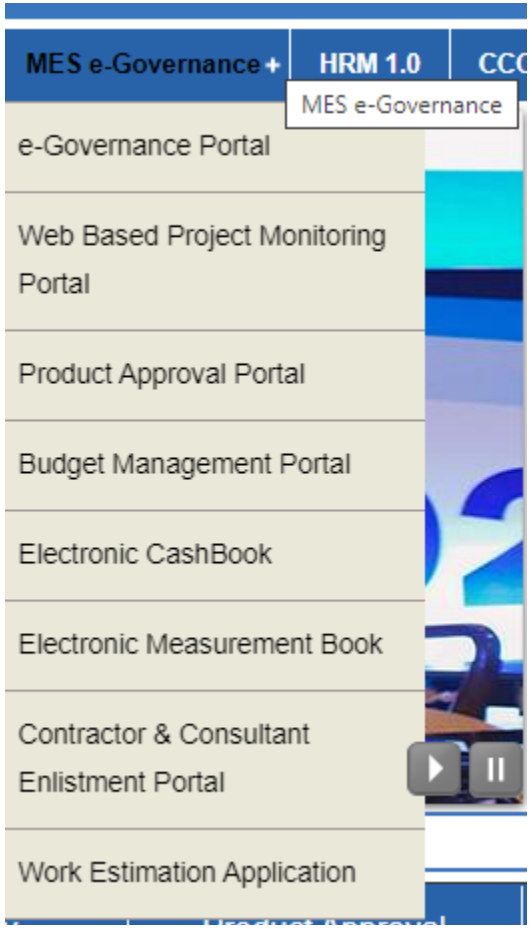


# Digital Assets - MES

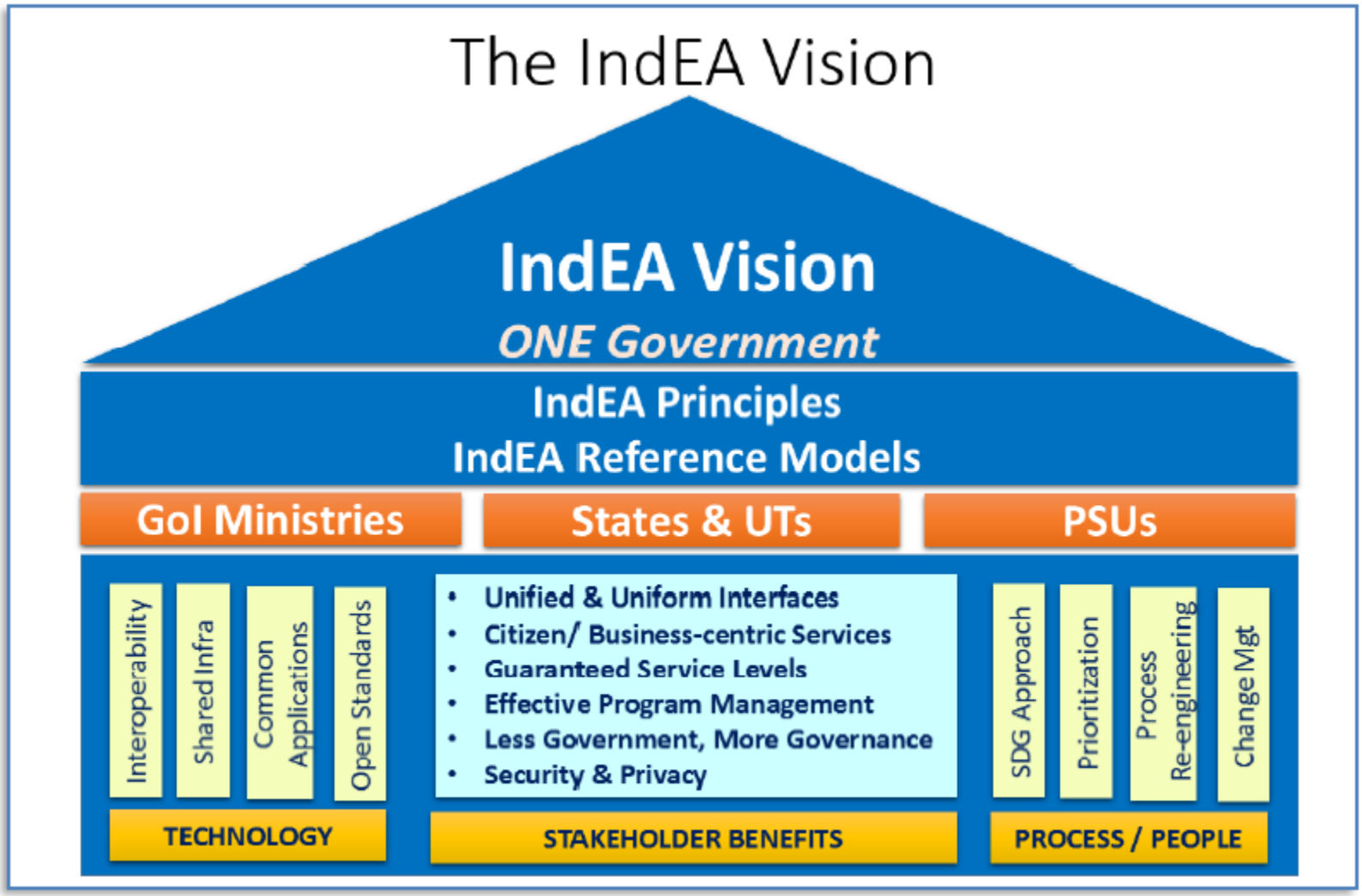


# MES - eGov

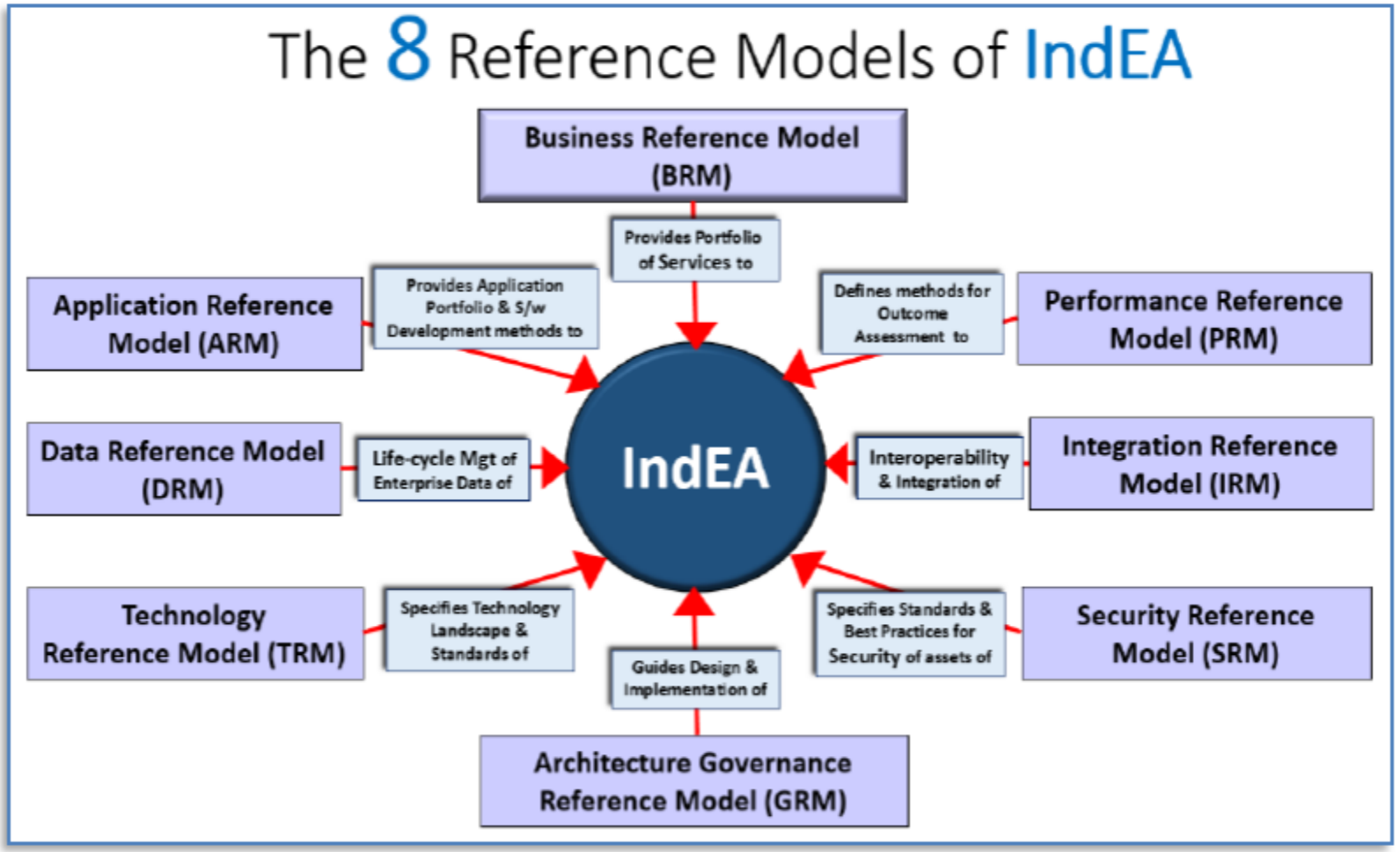
**MES - eGov**



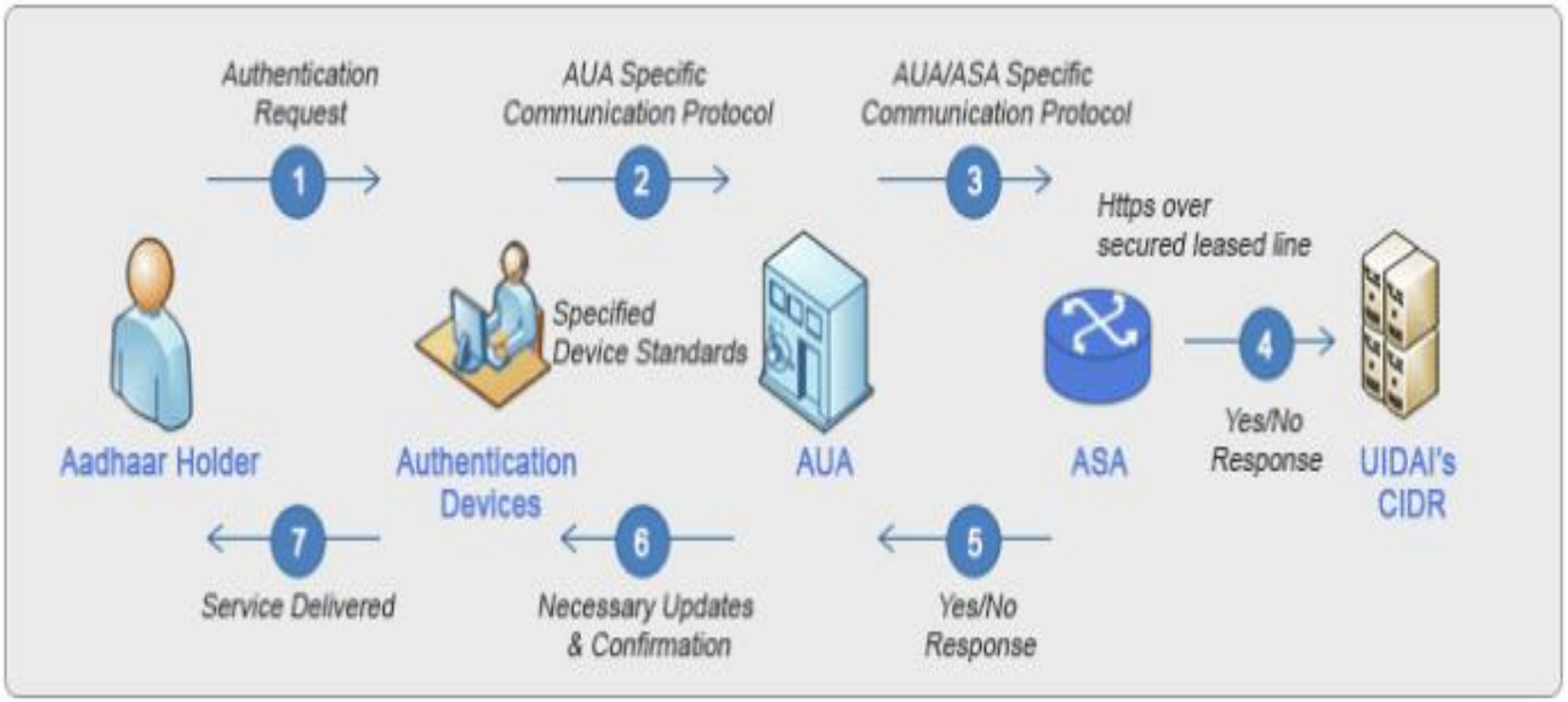
# IndEA


The IndEA Vision
IndEA Vision
ONE Government
IndEA Principles
IndEA Reference Models
GoI Ministries
States & UTs
PSUs
Interoperability
Shared Infra
Common Applications
Open Standards
TECHNOLOGY
Unified & Uniform Interfaces
Citizen/ Business-centric Services
Guaranteed Service Levels
Effective Program Management
Less Government, More Governance
Security & Privacy
STAKEHOLDER BENEFITS
SDG Approach
Prioritization
Process Re-engineering
Change Mgt
PROCESS / PEOPLE

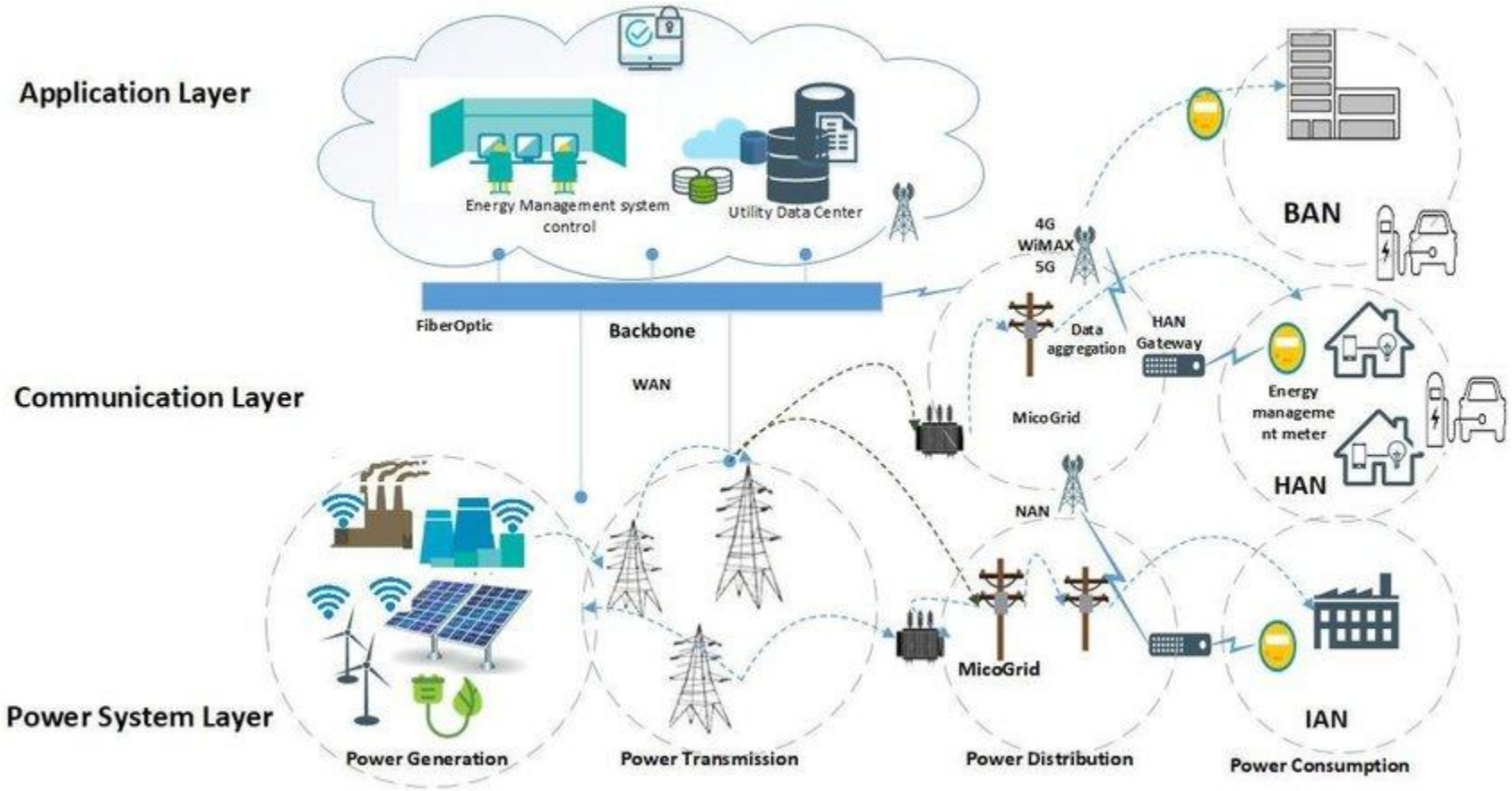
# IndEA Reference Models



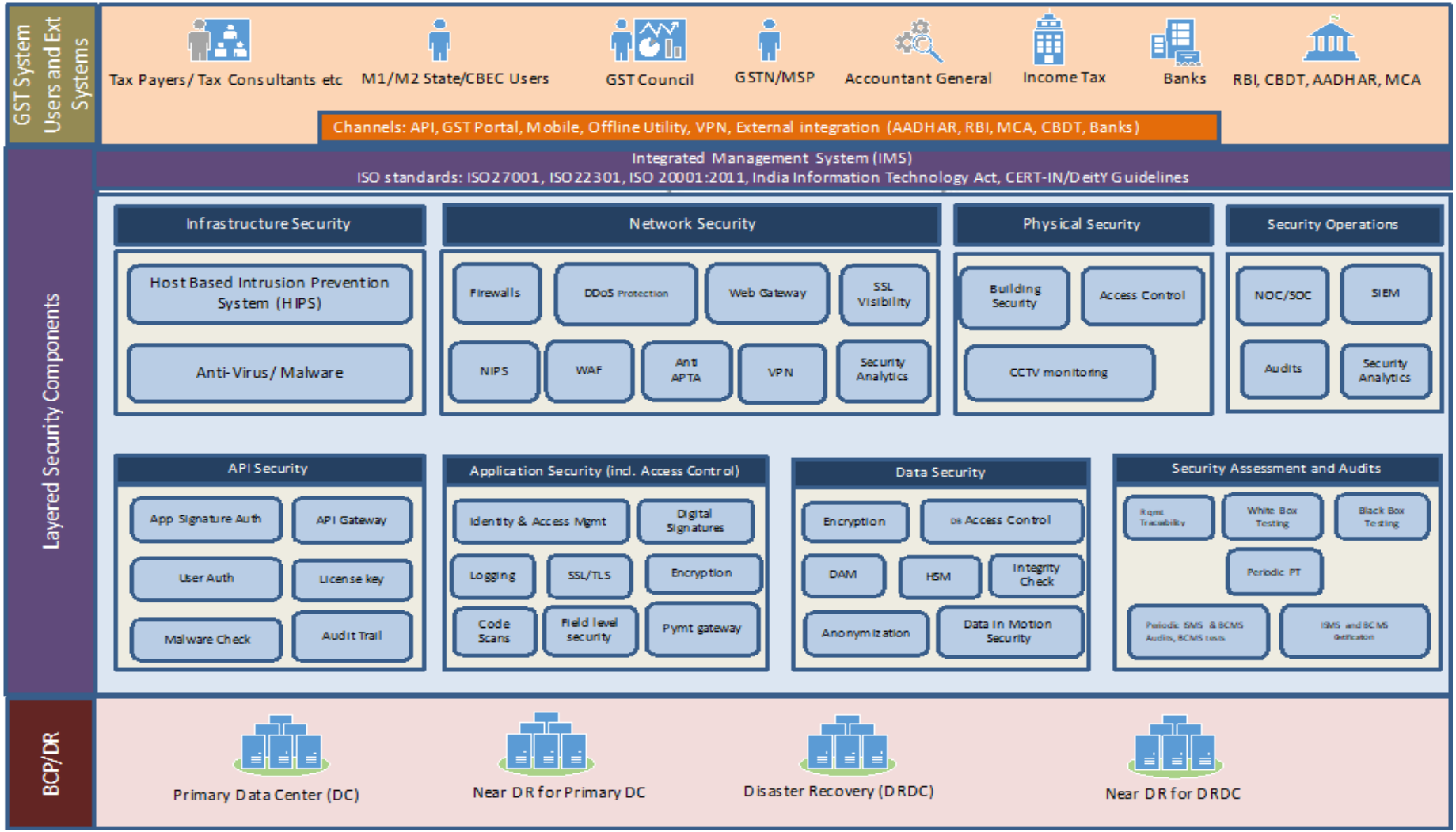
# UIDAI - Authentication



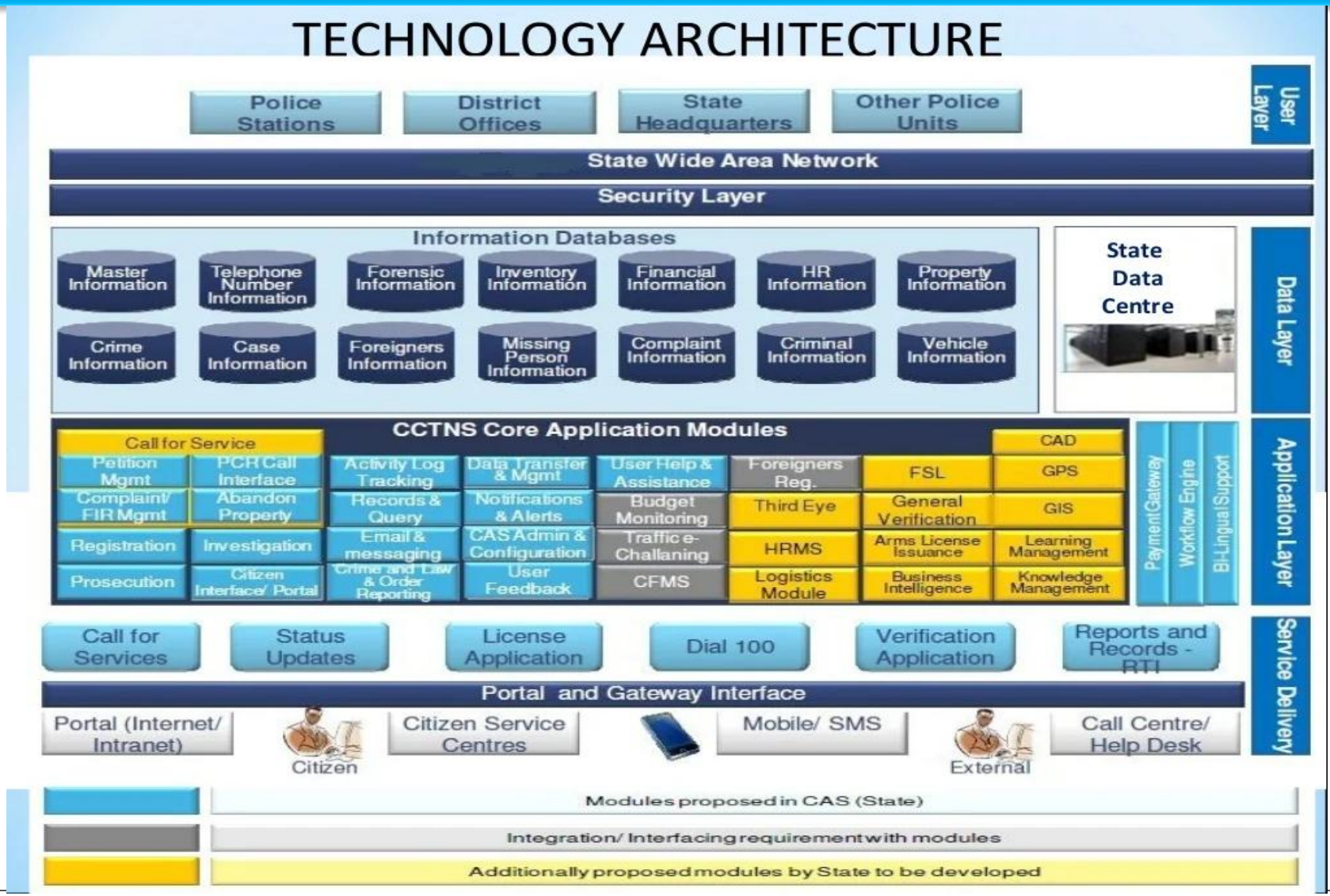
# Digital Smart Grids



# GSTN System

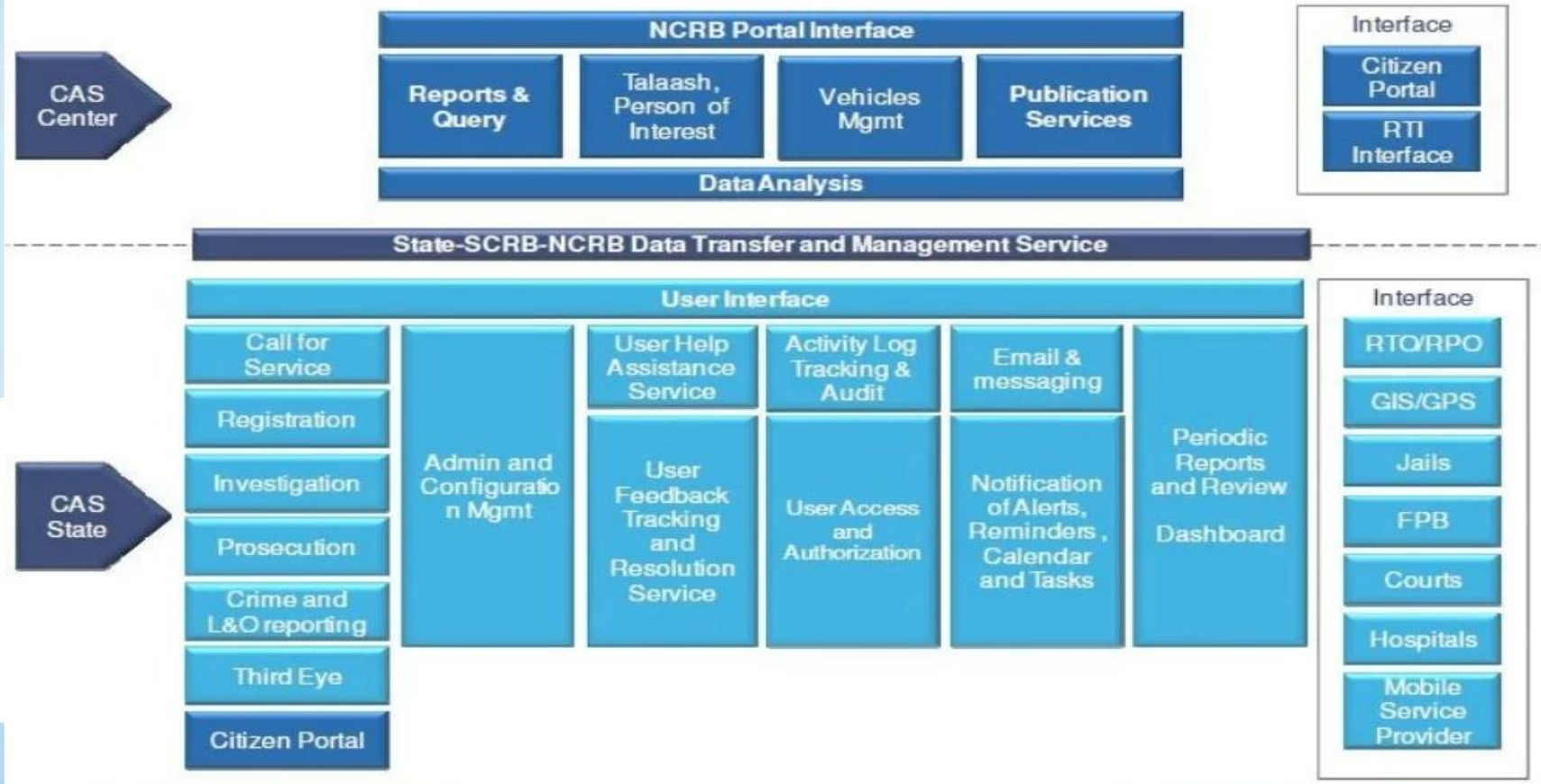

GST System Users and Ext Systems
Tax Payers/ Tax Consultants etc
M1/M2 State/CBEC Users
GST Council
GSTN/MSP
Accountant General
Income Tax
Banks
RBI, CBDT, AADHAR, MCA
Channels: API, GST Portal, Mobile, Offline Utility, VPN, External integration (AADHAR, RBI, MCA, CBDT, Banks)
Layered Security Components
Integrated Management System (IMS)
ISO standards: ISO27001, ISO22301, ISO 20001:2011, India Information Technology Act, CERT-IN/DeitY Guidelines
Infrastructure Security
Host Based Intrusion Prevention System (HIPS)
Anti-Virus/ Malware
Network Security
Firewalls
DDoS Protection
Web Gateway
SSL Visibility
NIPS
WAF
Anti APTA
VPN
Security Analytics
Physical Security
Building Security
Access Control
CCTV monitoring
Security Operations
NOC/SOC
SIEM
Audits
Security Analytics
API Security
App Signature Auth
API Gateway
User Auth
License key
Malware Check
Audit Trail
Application Security (incl. Access Control)
Identity & Access Mgmt
Digital Signatures
Logging
SSL/TLS
Encryption
Code Scans
Field level security
Pymt gateway
Data Security
Encryption
DB Access Control
DAM
HSM
Integrity Check
Anonymization
Data In Motion Security
Security Assessment and Audits
Rqmt Traceability
White Box Testing
Black Box Testing
Periodic PT
Periodic ISMS & BCMS Audits, BCMS tests
ISMS and BCMS Certification
BCP/DR
Primary Data Center (DC)
Near DR for Primary DC
Disaster Recovery (DRDC)
Near DR for DRDC

# CCTNS

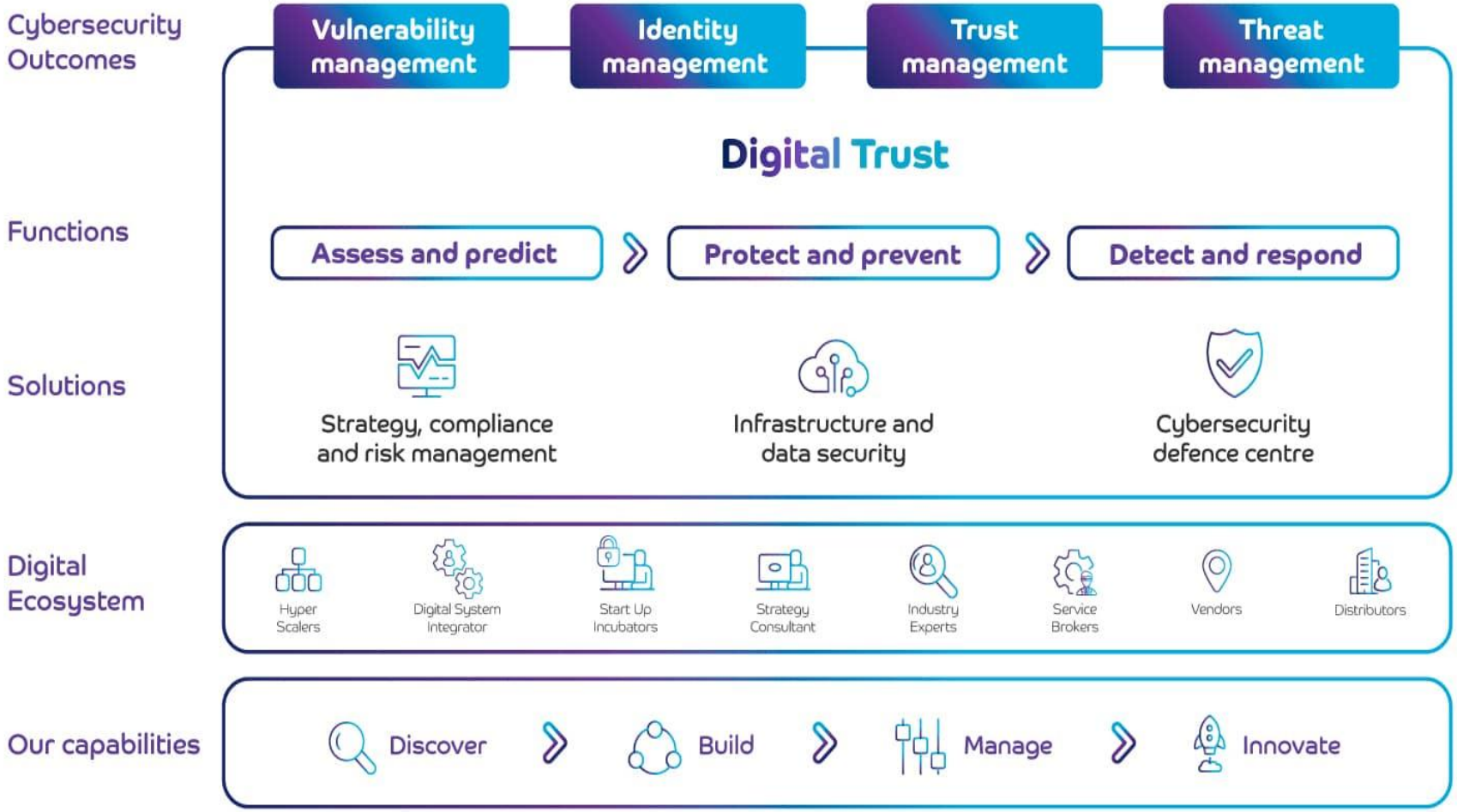

TECHNOLOGY ARCHITECTURE
Police Stations
District Offices
State Headquarters
Other Police Units
User Layer
State Wide Area Network
Security Layer
Information Databases
Master Information
Telephone Number Information
Forensic Information
Inventory Information
Financial Information
HR Information
Property Information
Crime Information
Case Information
Foreigners Information
Missing Person Information
Complaint Information
Criminal Information
Vehicle Information
State Data Centre
Data Layer
CCTNS Core Application Modules
Call for Service
Petition Mgmt
PCR Call Interface
Complaint/ FIR Mgmt
Abandon Property
Registration
Investigation
Prosecution
Citizen Interface/ Portal
Activity Log Tracking
Records & Query
Email & messaging
Crime and Law & Order Reporting
Data Transfer & Mgmt
Notifications & Alerts
CAS Admin & Configuration
User Feedback
User Help & Assistance
Budget Monitoring
Traffic e-Challaning
CFMS
Foreigners Reg.
Third Eye
HRMS
Logistics Module
FSL
General Verification
Arms License Issuance
Business Intelligence
CAD
GPS
GIS
Learning Management
Knowledge Management
PaymentGateway
Workflow Engine
BI and Reporting
Application Layer
Call for Services
Status Updates
License Application
Dial 100
Verification Application
Reports and Records - RTI
Service Delivery
Portal and Gateway Interface
Portal (Internet/ Intranet)
Citizen
Citizen Service Centres
Mobile/ SMS
External
Call Centre/ Help Desk
Modules proposed in CAS (State)
Integration/ Interfacing requirement with modules
Additionally proposed modules by State to be developed

# CCTNS

## INTEGRATION AND INTERFACING REQUIREMENTS



# DPI for Economic Dev



CYBER SECURITY
MAJOR THREATS
PROTECTING
SAFE PRACTICE
Modification
Destruction
Curiosity
Money
Pornography
Slander
False Accusations
Websites
Insults
Teasing
Name Calling
Sexual Activities
Unauthorised Access
Revenge
Fake Account
Libel
IM
Lies
Rumors
Threats
Threats
Grooming
Disruption
from
Attention
committed for
Defamation
including
through
E-mails
Disclosure
Information & Devices
Fun
Identity Theft
Cyber Stalking
is
Repeated Harassment
Phone
Online Groups
Cyber Bullying
Online Predators
Harassments
Use/Misuse
Theft
Cyber Crime
include
Share
Changed
should be
do not
Morphing
E-Mail Bombing
Website Defacement
Spam
Piracy
Spyware
Virus
Scareware
uses
Social Engineering
Securely
save
Password
from
Malware
include
Ransomware
Websites Spoofing
Strong
shoud be
use
Hoax
Scam
Hacking
Worms
Firewall
means
Password
protect
use
Phishing
Trojans
Adware
E-mail Spoofing
Software
update
for
legal
Latest Browser
Copyright Violation
obtaining
through
Click jacking
Desktop/ Laptop
Content Filtering
in using
Before Discarding
Sensitive Information
Data
backup
Cyber Laws
WiFi
use
Friendship
Authorised Store
Phone Call
Tab Napping
no to
use & update
in
use
avoid
with
format
Pirated Software
secure
Internet
update
Browser Pluggins
Unknown People Online
Mobile Devices
download app from
use current/ updated
Antivirus
E-mail Tracer
use
Instant Messaging
Operating System
regular/ automatic
any
any
check
never visit
Untrusted Website
avoid
do not accept
use
access only
like
Social Media
Threats
Auto Lock
Scan
URL
Meeting in Person
Call from Weired Number
Password
avoid
do not share
inform
beware of
do not open
avoid
record
Authorised WiFi
Strangers
Parents
clean
switch on
User Name
use
ensure
do not
Spy Camera
E-mail Attachments
Referral Links
and do not
Call back
IMEI Number
Personal Informtion
approach
save
from
only
Credit Card Details
Be Scared
instead
Privacy Options
Security Options
User to be Old Enough
Cyber Police
Chat Screen
browser's cookies and cache
Unknown Persons
Type the URL
Bluetooth
When Needed
CC:BY:SA-M.U.Paily

# MES - Responsibilities

**Construction and Infrastructure Development:** MES undertakes the planning, design, and construction of various military infrastructure projects such as airfields, barracks, training facilities, storage depots, roads, bridges, and other essential structures to support military operations.

**Facility Maintenance and Repair:** MES is responsible for the ongoing maintenance, repair, and renovation of military facilities to ensure they remain operational and in optimal condition. This includes repairing damages caused by natural disasters, accidents, or wear and tear.

**Logistics Support:** MES provides logistical support to the military by managing engineering equipment, supplies, and resources necessary for construction and infrastructure projects. This includes transportation, procurement, and distribution of materials and equipment.

# MES - Responsibilities

**Environmental Engineering:** MES may also be involved in environmental engineering activities such as waste management, pollution control, and environmental remediation to mitigate the environmental impact of military operations and facilities.

**Combat Engineering:** In addition to construction and infrastructure tasks, MES personnel may be trained in combat engineering skills such as fortification, demolition, mine clearance, and bridging to support military operations in combat zones.

**Disaster Response and Humanitarian Assistance:** MES units often play a crucial role in disaster response and humanitarian assistance missions by providing engineering support for disaster relief efforts, including search and rescue operations, temporary shelter construction, and infrastructure restoration.

# MES - Responsibilities

**Technical Advisory Services:** MES personnel may provide technical advice and expertise to military commanders and government agencies on engineering matters related to infrastructure development, construction projects, and environmental management.

The Military Engineering Service plays a vital role in supporting the operational readiness and effectiveness of the armed forces by ensuring they have the necessary infrastructure and engineering capabilities to carry out their missions effectively, both in peacetime and during conflicts or emergencies.

DPI implementation within MES can improve efficiency, effectiveness, and transparency in various aspects of military engineering operations.

# DPI in MES

**Digital Design and Planning:** MES can utilize advanced digital tools and software for architectural design, engineering planning, and project management. Computer-aided design (CAD) software, Building Information Modeling (BIM), and Geographic Information Systems (GIS) can facilitate the creation of detailed plans for military infrastructure projects, enhancing accuracy and efficiency in the design phase.

**Integrated Project Management Systems:** Implementing digital project management systems allows MES to streamline project scheduling, resource allocation, and progress tracking. Cloud-based project management platforms enable real-time collaboration among team members, contractors, and stakeholders, improving communication and coordination in construction projects.

**Asset Management and Maintenance:** DPI solutions can be used for asset management and maintenance of military infrastructure facilities. Utilizing digital asset management systems, MES can track the condition, maintenance history, and lifecycle of assets such as buildings, roads, and utilities, enabling proactive maintenance and optimizing asset utilization.

# DPI in MES

**Remote Monitoring and Surveillance:** MES can deploy digital sensors, cameras, and monitoring systems to remotely monitor critical infrastructure assets and detect potential issues or security threats. Remote surveillance technologies enhance situational awareness and security, allowing MES to respond promptly to incidents and vulnerabilities.

**Geospatial Intelligence (GEOINT):** Leveraging geospatial intelligence capabilities, MES can analyze terrain data, satellite imagery, and geographical information to inform decision-making in infrastructure planning, route optimization, and site selection for military installations and operations.

**Cybersecurity and Information Assurance:** Given the sensitive nature of military engineering operations, DPI implementation includes robust cybersecurity measures to safeguard digital infrastructure, data, and communication networks against cyber threats. Secure network architecture, encryption protocols, and intrusion detection systems are essential components of MES's cybersecurity framework.

# DPI in MES

**Digital Training and Skills Development:** MES personnel can undergo training programs focused on digital tools, technologies, and best practices relevant to military engineering operations. Digital training modules, simulations, and virtual reality environments enhance the proficiency and readiness of MES personnel in utilizing DPI solutions effectively.

Integrating Digital Public Infrastructure into the Military Engineering Service enhances its capabilities in planning, executing, and maintaining military infrastructure projects, ultimately contributing to the readiness and effectiveness of the armed forces.

# Thank you

Srinivas.bhoosarapu@gmail.com
9154035731