Fax:

Military College of Telecommunication Engineering, Mhow, Indore

MP – 453441

File No _____

May 2021

REQUEST FOR INFORMATION (RFI) FROM VENDORS FOR AUGMENTATION OF SAI MOBILE APPLICATION ECOSYSTEM

1. **Introduction**. An instantaneous mobile phone based messaging app named Secure Application for Internet (SAI) akin to various commercial application available on the internet has been developed by the Indian Army. The software application main emphasis is to provide an isolated messaging platform exclusively for the Indian Army with high emphasis on exclusivity (end to end encryption) and cyber security. The design of the software is proposed to be platform agnostic and can be used with authorized Android, iOS and compute devices. The application in its current form has been tested for functionality and is presently dply with approximately 18000 active users over the last one and half year. The end state desired is to have the application deployed on mobile devices of all Indian Army personal (approximately twenty lakh devices) located across India.

2. The SAI software application hosted in the National Informatics Center infrastructure under the Ministry of Electronics and Information Technology (MeitY), would need a team of dedicated software application developers to enable inclusion of additional features, ensure updates and patch management of the application along with mitigation of vulnerabilities as identified. Testing of the application by a CERT-India empaneled Red Team will also be covered in the project along with a dedicated in-house cyber security testing team in form of a Blue/ Purple Team. Moreover, to ensure a high level of cyber security protection a dedicated security overlay in form of a Security Operation Centre (SOC) is also envisaged. The SOC operating in a 24x7 mode will be entrusted with monitoring of the application cyber security posture in line with the industry standards and policies issued by Indian Army. **The aim of this Request for Information (RFI) is to identify companies in India who can provide converged management services in the field of application hosting/ development, application testing and a 24x7 managed security operation center for the SAI software**

MCTE
Date.....
MHOW (M. P)

application. Based on the responses received, a RFP will be formulated and tendering action as per the DPM will be undertaken.

3. This RFI consists of two parts as indicated below:-

a) **Part I.** The first part of the RFI incorporates operational characteristics and features that should be met by the vendor. Few important global standards and additional vendor requirements are also listed for compliance.

b) **Part II.** The second part of the RFI states the methodology of seeking response from the vendors. The project is planned on a turnkey basis and vendors compiling to partial requirements will not be considered for the same.

PART I

4. **Purpose.** The purpose of the Request for Information (RFI) is to gather information and come up with a robust and resilient info-infrastructure for development, deployment, testing, cyber security and 24x7 monitoring of the SAI mobile application. The information provided in the RFI will be used to determine the feasibility, scope, timeframe and approximate resource requirements for augmentation of SAI mobile application ecosystem. The SAI application will be hosted on the National Informatics Centre (NIC)'s national cloud. Meghraj – the cloud computing initiative of the Govt. of India. Major scope includes:-

a) Mobile Application Maintenance and Development (Android and iOS).
b) Application Testing (Load Testing/User Acceptance Testing (UAT)/ Vulnerability Assessment/ mitigation and Penetration Testing (VAPT))/ Integrated Application Security Testing (IAST).
c) Designing of security framework/guidelines and implementation.
    i. AAA (Authentication, Authorization, and Accounting)
    ii. Red Teaming to ensure cyber security
d) SOC services for monitoring of application.
e) Maintenance of backend infrastructure.
f) Software application life cycle management.

5. **Scope of Work.**

5.1 **Mobile Application development (Android and iOS)**

a) In delivery phase, the solution provider shall be responsible to deliver/publish the mobile application.
b) In delivery phase, the solution Provider shall also be responsible to hand over in writing all development components like source code, passwords, databases, text, graphics or any other relevant material.
c) Develop a training reference manual, training and change management Plan
d) SLA Monitoring and reporting plan
e) Exit Management Plan including transition management
f) Other deliverables include O&M Plan, Test Plan along with User Acceptance Test Plan, Training Plan, Exit Management & KT Plan and Security Matrix/Plan.
g) Source code
h) The present SAI application will be maintained and updated as requested by the Indian Army.

5.2 **Application Testing**

5.2.1 **Performance & Load Testing**

a) Testing workload profiles and test scenarios based on the various functional requirements should be defined. Application as well as system resource utilization parameters that need to be monitored and captured for each run also needs to be defined.
b) Successful bidder should perform the load testing of Project for multiple workload profiles, multiple scenarios, and user loads to handle the envisaged users of the system.
c) Different activities before load testing i.e. identification of work load profiles, scenarios, information capturing report formats, creation of testing scripts, infrastructure detailing and workload profile should be prepared before the start of actual load testing exercise.
d) Solution parameters needs to be tuned based on the analysis of the load testing reports. The tuning process could be iterative until the issues are closed. Multiple load runs needs to be executed for users to simulate different scenarios, such as peak load etc, load generation within the LAN, Load generation across WAN or mobile network simulator while introducing configurable latency/jitter/packet loss etc.
e) Should eliminate manual application/ user data manipulation and enable ease of creating data-driven tests/ analytics.

MCTE
Date.....
MHOW (M. P.)

f) Should identify root cause of performance issues at application or code level. Include code performance analysis to quickly pinpoint component-level bottlenecks. Slowest classes and methods, most frequently called methods, most costly (aggregate time spent for each method), response time variance etc.

g) Should be able to monitor various system components e.g. Server (OS, Web, Application & Database) Monitoring, Network (between Client & Server) Delay Monitoring, Network Devices (Firewall, Switch & Router) Monitoring during the load test without having to install any data capturing agents on the monitored servers/components.

h) Should correlate response times and system performance metrics to provide quick insights in to root cause of performance issues.

i) Reports on following parameters (but not limited to) such as transaction response time, transaction per second (Passed), user interface rendering time, transaction per second (Failed), web transaction breakdown graphs, hits per second, throughput, HTTP responses per Second, pages downloaded per second, system infrastructure performance metrics etc.

5.2.2 **User acceptance Testing (UAT)**

a) The user might appoint third party auditor to perform User Acceptance Testing

b) Compliance to user specified Acceptance Testing (UAT) test cases.

c) UAT to be carried out in the exact same environment/architecture that would be set up for production.

d) Successful bidder should fix bugs and issues raised during UAT and get approval on the fixes from Indian Army / designated third party auditor prior to production deployment of the application.

e) Changes in the application as an outcome of UAT shall not be considered as a Change Request.

f) UAT period will be discussed with the successful bidder.

5.2.3 **Vulnerability Assessment and Penetration Testing (VAPT)**

a) The service provider shall conduct vulnerability and penetration test internally and ratified by an external third party testing agency specified by the Indian Army. This testing would be undertaken at a pre-defined periodicity by the user.

b) Corrective action should be taken by the service provider immediately from the date of submission of the report.

c) Compliance review should be done within a month from the date of submission of the report.

d) Any non-compliance in the reports may lead to penalty clauses. The service provider needs to update the system in response to any adverse findings in the report, without any additional cost to the user. The user may also depute auditors to conduct security check/ vulnerability test/penetration test.

5.2.4 **Integrated Application Security Testing (IAST)**

a) INTEGRATION TESTING is defined as a type of testing where software modules are integrated logically and tested as a group. A typical software project consists of multiple software modules, coded by different programmers. The purpose of this level of testing is to expose defects in the interaction between these software modules when they are integrated.
b) IAST tools use a combination of static and dynamic analysis techniques. They can test whether known vulnerabilities in code are actually exploitable in the running application.

5.3 **Designing of security framework/guidelines and implementation**

5.3.1 **AAA (Authentication, Authorization and Accounting)**

a) Authentication, authorization, and accounting (AAA) framework should be design and deployed for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services.
b) Authentication: Solution should provide a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted. The process of authentication should be base on each user having a unique set of criteria for gaining access.
c) Authorization: A user must gain authorization for doing certain tasks. After logging into a system, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted.
d) Accounting: This can include the amount of system time or the amount of data a user has sent and/or received during a session. Accounting has to be carried out by logging of session statistics and usage information and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

5.3.2 **Captive Red Teaming to Ensure Cyber Security.** Red Team exercise should cover the following broad activities –

a) Recognizing Information security issues within the Client through this exercise.
b) Identification of misconfigured and unpatched devices to compromise the client network and to ex-filtrate the data.
c) Identification of possible weak points in physical and logical security of Data Center
d) Vulnerability Assessment, Verification and Recommended Solution to mitigate vulnerability in Local / remote networks (automated and manual).

MCTE
Date.....
MHOW (M. P)

e) Examining Client for weaknesses as through the eyes of an industrial spy or a competitor or attacker using following techniques –
   i. Reconnaissance
   ii. Enumeration
   iii. External Recon
   iv. Internal Recon
   v. Social Engineering Attacks (Spear phishing)
   vi. Password Cracking , and Bypassing Windows User Account Control (UAC)
   vii. PowerShell exploitation
   viii. Lateral Movement
   ix. Network Domination & Persistence
   x. Network Infrastructure Exploitation for cases such as Firewall bypass, Router testing/configuration, DNS footprinting, Proxy Servers, Vulnerability exploits, Configuration
   xi. Evasion & Obfuscation Techniques
   xii. Data Exfiltration
   xiii. Attacking Linux/Unix Environments
   xiv. Privilege Escalation
   xv. Virtualization Attacks
f) Web application compromise and exploitation – physical and Cloud
g) Internal application Security Testing through Red team exercise
h) Conduct simulated cyber-attacks on the client's infrastructure
i) Validate protections and monitoring around high-value systems
j) Blended, covert test that can encompass network testing, phishing, wireless, and physical attacks
k) Send email with malicious attachment to users
l) Compromise the machine assigned to Red Team using the inherent vulnerabilities
m) Perform privilege escalation to obtain root privileges
n) Create a C2 channel from the compromised machine to communicate outside the Core Client network
o) Scan the network to understand topology and restrictions
p) Lateral movement to other machines.
q) Pivoting and executing various attacks (Pass the hash, Kerberoasting, PowerShell, scripts)
r) Map the critical servers in the network
s) Attempting to compromise the critical servers and provide evidence
t) Bidder may use additional methodologies to penetrate the Client security

5.4 **SOC Services**

a) Vendor shall be responsible for provisioning, securing, monitoring and maintaining the hardware, network(s), and software that supports the infrastructure and present Virtual Machines (VMs) and IT resources to the user.

MCTE
Date .....
MHOW (M.P)

b) The Data Center Facility of the Vendor shall at minimum implement the security toolset: Security & Data Privacy (Data & Network Security including Anti-Virus, Virtual Firewall, Multi Factor Authentication, VPN, IPS, Log Analyzer / Syslog, SSL, DDoS Protection, HIDS/ NIDS, Rights Management, SIEM, Integrated Vulnerability Assessment, SOC, Private Virtual Zones, Data Privacy, Data Encryption, Authentication & Authorization, and Auditing & Accounting)
c) Vendor shall ensure that they meet the ever-evolving security requirements as specified by CERT-In (http://www.cert-in.org.in/) and other global agencies in this field.
d) Implement industry standard storage strategies and controls for securing data in the Storage Area Network so that clients are restricted to their allocated storage.
e) Ability to create non-production environments and segregate (in a different VLAN) nonproduction environments from the production environment such that the users of the environments are in separate networks.
f) Traffic between two different VLAN should pass through firewall with VPN control over the non-production/ testing environment.
g) Offerings should have built-in user-level controls and administrator logs for transparency and audit control.
h) Platform should be protected by fully managed Intrusion detection system using signature, protocol, and anomaly-based inspection, thus providing network intrusion detection monitoring.
i) Platform should provide Edge-to-Edge security, visibility and carrier-class threat management and remediation against security hazards like Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, botnets, etc
j) Vendor shall provide protection against network issues such as traffic and routing instability.
k) Access to the user provisioned servers on the Cloud should be through SSL VPN clients only
l) Vendor shall allow audits of all administrator activities performed by the user.
m) Maintain the security features described below, investigate incidents detected undertake corrective action, and report to the user, as appropriate.
n) Vendor shall provide consolidated view of the availability, integrity and consistency of the Web/App/DB tiers.
o) Vendor shall ensure that password policies adhere to security requirements as defined by CERT-IN.
p) Vendor shall meet and comply with all GoI IT Security Policies and all applicable GoI standards and guidelines, other Government-wide laws and regulations for protection and security of Information Technology.
q) Vendor shall generally and substantially and in good faith follow GoI guidelines and CERT In and MeiTY security guideline.

MCTE
Date.....
MHOW(M.P.)

r) Vendor has industry standard certifications (assessed by a Third Party Auditor) that verify compliance against the security requirements of the application document, SLA & MSA, results, relevant reports, certifications may be provided with evidence along with the mapping of the industry standard certification controls against the application document requirements.

s) Vendor shall allow the user's designated third party auditors to conduct activities to include control reviews that include but are not limited to operating system vulnerability scanning, web application scanning and database scanning of applicable systems that support the processing, transportation, storage, or security of the user's information. This includes the general support system infrastructure.

t) Vendor shall be responsible for mitigating all security risks found and continuous monitoring activities

u) All high-risk vulnerabilities must be mitigated on priority.

v) All moderate risk vulnerabilities must be mitigated as detected/ notified. Steps should be initiated to minimize users risk rating against the specific vulnerabilities.

w) The user reserves the right to conduct on-site inspections.

x) Vendor shall provide vulnerability scan reports from Web Application, Database, and Operating System Scans or the services for the user to run the vulnerability scan.

y) Vendor shall protect the user data, equipment, etc. by treating the information as sensitive.

z) Sensitive but unclassified information, data, and/or equipment shall only be disclosed to empaneled personnel from the user When no longer required, this information, data, and/or equipment shall be returned to the user control, destroyed, or held until otherwise directed by the user.

aa) Vendor shall allow the user logical and physical access to the Vendor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request.

bb) Automated audits shall include but are not limited to the following methods:

cc) Authenticated and unauthenticated operating system/network vulnerability scans.

dd) Authenticated and unauthenticated web application vulnerability scans

ee) Authenticated and unauthenticated database application vulnerability scans

ff) Automated scans shall be performed by the user designated third party auditors.

gg) Vendor chooses to run its own automated scans or audits, results from these scans may, at the user discretion, be accepted in lieu of the user performed vulnerability scans.

hh) All data functions and processing shall be performed within the boundaries of India

ii) Vendor shall have capability/ feature to define strong password policy and maintaining password complexity rules and shall also include the prohibition of changing of password/ PIN lengths and any authentication requirements.

jj) Vendor shall ensure that all the policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal.

kk) Complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.

MCTE
Date.....
MHOW (M. P.)

ll) Vendor shall ensure that all the policies and procedures are established and supporting processes and technical measures are implemented for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components to ensure the efficiency of implemented security controls.

5.5 **Hosting**

Scope of the project includes designing, implementing & maintenance of SAI software application hosted within MeitY, Government Community Clouds primary data center (DC). Bidders are also required to include aspect related to host the application with the MeitY infrastructure which would entail setup of Virtual envt, application installation, testing, addressing requirements of end user support in terms of application installation and use for a period of three years. The expected outcome from this project is in the implementation of software application Development (DEV), Quality Assurance (QAS) and Production Management (PRD) layers fully deployed on MeitY, Government Community Cloud infrastructure/ premises. The tasks associated with this scope are broadly classified into following sub categories:-

a) Environment preparation within MeitY cloud for hosting the application
b) Designing & Implementation of SAI software application within MeitY infrastructure.
c) Development and addition of features in the application
d) Testing and ensuring desired cyber security posture of the software application.
e) Provisioning of SOC including AAA functionalities.
f) User management and help desk.
g) Software life cycle management and component upgrade aligned to user specifications.

5.5.1 Preparation of Government Community Cloud Environment: -

Service provider to setup complete environment (Production, Quality & Development) on Government Community cloud to host the user environment, service provider will be required to perform the following technical tasks for the assigned areas.

a) Setup virtual private cloud with VM's designated for individual modules with entire production environment in high availability mode.
b) Individual VM's running respective App/DB instance should deliver the given as per the table given in section 3 Landscape.
c) High Availability to be configured for Production environment.
d) Different VLAN's to be created to segregate front ending servers and database servers.
e) Storage proposed for DC should support IOPs as required.
f) Service provider should propose firewall, load balancer & security solution to protect the VM's, Application, Database from any type of external attacks like Virus attack, DDOS attack, hacking attempt, etc.

MCTE
Date
MHOW (M. P)

5.5.2 Provisioning of SOC including AAA Functionalities: -

The security framework /guidelines and implementation of this SOC will include AAA (Authentication, Authorization and Accounting) that control access to resources enforces policies and audits uses AAA and its combined processes should carryout network management and cyber security by screening users and keeping track of the activity.

a) **Authentication**: The process of authentication should be based on each user having a unique set of criteria for gaining access user specified framework to be incorporated for this feature.
b) **Authorization:** The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted.
c) **Accounting**: Accounting has to be carried out by logging of session statistics and usage information and is used for authorization control, trend analysis, resource utilization, and capacity planning activities.

5.5.3 Post Implementation Support: -

Post implementation support will be provided to users for installing, operating and functional assistance. Following maintenance support is required to be provided by the shortlisted bidder at least for a period of three years.

(a) Software life cycle management.

(b) Component upgrade aligned to user specifications.

(c) Red and Blue Team based cyber security testing of the software application to identify any vulnerability in the application/ hosting environment.

6. **Vendor Parameters**. This RFI is limited to indigenous service providers and operators of India origin meeting the pre-requisites criteria.

a) Screening of RFIs shall be carried out as per Pre-Qualification criteria mentioned in the RFI document and based on verification of documents submitted.
b) All eligible agencies who fulfill the Pre-Qualification criteria shall be invited for a meeting and shall be provided a brief about project.
c) No Consortium is allowed.
d) The following will be the minimum Pre-Qualification Criteria (PQC). Responses not meeting the minimum PQC will be summarily rejected and will not be evaluated further.

MCTE Date MHOW (M. P)

Sr. No.	Point	Clause	Supporting Document
1.	Legal Entity	Service Provider (SP) should be a company registered under Indian Companies Act 1956.	Incorporation Certificate
2.	Documents	The financial documents will be made available.	1. Copy of certificate from CA 2. P&L Account 3. Balancer Sheet
3.	Financial Position	The Positive Net Worth in Indian Rupees for last year should be minimum net worth 10 Crores.	Copy of certificate from CA.
4.	Company Presence	The company should be providing IT/ITES related services in India for at least the last ten (10) financial year ending 31st March 2021.	Self-Undertaking with documentary proof
5.	Blacklisting	Bidder should not be debarred/ blacklisted by any Government/PSU in India as on date of submission of the Bid.	A self-certified letter signed by the Authorized Signatory of the bidder.
6.	Experience	Service Provider should have successfully implemented / commissioned at least 5 project of each scope	Purchase order/LOI as per the format provided in RFI
7.	Compliance	Service provider should provide a certificate valid copy of, a) ISO 9001 b) ISO 27001 c) ISO 20000-1 d) CMMI Level V e) SOC1,SOC2 and SOC 3 f) ISO 22301	Copy of valid Certificates,

MCTE
Dist.
M.P.)

8.	Resource	Service Provider should have technical staff (developers, security experts, network experts etc.) on its payroll having following certifications/ Skillsets. a) CEH b) LPT c) OSCP d) CISSP e) CISA f) Networking (CISO, etc) g) SIEM h) DLP i) Cloud Security & cloud technologies j) Threat Intel The technical staff should be a Bachelor/ Master in Cyber Security / Computer Science / IT	Copy of valid Certificates of proposed resources. Provide a matrix of these qualifications and certifications in these and other domains

PART – II

7. Procedure for Response

a) The information is being issued with no financial commitment and MoD reserves the right to change/withdraw or vary any part at any stage.

b) Acquisition procedure would be carried out under the provisions of DAP 2020.

c) Vendor interaction in accordance with DAP 2020 to willing vendors.

d) Response to RFI will be **submitted within 04 weeks after the issue date** at under mentioned address

Brigadier General Staff
Military College of Telecommunication Engineering,
Mhow, Indore
MP – 453441
Email: nsi.3112@nic.in

e) All the pages of the RFI response paper must be sequentially numbered and must contain the list of contents with page numbers.

MCTE
Date.....
MHOW (M. P.)

f) All pages of the RFI shall be initialed and stamped by the person who signs the application. Documents to be submitted by RFI respondents.

i. Compliance Sheet (Annexure I to Appendix)
ii. Particulars of applicant (Annexure II to Appendix)
iii. Acceptance of Terms and Conditions (Annexure III to Appendix)
iv. List of Previous Works (Annexure IV to Appendix)

7.1 **Evaluation Committee**

a) The Evaluation Committee constituted by experts shall evaluate the responses to the RFI and all supporting documents & documentary evidence. Inability to submit requisite supporting documents or documentary evidence, may lead to rejection of the RFI Proposal. The Committee may seek additional documents as it deems necessary.

b) Each of the responses shall be evaluated to validate compliance of the applicant according to the eligibility criteria, Forms and the supporting documents specified in this document.

c) The decision of the Evaluation Committee in the evaluation of responses to the RFI shall be final. No correspondence will be entertained outside the evaluation process of the Committee.

d) The Evaluation Committee reserves the right to reject any or all proposals. The RFI Proposal will be evaluated based on the documentary evidences provided.

Brigadier Dinesh Tiwari

Brigadier General Staff
Military College of Telecommunication Engineering, Mhow, Indore
MP – 453441

MCTE
Date.....
MHOW (M.P.)

Annexure I to Appendix

Compliance Sheet

Sl. No	Enclosure description	Enclosed (Yes/No)	Annexure/Attachment/ Page No./ Envelop No. of the enclosure
1.	Copy of Certificate of Incorporation of Company or Registration Firm		
2.	Copy Goods Service Tax Registration		
3.	Copy of PAN no allotted by Income Tax Department		
4.	Copies of Annual audited accounts statements (P&L and Balance Sheets last three FY certified by a chartered Accountant)		
5.	Application Letter		
6.	ISO 9001 ISO 27001 ISO 20000-1 ISO 22301 CMMI Level V SOC1,SOC2 and SOC 3		
7.	Particulars of the Applicant (Appendix B)		
8.	Self Declaration that the applicant hasn't been black listed / performance issues by any Govt./PSU		
9.	Acceptance Of Terms & Conditions Contained In the RFI Document (Appendix C)		
10.	Project Experience (Appendix D)		
11.	Resource Certificates as mentioned in PQC		
12.	Technical Staff Details as mentioned in RFI		
13.	Signed RFI Document		
14.	Signature with Date & Seal		
15.	Name		

MCTE
Date.....
MHOW (M.P.)

Annexure II to Appendix

Particulars of Applicant

1.	Name of the Organisation	
2.	Organisation Status of Registration	
3.	Address of Corporate Office	
4.	Address of Office in AP (if any)	
5.	Telephone No	
6.	Email Address	
7.	Website	
8.	Registration No of Certificate of Incorporation & Date	
9.	Registration No of G.S.T & Date	
10.	Permanent Account Number of Income Tax & Date of Regn	
11.	No. of years of proven experience of providing similar Services	

Annexure III to Appendix

Acceptance of Terms and Conditions

RFI No: _____, Date: _____, Location: _____

To

<.....>

Dear Sir/Madam,

I have carefully gone through the Terms & Conditions contained in the RFI No:_____, regarding RFI. <.....>.

I declare that all the provisions of this RFI Document are acceptable to my company. I further certify that I am an authorised signatory of my company and am, therefore, competent to make this declaration.

Signature of the Applicant

Date:

Place:

Company Seal

Annexure IV to Appendix

List of Previous Works

EOI No: _____, Date: _____

SL. No	Name of Client, Contact Person, Contact Telephone No, Mobile No, Physical Address	Name of Project	Project Start Date and End Date, Brief of Project	Project Cost	Scope of Project (Hosting, Development or SoC services)	Status (Complete/ In Progress/ Delay)

The information provided in the above table must supported by copies of relevant work order and completion certificate.

Signature of the Applicant
Date:
Place:

Company Seal

MCTE
Date
MHOW (M. P)