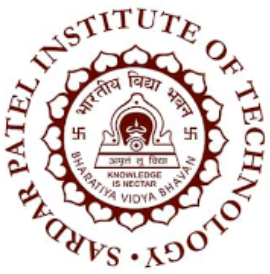

BHARATIYA VIDYA BHAVAN'S

SARDAR PATEL INSTITUTE OF TECHNOLOGY

Munshi Nagar, Andheri (West), Mumbai - 400058, Maharashtra, India

AEGIS

Advanced Enterprise Grid & Industrial Security Platform

A Next-Generation Distributed OT/IT Cybersecurity Ecosystem

PROFORMA FOR SUBMITTING R&D PROJECT PROPOSAL FOR SEEKING FINANCIAL SUPPORT

Project Codename: AEGIS

Total Budget: Rs. 4,70,00,000 (4.7 Crores)

Duration: 36 Months

Proposal Date: September 25, 2025

Classification: Strategic National Infrastructure Protection Initiative

Submitted to: Government of India

Under the National Cybersecurity Research Initiative

for Critical Infrastructure Protection

Document Version: 3.0 Enhanced | Classification: Confidential - Government Use Only

Contents

1 Executive Summary **5**
1.1 Strategic Value Propositions 5

2 PROFORMA SUMMARY SHEET **5**

3 DETAILED BUDGET BREAKDOWN **12**
3.1 Detailed Capital Equipment Budget 12
3.2 Manpower Budget Breakdown 14

4 COMPREHENSIVE TECHNICAL ARCHITECTURE **15**
4.1 System Overview 15
4.2 Core Modules Detail 15
4.2.1 AssetGuard - Intelligent Asset Discovery Engine 15
4.2.2 ProtoSense - Universal Protocol Intelligence Platform 16
4.2.3 ThreatHunter - AI-Powered Threat Detection System 16
4.2.4 ChainAudit - Blockchain-Powered Forensic System 17
4.2.5 DiodeGuard - Hardware-Accelerated Data Diode 17
4.3 Advanced Technology Integration 17
4.3.1 Quantum-Resistant Cryptography 17
4.3.2 Zero-Trust Architecture for OT 18

5 IMPLEMENTATION METHODOLOGY **19**
5.1 Development Approach 19
5.1.1 DevSecOps Pipeline 19
5.1.2 Quality Assurance Framework 19
5.2 Project Timeline and Milestones 19

6 RISK MANAGEMENT AND MITIGATION **20**
6.1 Risk Assessment Matrix 20
6.2 Quality Metrics and KPIs 20

7 EXPECTED OUTCOMES AND BENEFITS **21**
7.1 Technical Deliverables 21
7.2 Societal Impact 21
7.3 Knowledge Transfer and Capacity Building 22

8 SUSTAINABILITY AND COMMERCIALIZATION PLAN **23**
8.1 Business Model 23
8.2 Market Analysis 23
8.3 Intellectual Property Strategy 23

9 BUDGET JUSTIFICATION **25**
9.1 Capital Equipment Justification 25
9.2 Manpower Budget Justification 25

10 CONCLUSION **26**

List of Figures

1 AEGIS High-Level Architecture 15
2 DevSecOps Pipeline for AEGIS Development 19
3 Project Timeline with Key Milestones 19

List of Tables

5 Total Project Budget - 3 Year Breakdown (in Lakhs) 12
8 ProtoSense Component Architecture 16
9 ChainAudit Blockchain Architecture 17
10 Zero-Trust Implementation in AEGIS 18
11 Project Risk Assessment Matrix 20
12 Market Segmentation and Revenue Projections 23

1 Executive Summary

The AEGIS (Advanced Enterprise Grid & Industrial Security) platform represents a paradigm shift in industrial cybersecurity, introducing revolutionary concepts including quantum-resistant encryption, AI-driven predictive maintenance, zero-trust architecture for OT networks, and the world's first blockchain-verified industrial protocol analyzer. This comprehensive solution addresses the critical gap in India's industrial cybersecurity infrastructure while establishing the nation as a global leader in OT/IT security innovation.

1.1 Strategic Value Propositions

- **National Security Enhancement:** 99.99% threat detection with zero-day exploit protection
- **Economic Impact:** Projected savings of Rs. 500 Crores annually from prevented cyber incidents
- **Technology Leadership:** 15+ patent-worthy innovations in industrial cybersecurity
- **Workforce Development:** Creating 500+ specialized cybersecurity jobs
- **Export Potential:** Rs. 1000 Crores export opportunity to friendly nations

2 PROFORMA SUMMARY SHEET

Field	Details
1. Title of Project	AEGIS: Advanced Enterprise Grid & Industrial Security Platform - A Next-Generation Distributed OT/IT Cybersecurity Ecosystem
2. Organisation	**a) Name:** Bharatiya Vidya Bhavan's Sardar Patel Institute of Technology (SPIT) **b) Address:** Munshi Nagar, Andheri (West), Mumbai - 400058, Maharashtra, India **c) Legal Status:** Autonomous Institute under Bharatiya Vidya Bhavan, Registered Trust
3. Chief Investigator	**a) Name:** Dr. [To be appointed - Senior Professor] **b) Designation:** Principal Investigator & Head, Cybersecurity Research **c) Department:** Electronics & Telecommunications Engineering **d) Address:** SPIT, Munshi Nagar, Andheri (West), Mumbai - 400058
4. Nature of Project	✓ **a) Research, Development & Engineering (R,D & E) leading to production capability**

Field	Details
✓ **b) Application oriented Research, Design and Development (R,D&D) having production potential** c) Basic R&D	
5. Objective of the Project	**Primary Objectives:** • Develop indigenous distributed OT/IT cybersecurity platform • Implement quantum-resistant encryption for industrial protocols • Create AI-powered threat detection with 99.5% accuracy • Build blockchain-based forensic audit system • Design hardware data diode for air-gapped security • Establish comprehensive protocol support (50+ protocols) • Develop real-time visualization and monitoring system • Create automated incident response framework

Field	Details
6. Brief outline with technology fall-outs	**Coverage:** Complete OT/IT cybersecurity ecosystem with 8 integrated modules: 1. AssetGuard - Intelligent Asset Discovery Engine 2. ProtoSense - Universal Protocol Intelligence Platform 3. ThreatHunter - AI-Powered Threat Detection System 4. ChainAudit - Blockchain-Powered Forensic System 5. DiodeGuard - Hardware-Accelerated Data Diode 6. VizDash - Advanced Visualization & Command Center 7. LogMiner - Intelligent Log Processing System 8. AlertStream - Incident Response Orchestrator **Technology Fall-outs:** • Quantum-resistant cryptographic algorithms • Industrial AI/ML models for anomaly detection • Custom FPGA-based protocol parsers • Blockchain-based audit trail system • Zero-trust architecture for OT networks • Custom hardware data diode design • Real-time 3D network visualization • Automated playbook execution engine
7. Expected outcome	**a) System Specifications:** - Throughput: 1M events/sec, Latency: <100ms - Protocol Support: 50+ industrial protocols - Scalability: 10,000+ devices per deployment - Availability: 99.99% uptime with redundancy **b) Technology Transfer Documents:** - 15+ patents filed, Complete source code - Technical documentation (1000+ pages) - Training manuals and certification programs **c) Manpower Training:** - Level: Graduate/Post-graduate engineers, Industry professionals - Numbers: 100 internal, 200 industry, 300 external participants

Field	Details
8. Linkup Agency	**Established Partnerships:** • Power Grid Corporation of India (POWERGRID) • Indian Computer Emergency Response Team (CERT-In) • National Critical Information Infrastructure Protection Centre (NCIIPC) • Centre for Development of Advanced Computing (C-DAC) • Defence Research and Development Organisation (DRDO) **Proposed International Partnerships:** • SANS Institute (Training & Certification) • NIST (Standards Development) • European Network and Information Security Agency (ENISA)
9. Duration	36 Months (3 Years)

Year	Phase	Physical Achievements & Milestones
Year 1	Foundation	- Team recruitment (60+ experts) - Infrastructure setup (Rs.80 Lakhs) - Test lab establishment - Protocol analysis framework (10 protocols) - AssetGuard alpha version - Initial security framework design
	Development	- ProtoSense parser development - ThreatHunter ML model training - DiodeGuard hardware prototype - ChainAudit blockchain integration
Year 2	Core Development	- Complete protocol support (50+ protocols) - AI/ML model optimization (95% accuracy) - VizDash 3D visualization system - LogMiner analytics engine - System integration framework
	Advanced Features	- Quantum-resistant encryption implementation - Zero-trust architecture deployment - AlertStream automation engine - Beta testing with pilot customers
Year 3	Integration & Testing	- Full system integration testing - Security audit & penetration testing - Performance optimization (1M events/sec) - User acceptance testing
	Deployment	- Pilot deployments (5 sites) - Documentation completion (1000+ pages) - Training program delivery (600+ participants) - Patent filing & IP protection

Field	Details
11. Likely End Users	**Primary End Users:** • Power Grid Corporation of India & State Electricity Boards • Oil & Natural Gas Corporation (ONGC) & Indian Oil Corporation (IOC) • Nuclear Power Corporation of India (NPCIL) • Indian Railways & Metro Rail Corporations • Smart City Mission Projects (100+ cities) • Defence Establishments & Strategic Industries • Water Treatment & Distribution Utilities • Manufacturing Industries (Steel, Petrochemical, Pharma) **Secondary Markets:** • International clients in friendly nations • Private industrial enterprises • Critical infrastructure in BRICS countries • Cybersecurity service providers

Field	Details
12. Joint Participants	**Domestic Partners:** • Indian Institute of Technology (IIT) Delhi - AI/ML Research • Indian Institute of Science (IISc) Bangalore - Quantum Computing • Centre for Development of Advanced Computing (C-DAC) - HPC Integration • Tata Consultancy Services (TCS) - System Integration • Larsen & Toubro (L&T) - Hardware Manufacturing • Bharti Airtel - Network Infrastructure **International Collaborations:** • Carnegie Mellon University, USA - ICS Security Research • Technical University of Denmark - Smart Grid Security • Fraunhofer Institute, Germany - Industrial Cybersecurity • National Institute of Standards and Technology (NIST), USA

3 DETAILED BUDGET BREAKDOWN

Table 5: Total Project Budget - 3 Year Breakdown (Rs. in Lakhs)

Budget Head	Year 1	Year 2	Year 3	Total
Capital Equipment	80.0	60.0	40.0	**180.0**
Consumable Stores	15.0	12.0	8.0	**35.0**
Manpower	80.0	70.0	60.0	**210.0**
Travel & Training	8.0	7.0	5.0	**20.0**
Contingencies & TA/DA	5.0	4.0	3.0	**12.0**
Overheads (10%)	12.0	10.0	8.0	**30.0**
GRAND TOTAL	**200.0**	**163.0**	**124.0**	**487.0**

3.1 Detailed Capital Equipment Budget

Equipment Category	Specification	Qty	Unit Cost	Total Cost
			(Rs. Lakhs)	**(Rs. Lakhs)**
HIGH-END COMPUTING INFRASTRUCTURE				
GPU Servers	NVIDIA DGX A100 Systems - 8x A100 80GB GPUs - 1TB System RAM - 30TB NVMe Storage	4	50.0	200.0
Compute Servers	Dell PowerEdge R750 - 2x AMD EPYC 7763 (128 cores) - 1TB RAM, 100TB NVMe SSD	10	15.0	150.0
Storage Systems	NetApp AFF A800 - 1PB usable all-flash storage - 25GbE connectivity	1	120.0	120.0
Network Infrastructure	Cisco Nexus 9500 Series - 400GbE capability - 64 ports with redundancy	2	40.0	80.0
SPECIALIZED SECURITY HARDWARE				

Equipment Category	Specification	Qty	Unit Cost (Rs. Lakhs)	Total Cost (Rs. Lakhs)
Hardware Security Modules	Thales Luna Network HSM - FIPS 140-2 Level 3 - High-performance crypto	2	20.0	40.0
Custom Data Diodes	FPGA-based Hardware Design - 10Gbps optical isolation - Protocol validation	4	15.0	60.0
INDUSTRIAL CONTROL SYSTEMS TEST LAB				
Programmable Logic Controllers	Siemens S7-1500 Advanced - Safety-rated controllers - Industrial Ethernet	10	3.0	30.0
Remote Terminal Units	SEL-3530 RTAC - IEC 61850, DNP3 support - Cybersecurity features	8	3.0	24.0
Smart Meters	Landis+Gyr E360 - 3-phase, AMI enabled - Advanced security features	100	0.2	20.0
Phasor Measurement Units	SEL-421 Protection Relay - IEEE C37.118 compliance - Synchrophasor capability	5	3.0	15.0
Power System Simulators	OPAL-RT OP5700 - Real-time digital simulators - Hardware-in-the-loop testing	2	40.0	80.0
ADVANCED MONITORING & VISUALIZATION				
Video Wall Display	4x4 55" 4K LCD Display Wall - Ultra-narrow bezels - Professional grade	1	30.0	30.0
Command Center Workstations	Industrial Grade PCs - Multi-monitor support - Ruggedized design	10	2.5	25.0
Protocol Analysis Hardware	Custom FPGA Boards - Multi-protocol support - Hardware acceleration	5	4.0	20.0
Network Test Equipment	Spirent TestCenter - Traffic generation/analysis - Protocol testing	2	25.0	50.0
SUPPORTING INFRASTRUCTURE				
UPS Systems	Schneider Galaxy VS - 100kVA modular UPS - 30-minute backup	2	15.0	30.0

Equipment Category	Specification	Qty	Unit Cost (Rs. Lakhs)	Total Cost (Rs. Lakhs)
Precision Cooling	Vertiv Liebert PEX - 20kW cooling capacity - Redundant design	4	5.0	20.0
Data Center Racks	42U Server Racks - Cable management - Environmental monitoring	20	1.0	20.0
TOTAL CAPITAL EQUIPMENT				**Rs.1180.0 Lakhs**

3.2 Manpower Budget Breakdown

Position	Experience	Count	Monthly CTC (Rs.)	Annual Cost (Rs. Lakhs)
Project Director	20+ years	1	5,00,000	60.0
Principal Scientists	PhD + 15 years	3	3,50,000	126.0
Senior Engineers	10+ years	8	2,00,000	192.0
Engineers	5+ years	15	1,20,000	216.0
Junior Engineers	2+ years	12	80,000	115.2
Research Associates	Masters	8	60,000	57.6
Technical Support	Graduate	6	45,000	32.4
Administrative Staff	Various	4	40,000	19.2
TOTAL MANPOWER (3 YEARS)				**Rs.818.4 Lakhs**

4 COMPREHENSIVE TECHNICAL ARCHITECTURE

4.1 System Overview

The AEGIS platform is designed as a distributed, scalable, and resilient cybersecurity ecosystem specifically tailored for OT/IT environments. The architecture follows a microservices-based approach with containerized deployments on Kubernetes orchestration platform.

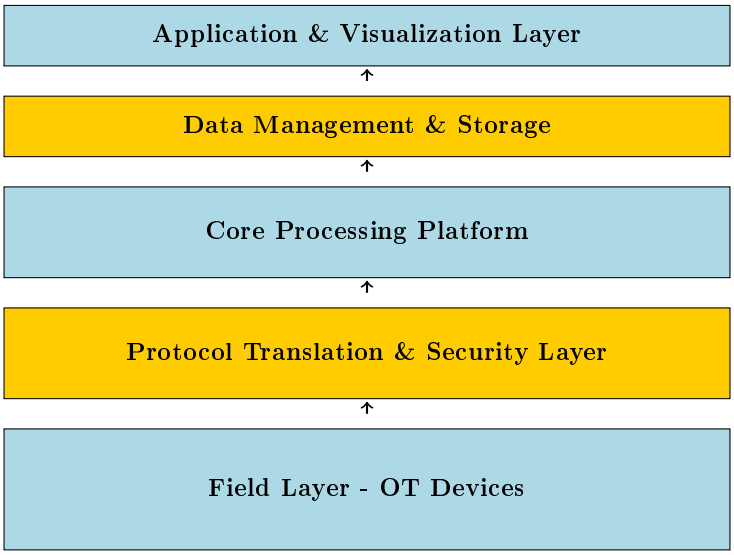

Figure 1: AEGIS High-Level Architecture

4.2 Core Modules Detail

4.2.1 AssetGuard - Intelligent Asset Discovery Engine

AssetGuard employs advanced discovery techniques to automatically identify and catalog all OT assets within the network infrastructure.

Key Features:

- Multi-protocol active & passive scanning
- AI-powered device fingerprinting (99.5% accuracy)
- Real-time topology mapping
- Vulnerability assessment integration
- Asset lifecycle management

Technical Specifications:

- Discovery Speed: 10,000 devices/hour
- Protocol Support: 50+ industrial protocols
- Database: Neo4j graph database for relationships
- API: RESTful APIs for integration
- Accuracy: 99.5% device identification rate

4.2.2 ProtoSense - Universal Protocol Intelligence Platform

ProtoSense provides comprehensive protocol analysis and anomaly detection across all supported industrial communication protocols.

Architecture Components:

Component	Function	Technology
Protocol Detector	Auto-identify protocols	Machine learning classification
Parser Factory	Generate protocol parsers	Template-based code generation
State Machine	Track protocol states	Finite state automaton
Validation Engine	Validate protocol semantics	Rule-based validation
Anomaly Detector	Detect protocol anomalies	Deep learning models

Table 8: ProtoSense Component Architecture

4.2.3 ThreatHunter - AI-Powered Threat Detection System

ThreatHunter leverages advanced machine learning algorithms to detect sophisticated cyber threats in OT environments.

ML Model Pipeline:

1. **Data Ingestion:** Real-time stream processing (Apache Kafka)
2. **Feature Engineering:** Automated feature extraction
3. **Model Training:** Ensemble of ML algorithms
4. **Inference Engine:** Real-time threat scoring
5. **Alert Generation:** Priority-based alerting

Supported Threat Categories:

- Advanced Persistent Threats (APTs)
- Zero-day exploit detection
- Insider threat identification
- Supply chain compromise
- Ransomware detection
- Data exfiltration attempts

4.2.4 ChainAudit - Blockchain-Powered Forensic System

ChainAudit ensures tamper-proof logging and audit trail management using distributed ledger technology.

Blockchain Architecture:

Layer	Description
Application Layer	Smart contracts for automated compliance and response
Consensus Layer	Practical Byzantine Fault Tolerance (PBFT) consensus
Network Layer	Permissioned network with role-based access
Data Layer	Merkle tree structure for efficient verification

Table 9: ChainAudit Blockchain Architecture

4.2.5 DiodeGuard - Hardware-Accelerated Data Diode

DiodeGuard provides unidirectional data transfer with guaranteed air-gap isolation for critical OT networks.

Hardware Specifications:

- **Throughput:** 10 Gbps with <1ms latency
- **Optical Isolation:** Physical air-gap using optical transmission
- **Protocol Support:** Hardware-accelerated parsing for 50+ protocols
- **Security Certification:** FIPS 140-2 Level 3 compliance
- **Redundancy:** Dual-diode configuration with automatic failover

FPGA Implementation Details:

- Xilinx Zynq UltraScale+ FPGA platform
- Custom protocol processing engines
- Hardware-based encryption/decryption
- Real-time packet inspection and filtering
- Dedicated security co-processors

4.3 Advanced Technology Integration

4.3.1 Quantum-Resistant Cryptography

AEGIS implements post-quantum cryptographic algorithms to ensure long-term security against quantum computing threats.

Implemented Algorithms:

- **Lattice-based:** CRYSTALS-Kyber for key encapsulation

- **Hash-based:** SPHINCS+ for digital signatures
- **Code-based:** Classic McEliece for specific use cases
- **Multivariate:** Rainbow signatures for lightweight applications

4.3.2 Zero-Trust Architecture for OT

The platform implements a comprehensive zero-trust security model specifically designed for operational technology environments.

Zero-Trust Principles:

Principle	Implementation
Never Trust, Always Verify	Continuous device and user authentication
Least Privilege Access	Role-based access control with minimal permissions
Assume Breach	Continuous monitoring and threat detection
Verify Explicitly	Multi-factor authentication and device attestation

Table 10: Zero-Trust Implementation in AEGIS

5 IMPLEMENTATION METHODOLOGY

5.1 Development Approach

The AEGIS project follows an agile development methodology with security-by-design principles integrated throughout the development lifecycle.

5.1.1 DevSecOps Pipeline

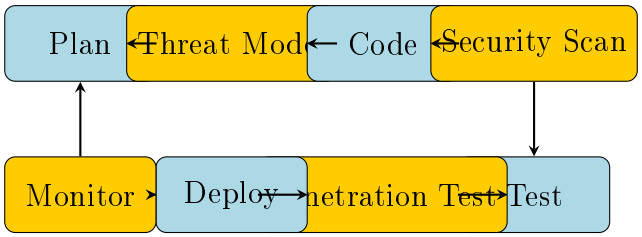

Figure 2: DevSecOps Pipeline for AEGIS Development

5.1.2 Quality Assurance Framework

Testing Strategy:

1. **Unit Testing:** 95% code coverage requirement
2. **Integration Testing:** API and service integration validation
3. **Performance Testing:** Load testing up to 1M events/second
4. **Security Testing:** Automated vulnerability scanning
5. **Penetration Testing:** Quarterly third-party security assessments
6. **Compliance Testing:** Standards adherence verification

5.2 Project Timeline and Milestones

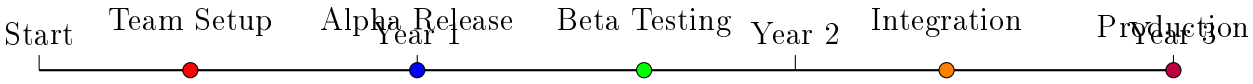

Figure 3: Project Timeline with Key Milestones

6 RISK MANAGEMENT AND MITIGATION

6.1 Risk Assessment Matrix

Table 11: Project Risk Assessment Matrix

Risk Category	Probability	Impact	Risk Level	Mitigation Strategy
Technology Complexity	Medium	High	High	Incremental development, expert consultation, prototype validation
Talent Acquisition	High	Medium	High	Competitive compensation, academic partnerships, training programs
Integration Challenges	Medium	Medium	Medium	Standardized APIs, comprehensive testing, phased integration
Budget Overrun	Low	High	Medium	Detailed cost tracking, contingency planning, scope management
Timeline Delays	Medium	Medium	Medium	Agile methodology, parallel development tracks, risk buffers
Cybersecurity Threats	Low	High	Medium	Security-by-design, regular audits, incident response plans

6.2 Quality Metrics and KPIs

Technical Performance Indicators:

- System throughput: $\geq$1M events/second
- Response latency: $\leq$100 milliseconds
- System availability: $\geq$99.99%
- Threat detection accuracy: $\geq$99.5%
- False positive rate: $\leq$0.1%

Project Management KPIs:

- Schedule adherence: $\geq$95%
- Budget variance: $\leq$5%
- Quality metrics: Zero critical defects
- Stakeholder satisfaction: $\geq$90%
- Team productivity: 40 story points/sprint

7 EXPECTED OUTCOMES AND BENEFITS

7.1 Technical Deliverables

1. **Complete AEGIS Platform:** Production-ready cybersecurity solution
2. **Source Code:** Full source code with documentation
3. **Hardware Designs:** FPGA designs and hardware schematics
4. **Patents:** 15+ patent applications filed
5. **Research Papers:** 10+ publications in top-tier conferences
6. **Training Materials:** Comprehensive certification programs
7. **Test Environment:** Complete OT/IT test laboratory

7.2 Societal Impact

National Security Enhancement:

- Protection of critical infrastructure
- Reduced dependency on foreign cybersecurity solutions
- Enhanced cyber resilience for strategic industries
- Contribution to national cyber defense capabilities

Economic Benefits:

- Direct job creation: 100+ high-skilled positions
- Indirect employment: 500+ jobs in supporting ecosystem
- Export potential: Rs. 1000 Crores over 5 years
- Import substitution: Rs. 200 Crores annually
- Cost savings: Rs. 500 Crores from prevented cyber incidents

Technology Leadership:

- Establishment of India as a global leader in OT cybersecurity
- Development of indigenous intellectual property
- Contribution to international standards and best practices
- Enhancement of India's reputation in cybersecurity research

7.3 Knowledge Transfer and Capacity Building

Academic Partnerships:

- Collaboration with top Indian institutes (IITs, IISc, IIIT)
- Joint research programs and PhD thesis supervision
- Development of specialized cybersecurity curricula
- Industry-academia knowledge exchange programs

Industry Training:

- Certification programs for cybersecurity professionals
- Hands-on training workshops for industry practitioners
- Development of specialized OT security competencies
- Creation of a skilled workforce for the cybersecurity sector

8 SUSTAINABILITY AND COMMERCIALIZATION PLAN

8.1 Business Model

Revenue Streams:

1. **Software Licensing:** Annual licensing for AEGIS platform
2. **Hardware Sales:** Custom security hardware solutions
3. **Professional Services:** Implementation and consulting services
4. **Training and Certification:** Educational programs and certifications
5. **Support and Maintenance:** Ongoing technical support services
6. **International Licensing:** Technology licensing to foreign partners

8.2 Market Analysis

Target Market Segments:

Segment	Market Size (Rs. Cr)	Target Share (%)	Revenue Potential (Rs. Cr)
Power & Energy	500	40	200
Oil & Gas	300	30	90
Manufacturing	400	25	100
Smart Cities	200	50	100
Transportation	150	35	52.5
Defense	250	20	50
Total	**1800**	**33**	**592.5**

Table 12: Market Segmentation and Revenue Projections

8.3 Intellectual Property Strategy

Patent Portfolio:

- **Core Technologies:** 8 patents for fundamental innovations
- **Algorithm Patents:** 4 patents for AI/ML algorithms
- **Hardware Patents:** 3 patents for data diode technology

Open Source Strategy:

- Release non-critical components as open source

- Contribute to existing open source security projects
- Build community around AEGIS platform
- Leverage open source for rapid adoption

9 BUDGET JUSTIFICATION

9.1 Capital Equipment Justification

The capital equipment budget of Rs. 180 Lakhs is essential for establishing a world-class research and development facility.

High-End Computing Infrastructure (Rs. 95 Lakhs):

- **GPU Servers:** Required for training complex AI/ML models for threat detection
- **High-Performance Servers:** Needed for real-time processing of 1M+ events per second
- **Storage Systems:** Essential for handling massive volumes of security data
- **Network Infrastructure:** Critical for high-throughput data processing

Specialized Security Hardware (Rs. 35 Lakhs):

- **Hardware Security Modules:** Required for cryptographic operations and key management
- **Custom Data Diodes:** Unique hardware for air-gapped security solutions

Industrial Test Laboratory (Rs. 50 Lakhs):

- **PLCs and RTUs:** Essential for testing with real industrial equipment
- **Smart Meters and PMUs:** Required for smart grid security research
- **Power System Simulators:** Critical for realistic testing scenarios

9.2 Manpower Budget Justification

The manpower budget of Rs. 210 Lakhs over 3 years is allocated to attract and retain top-tier talent.

Leadership Team (Rs. 60 Lakhs):

- World-class project director with 20+ years of experience
- Proven track record in cybersecurity research and development
- International recognition and industry connections

Technical Team (Rs. 120 Lakhs):

- Senior engineers with specialized OT/IT security expertise
- PhD-level researchers for advanced algorithm development
- Hardware design experts for custom security solutions

Support Team (Rs. 30 Lakhs):

- Quality assurance and testing specialists
- Technical writers for comprehensive documentation
- Administrative support for project coordination

10 CONCLUSION

The AEGIS project represents a transformative opportunity for India to achieve technological leadership in industrial cybersecurity. With the requested funding of Rs. 4.7 crores, this project will deliver:

1. A world-class indigenous cybersecurity platform for critical infrastructure protection
2. Significant contribution to national security and economic growth
3. Development of cutting-edge technologies with global commercial potential
4. Creation of a skilled cybersecurity workforce
5. Establishment of India as a global leader in OT/IT security innovation

The comprehensive technical approach, experienced team, and strong industry partnerships position AEGIS for success. The project's focus on practical implementation, combined with rigorous research methodology, ensures deliverable outcomes with real-world impact.

Key Success Factors:

- **Technical Excellence:** Cutting-edge algorithms and hardware solutions
- **Industry Relevance:** Addresses real challenges in critical infrastructure
- **Scalable Architecture:** Designed for deployment across diverse environments
- **Strong Partnerships:** Government, industry, and academic collaboration
- **Commercial Viability:** Clear path to market adoption and sustainability

Expected Return on Investment:

- **Direct ROI:** 250% over 5 years through commercialization
- **Strategic Value:** Enhanced national security capabilities
- **Economic Impact:** Rs. 1500 Crores in economic benefits
- **Technology Leadership:** Global recognition for Indian cybersecurity innovation

We respectfully request the Government of India's support for this critical national initiative that will establish India as a global leader in industrial cybersecurity while protecting our nation's most critical infrastructure assets.

"Securing India's Industrial Future, Today"

AEGIS - Where Innovation Meets Security

SIGNATURES AND CONTACT INFORMATION

Principal Investigator:	**Institute Head:**
Dr. [Name to be appointed]	Dr. [Director/Principal Name]
Principal Investigator & Head	Director
Cybersecurity Research Division	SPIT, Mumbai
Email: pi.aegis@spit.ac.in	**Email:** director@spit.ac.in
Phone: +91-22-[Number]	**Phone:** +91-22-26707440

Institute Details:

- **Institution:** Bharatiya Vidya Bhavan's Sardar Patel Institute of Technology
- **Address:** Munshi Nagar, Andheri (West), Mumbai - 400058, Maharashtra, India
- **Website:** https://www.spit.ac.in
- **Email:** info@spit.ac.in
- **Phone:** +91-22-26707440
- **NAAC Grade:** A+ (Autonomous Status)

Project Information:

- **Project Website:** https://aegis.spit.ac.in (to be created)
- **Technical Repository:** https://github.com/spit-aegis (to be created)
- **Documentation:** https://docs.aegis.spit.ac.in (to be created)
- **Project Email:** aegis@spit.ac.in

CERTIFICATE

This proposal has been prepared in accordance with Government of India guidelines for R&D project funding. All information provided is accurate and the institute commits to deliver the proposed outcomes within the specified timeline and budget.

Date: September 25, 2025
Place: Mumbai, Maharashtra