

**GOVERNMENT OF INDIA
MINISTRY OF RAILWAYS
RAILWAY BOARD**

No. 2017/Sec.(Int.)/51/9/1Pt.

Dated: 16.12.2022

**The Principal Chief Security Commissioners,
Railway Protection Force,
All Zonal Railways, PUs, RPSF,
RDSO, KRCL & Metro Railway Kolkata,
Dir./JRPFA/LKO & TC/KGP,
IG/CORE, IG/CON/ECOR & IG/Tech.**

Sub: Revised Chapter- X (Operation of Special Wing) of RPF
Establishment Manual - 2019.

*** ** **

In reference to this office letter of even No. dated 15.12.2022, an updated version of revised Chapter -X (Operation of Special Wing in RPF) of RPF Establishment Manual - 2019 duly approved by DG/ RPF, is enclosed herewith for information and necessary action, please.

DA: As above.

**Signed by S.shandilya
Date: 16-12-2022 17:25:19**

**(Sumati Shandilya)
Inspector General/RPF/HQ**

Copy to: DIG/ Estt. – with request to replace existing Chapter-X of RPF Establishment with the revised Chapter-X (copy enclosed).

CHAPTER-X of Establishment Manual

Operation of Special Wing in RPF

In exercise of the powers conferred under Rule 28 of the RPF Rules, 1987, Director General/ Railway Protection Force hereby issues the following directive in supersession to Chapter X of the Establishment Manual 2019 in connection with the Operation of Special Wing in RPF.

1. Mandate:

As per the Rule 17.5 of the RPF Rules 1987:

“The Principal Chief Security Commissioner may deploy enrolled members of the Force working in Special Wing of his Security Commissariat in the divisions for collection of intelligence affecting the Security and Functioning of the Railways”

2. FUNCTIONS AND DUTIES OF SPECIAL WING

The Role of the Special Wing needs to be remodeled according to the changed Security Scenario of the Present Times. In addition to armed Militant Groups, the Railways are also a soft target for Agitational Programmes, by desperate Groups against the Government in Power.

From Rail ‘Rokos’ to the burning of Coaches and other Rolling Stock, to vandalizing the Railway Premises, these Groups have a mob mentality and resort to any amount of violence to further their Agenda.

The Special Wing of RPF needs to be remodeled according to the changed Security Scenario of the Present Times. Therefore, the detailed scope of activities has been outlined below:

- a)** Subversive activities, LWE activities, activities of Terror Outfits and forces inimical to National Security having direct/indirect bearing on Railway Working.
- b)** Intel Inputs that have a direct/indirect bearing on improving the punctuality and safety of Trains.

- c)** Collection of intelligence with regard to threat calls received through letters, Telephone Calls or Social Media.
- d)** Agitation Activities of trade Unions/Political Parties/Pressure Groups/Contrarian Forces having direct/indirect bearing on Railway Working.
- e)** Congregations connected with religious festivals, events of local and national importance having direct/indirect bearing on Railway working and security.
- f)** Intel about any planned disruption by vested interests in congregation to be addressed by the Hon. MR, MOSR & other VVIPs.
- g)** VIP Movement over Railway system likely to affect Railway Working.
- h)** Generating Intel about anti-social and other objectionable activities of Railway Employees including RPF/RPSF and Non-Railway Workers working in Railway system.
- i)** Generating Intel about Anti-Social and other objectionable activities of Civilians Linked with the Indian Railways with special focus on the Contractual Workers/Labourers working in the Railway Premises.
- j)** Development of Sources among Trackmen/Keymen/ Gangmen/ Gatemen/ Patrolmen/ ESMs/Pointsmen/Gate Mitras/other Railway and Non-Railway Staff living in nearby Villages, Schools, Colleges, other Establishments in or near Railway Premises, Coolies, Vendors, Auto/Taxi Drivers, Passenger Associations, Prominent Persons in Villages, Mohallas, Local Bodies to collect Human Intelligence (HUMINT). The List is Indicative and not Exhaustive.
- k)** Addition of New Sources.
- l)** Maintenance of Dossiers of Persons active in Railway System with antisocial/subversive leaning/ LWE sympathizers/Over Ground Worker (OGW) of Terror Outfits including Railway Employees and RPF, if any.
- m)** Close watch on the functioning of RPF at various levels and reporting misdeeds, indiscipline, corrupt practices etc., in order to keep the image and goodwill of RPF Protected.
- n)** Collection of information about money laundering, gun running, drug trafficking, narco-terrorism, cross border terrorism/intrusions on railways.
- o)** Sharing of Intel Inputs having bearing on the National Security with the concerned sister Intel Agencies on Real Time Basis. For the said Purpose, Constant and Real Time Coordination with Sister Agencies on SMAC Platform is to be ensured.
- p)** Operation of Threat Management System (TMS).

- q) To submit such Reports and Returns relating to Intelligence and other Allied Matters which are considered essential for efficient functioning of Special Wing.

The Intel collected shall be evaluated properly to assess its correctness before submission of the Intel Reports to the Concerned Authorities for taking necessary action. It shall keep the Director General, RPF duly informed of all matters of importance through Intelligence Cell, Security Directorate, Railway Board.

- r) To keep the record of Protection Schemes/Strike Schemes/Contingency Plans of the concerned Unit duly vetted by the Local District Administration/State Authorities. (The Format is annexed as **Annexure- 7**).
- s) To maintain record of Vital Installations and Protected/Prohibited Places of the concerned Railway Unit (The Details are appended as **Appendix 2 & 3** Respectively).
- t) To maintain the record of the visit of the Unit by Foreign Nationals along with their Clearance.
- u) PCSC of all Zonal Railways & Intelligence Cell, Security Directorate, Railway Board shall process the Monthly Intelligence Reports received from the Zonal Units/Zonal Railways respectively and prepare a consolidated Monthly Intelligence Report for publishing in the Monthly Intelligence News Letter to be circulated on 'Need to Know Basis'.
- v) To prepare Case Studies of Major Incidents highlighting the Role of Intel.
- w) Any other task assigned by the Competent Authority.

There is a tendency among Zonal Railways to entrust non-mandated duties like conducting Fact Finding Enquiries/DAR Enquiries, lodging FIR on behalf of RPF Administration, conducting visible watch/patrolling at vulnerable spots, taking action to stop stone pelting over trains or placing foreign material on track etc.

These activities expose the Intel operatives and hamper their work. Therefore, these responsibilities are to be performed by the Executive Wing (RPF Posts/Out Posts/CIB etc) and not by the Special Intelligence Branch. PCSCs may desist from entrusting these responsibilities to SW.

3. INTEL STRATEGY

The following strategy needs to be adopted for improving the functioning of Special Wing:

(a) Development of Independent Sources: SW operatives seldom cultivate independent sources. They are largely dependent on information received through Casual Contacts or intelligence inputs received through other Sister Agencies. It is high time that they start cultivating their Independent Sources.

The cultivation and maintenance of Sources is a Standardised Process which has been mentioned in **Appendix - 1**.

(b) Effective Coordination with other Agencies: In order to obtain input, verification of the input from other sources and to collate different inputs, it is imperative to exchange inputs with Sister Agencies.

Intelligence Fraternity cannot work in Water Tight Compartments. They need to coordinate with other agencies, reach out to them, exchange inputs, provide help and back up when needed and give actionable input to concerned agency in time if the input is relevant to them.

Timely Exchange is crucial while exchanging Inputs. Moreover, the inputs need to be shared not indiscriminately, but strictly on **'Need to Know Basis'**.

(c) Use of Intelligence Databank for generating Quality Intel Inputs: We generally do not create databank of Intel inputs due to which all these inputs remain strictly stand alone. A digital databank is necessary to analyse past inputs, examine an input in the context of past inputs, observe a pattern in the inputs received in the Past and forecast by extrapolating the Pattern **in order to generate Quality Intel Inputs**.

(d) Greater use of TECHINT: More than half of the Nation's Population uses Mobiles and Internet. Anyone using the Mobile Phone/Internet will leave his footprints in the Digital World. Therefore, in order to gather information, we need to venture into the world of mobile calls and Internet.

Lot of inputs can be received by analysing Call Detail Records/Subscriber Detail Records/ Tower Dump Data/Internet Protocol Detail Records/Social Media Activity etc. We need to develop expertise in handling new and emerging World of Data.

Therefore, it is being insisted to procure necessary software and get operatives trained in CDR and IPDR Analysis. The use of Cyber Investigative Tools and Collection of Open Source Intelligence (OSINT) through Social Media Analysis tools by deploying suitable IT based software will also come in handy for collection of Inputs. Cyber Cells are functional in all zonal Railways which may render necessary help to SW of RPF in cyber surveillance and investigation, social media patrolling and analysis with a view to generate actionable leads.

Special Focus on use of TECHINT for building Social Profile: There is a need to have a special focus on building Social Profile of the 'Target of Interest'. Building Social Profile is an Intel Technique designed for targeting Individuals, Groups, Locations or specific Operational Threats

It is, in essence, an Executive Summary of intelligence information and analysis to better understand the background, history or involvement of a target within a specific Operational Context

Each Profile is typically collated and updated as more information is collected and analysed. Target profiles assists in Operation Planning. They're often used as a way to summarise Reporting

Target Profiles should typically include:

- Lifestyle and Habits;
- Employment Details;
- Criminal Record Details;
- Financial Profile; and,
- Links to anti-social Group(s) who can hamper the Railway Working
- Relevant Inputs about the Target's Family and Relationships

4 INTELLIGENCE PROCESS:

The Process entails the following steps:

A. Planning

- **Collection:**
- Through Open Sources (**OSINT**) like Electronic, Print Media, Social Media (**SOCINT**) etc
- Closed Sources developed by the Intelligence Operative(**HUMINT**)

- Through Coordination with sister agencies etc
- Technical Sources (**TECHINT**) like CDR/IPDR, Intercepted Call, Snooping Devices and other Technical Gadgets.
- **Evaluation (Verification and Grading):** The information collected is verified through different Sources and graded on the basis of Reliability. The Grading Grid is shown in MAC MATRIX enclosed as **Annexure- 1**.
- **Collation:** different pieces of information received through different sources are collated together to get the complete information.
- **Analysis:** The information thus processed will be analysed.
- **Prediction:** The outcome of analysis will be prediction of a future outcome which forms the basis of resource allocation and future planning by the security agency. The outcome of analysis is called **“Intelligence”**.
- **Dissemination:** The Intelligence is, then, disseminated to executive body of the Security Agency and other Sister Agencies strictly on “Need to Know” basis.

B. Review & Feedback:

After Dissemination, the Intel also needs review on the basis of further Developments and Inputs Received. Subsequently, a feedback mechanism has to be put in place to find out the veracity of input and efficacy of action taken based on the Input.

The **raw, incomplete, unverified** and **unprocessed** information should not be dished out as intelligence. Further, focus of SW should not remain on Incident Reporting. **Incident Reporting** should be resorted to only if the incident has **future implications** for the Security Agency or has some **hidden dimension** which the Executive Wing of the Security Agency is not yet aware of. In other Cases, information regarding the Incident should be treated as information received from Open Source and subjected to the above mentioned steps before conveying to Executive.

5. ORGANISATIONAL PATTERN OF SPECIAL WING

a) Sanctioned Strength of SW of Zonal Railways

Sanctioned Strength of SW of Zonal Railways shall be as decided from time to time by the DG/ RPF. PCSCs may submit proposals with justification for revision of sanctioned strength as and when required.

b) Constitution of SW wing in the Zonal Railway:

The Posts will be in the rank of Constable, Head Constable, ASI, SI and IPF. These ranks are re-designated as:

S. No.	Rank	Designation in the SW Wing
A	Constable	Watcher
B	Head Constable	Security Assistant (SA)
C	Asst. Sub Inspector	Assistant Intelligence officer (AIO)
D	Sub Inspector	Deputy Intelligence officer (DIO)
E	Inspector	Intelligence Officer (IO)

The TechInt generated by Social Media Analysis Cells of Zones/TOP ARC at FHQ will be shared with SW for verification, collation and analysis.

(c) MULTI AGENCY CENTRE (MAC)

"Multi-Agency Centre (MAC) has been established for Courter Terrorism whose mandate is to stare terrorism related inputs on day to day basis". As per GoM Recommendation, Multi Agency Centre MAC) was created at Delhi and Subsidiary Multi Agency Centers (SMACs) in various States comprising Representatives from various Security Agencies, for streamlining Intelligence Efforts.

MAC & SMAC started its full-fledged functioning w.e.f. 01.01.2009 for sharing of information & better coordination among Intelligence Agencies. INTELLIGENCE CELL, SECURITY DIRECTORATE, RAILWAY BOARD is the nodal office of MAC. The Unit operating the TMS of MAC/SMAC will be part of the SW.

6. ZONAL RAILWAY SPECIAL WING

6.1 Each Zonal Railway Headquarter shall have its Special Wing which will be manned by such members of the Force as are sanctioned from time to time. A Gazetted Officer will be the In-charge of the Special Wing who will work under the supervision & direction of the PCSC, RPF of the Zone.

6.2 RESPONSIBILITIES OF ZONAL RAILWAY SPECIAL WING (SW)

- i)** The main function of Special Wing at the Zonal Railway Level is to ensure implementation of the orders, instructions, circulars and guidelines issued from Security Directorate and to provide aid, guidance and assistance to the concerned Divisional Units for their Efficient Functioning.

- ii)** The Prime Responsibility of Special Wing In-charge is that if any incident as enumerated in Para 1.3 (Chapter - 1) takes place in his/her jurisdiction, the same must be communicated to Intelligence Cell, Security Directorate/PCSC RPF of the concerned Zonal Railway by quickest possible means, including through Intelligence Setup e-Mail.

- iii)** The In-charge, Special Wing will obtain information through sources, surprise visits etc, to ensure that no Special Wing Personnel including the In-charge, Special Wing of the Divisional Unit under his jurisdiction is involved in any type of Corruption/ Irregularities/Malpractices etc.

- iv)** The In-charge, Special Wing will inform Intelligence Cell, Security Directorate, Railway Board through e-mail prior to his or any SW staff visit to any Unit/Location for Raid/Surprise Checking/Enquiry/ Collection of information etc.

6.3 DUTIES OF ZONAL RAILWAY SPECIAL WING

The following shall be the duty of the Zonal Railway Special Wing.

- i)** To guide the Field Units in all matters relating to intelligence matters to ensure implementation of the Orders, instructions issued by the Competent Authority.

- ii)** To ensure that all Reports and Returns prescribed by the Competent Authority are properly complied with and furnished in time by the Divisional Intelligence Unit.

- iii)** To maintain record of important Incidents, State of Employees, Unit at a Glance, Trade Union Activities, dossiers of anti-social Elements and RPF Personnel noticed for Prejudicial Activities, Strike Schemes/Contingency Plan,

visit to the concerned Zonal/Divisional Units by the Foreign Nationals particularly Vital Installations, Protected/Prohibited Places etc.

- iv)** To verify the veracity of information/Intel received from Divisional Units/Security Directorate and give Comments/Views thereon.
- v)** To collect, collate and forward the important news inputs having direct/indirect bearing on the Railway Working of the concerned Zone to Intelligence Cell, Security Directorate, Railway Board with English Translation (in case of Vernacular Language Inputs).
- vi)** To keep liaison with officials of the Railway Management, District Administration, Police, SW (IB) and State Authorities.
- vii)** To conduct Secret/discreet enquiry into the cases specifically assigned to them by the Competent Authority.
- viii)** To evaluate the information sent by field units with particular reference to:
 - a)** Reports relating to the Trade Union Activities, Labour Unrest, incidents of clashes between Members of the Force and Employees of the concerned Divisional Unit/Other Outsiders.
 - b)** Information relating to the discipline and morale of the Force and dissatisfaction amongst them, if any, and send further report to Intelligence Cell, Security Directorate, Railway Board, duly vetted by the PCSC of the concerned Zonal Railway, with Comments.
- ix)** To collect, collate and disseminate information/intel relating to all Intelligence Matters including those Matters which are directly or indirectly connected to the new scope of activities of the Special Wing as mentioned in the Para 1.3 (Chapter - 1) of this Manual to the concerned Authorised User strictly on Need to Know Basis.
- x)** To Develop Sources at the Zonal Level with special focus on developing Sources who can operate in areas where the Vital Installations,

Prohibited/Protected Areas, Political Agitation Prone Areas, Communally Sensitive Areas etc of that particular Zone are Located.

xi) Any other Work assigned by the authorized Competent Authority.

7.0 DIVISIONAL UNIT SPECIAL WING (SW)

7.1 Special Wing of the Divisional Unit is practically the key base of the entire Special Intelligence Setup of the Force.

Each Divisional Unit shall have a Special Wing Unit and shall be manned by such number of Force Personnel as are sanctioned from time to time.

The Officer In-charge of the Wing (I/C, SW) shall be mainly responsible for collection, collation, analysis and dissemination of Intel of Importance and Interest relating to Labour/Union Affairs, matters which are directly or indirectly connected to the new scope of activities of the Special Wing as mentioned in the Para 2 of this Chapter and other Cognate Subjects having direct/indirect bearing on the Railway Working of the concerned Divisional Unit. He/ She will also ensure compliance of the provisions contained in Security Circular 01/2022 issued vide Letter No. 2021/Sec (CCB)/45/64 Bad Work dated 31.01.2022.

Reports generated by SW of the zone shall be filed by the SW Unit In-charges himself who will ensure its Confidentiality. Unit In-charges should give his comments on the inputs in the Report for further evaluation by the Superior Officers of the concerned Zonal Railway.

7.2 DUTIES & RESPONSIBILITIES OF DIVISIONAL UNIT SPECIAL WING.

Since, Special Wing of the Unit is the key base of the entire Intelligence Setup of the Force, its Staff have to remain extra alert and vigilant round the clock so as to notice any Development which may pose a threat to Railway Working.

Timely and prompt reporting on their part is bound to strengthen the security of the concerned Divisional Unit by way of taking appropriate preventive measures at the level of the Management and Higher Echelons of the Force.

Their Main Functions shall be:

- i)** To collect, collate und disseminate all kinds at information relating to the Local Area where the concerned Divisional Unit Premises is located including the surrounding suburban area.
- ii)** To collect intelligence of subversive and antisocial elements, political and communal issues, espionage, Railway affiliated trade unions and labour activities/movements and their meetings, processions, demonstrations, dharnas, strikes etc. and forecast probable Future Incidents.
- iii)** To maintain the record of activities and dossiers of undesirable employees of the Divisional Unit, other ant-social elements which may prove potential threat to working of that particular Divisional Unit.
- iv)** To maintain regular and/or casual source/contacts who are providing useful Intel Inputs. **For this purpose, they shall maintain a Source Register.**
- v)** To keep track with the agitational activities, if any, of the members of the Force and to maintain their dossiers.
- vi)** To compile and submit various reports and returns prescribed by the Special Wing of the Force Headquarters.
- vii)** To prepare and submit any specific information called by the higher authorized authorities.
- viii)** To prepare and submit Daily Intelligence Report.
- ix)** To maintain vigil over the security arrangements of the concerned Railway Divisional Unit and to bring out the lacunae therein, if any, to the notice of the concerned Competent Authority.
- x)** To maintain:
 - a.** Complete and up to date record of all important incidents which affected the concerned Divisional Unit Working.
 - b.** Statistics of Disgruntled Railway Employees/Railway Employees involved in any undesirable activity/Behavior.
 - c.** Divisional Unit at a glance
 - d.** strike scheme
 - e.** contingency plan duly vetted
 - f.** Vital Installations/Vulnerable points
 - g.** protected and prohibited places
 - h.** Standing Orders and Instructions related to the Special Wing
- xi)** Submission of relevant important news items by collating relevant inputs through OSINT from local newspapers, magazines, periodical, Social Media

Platforms etc, to the Divisional RPF Unit Head & to the concerned Special Wing Authority at the Zonal Level.

- xii)** To collect information in the form of hand-bills, leaflets, pamphlets, posters and by attending open, general, secret Executive/General Meetings, Dharnas, Processions, Demonstrations etc. held by labour unions/associations and forwarding the same to the concerned higher authorities.
- xiii)** To maintain close liaison with local Police, Civil Administration, Fire Station, SW, CID and other related departments.
- xiv)** To undertake such general and secret enquiries into cases specifically handed over to them by the authorized competent authority.
- xv)** To keep informed Zonal Special Wing Authority about the Employees and Members of the Force involved in Corrupt Practice and Undesirable or Prejudicial Activities.
- xvi)** To keep watch on the Force Personnel suffering from Psycho/Neurotic Problems and Unusual Behavior. Further, whenever such individuals relieved on Posting/Transfer to another Unit, full details of mental ailment/medical history should be forwarded to the new Unit Head as well as to the new In-charge, SW in a Confidential Manner.
- xvii)** Considering the stressful life of Force and recurrence of undesired incidents, the Unit RPF Head should also identify such Personnel who has abnormal behavior pattern and keep him/her under close watch through Unit SW. At the same time, there is a need to take some proactive steps at Unit Level to counter stress among personnel.
- xviii)** Unit SW I/C to report present status of various prescribed welfare measures which are mandatory requirement to be implemented in the Unit like grievance redressal mechanism, accessibility of the Unit Head to the Unit Personnel, accommodation allotment, timely Weekly Rest given to the Force Personnel when due etc.
- xix)** To collect, collate and disseminate information relating to all Intelligence Matters including those matters which are directly or indirectly connected to the new scope of activities of the Special Wing as mentioned in the Para 1.3 (Chapter - 1) of this Manual to the concerned User strictly on 'Need to Know Basis'.
- xx)** To Develop Sources at the Zonal Level with special focus on developing sources who can operate in areas where the vital installations,

Prohibited/Protected Areas, Political Agitation Prone Areas, Communally Sensitive Areas etc of that Particular Zone are Located.

xxi) To comply with the provisions contained in Security Circular 01/2022 issued vide Letter No. 2021/Sec{CCB}/45/64 Bad Work dated 31.01.2022.

xxii) Any other Work assigned by the Authorized Competent Authority.

7.3 GUIDELINES FOR SHARING OF INFORMATION

In order to streamline the process of information sharing at different Formation Level, informations are categorized on the basis of type, content and the level up to which the information need to be shared.

7.4 Channel of Reporting

The following channel of reporting will be adhered to:

- (i)** Intelligence requiring immediate attention and action on the part of the Division shall be passed on directly to the Sr. DSC/DSC by the unit deployed in that Division.
- (ii)** Earlier requirement of the intelligence inputs/forecasts being approved by PCSC/CSC of the Zone before sending to Intelligence Cell, Security Directorate, Railway Board has already been dispensed with. It has to be shared on real time basis endorsing a copy to the PCSC/CSC of the Zone.
- (iii)** All important and urgent intelligence input which requires attention of Railway Board should be passed on directly by SW/IPFs of Divisions to Railway Board Intelligence Cell as well as to PCSCs of the Zone.

7.5 However, depending upon the Criticality Grading of the information, the information sender shall pass Extremely Critical (EC) & Critical (C) graded inputs to Intelligence Cell, Security Directorate, Railway Board Office by quickest possible Secured Means.

(A) Divisional Unit Level Information

- i)** Attack/Probable Attack by Naxalites/Militants/Terrorists etc in the Divisional Unit. **(EC)**
- ii)** Exchange of fire between RPF personnel & Naxalites/Miscreants. **(EC)**
- iii)** Use of force by RPF while dispersing criminal/unlawful assembly/unruly mobs/employees including firing Incidents. **(C)**
- iv)** Death of RPF personnel in action. **(EC)**
- v)** Loss of Arms & Ammunitions. **(EC)**
- vi)** Major incidents happened in the concerned Divisional Unit causing loss of life & property. **(C)**
- vii)** Assault on civilian by RPF personnel & vice-versa. **(C)**
- viii)** Major communal/caste clashes in the area. **(EC)**
- ix)** Deterioration of Law & Order situation in and around the unit including township affecting security of the Divisional Unit.
- x)** Altercation between RPF personnel and local public/local police/media/VIP/VVIP/any other Govt. or public agency. **(C)**
- xi)** Reporting of press and electronic media on any major issues related to the security and all issues related to RPF.
- xii)** Major crime happened at the Divisional Unit other than theft cases.
- xiii)** Malpractices/corruption/espionage in the Divisional Unit. **(C)**
- xiv)** Threat/Alert information from militants/extremist group to the Divisional Unit with special Focus on the vital installations.**(EC)**
- xv)** Strike/labour unrest/gherao by the employees/worker of the Divisional Unit and important trade union activities.
- xvi)** Public activities in the local area which can have a bearing on the Divisional Unit.
- xvii)** Reports on the activities in and around the Recruitment Centre to avoid any nefarious activity
- xviii)** Criminal cases registered against RPF personnel/Railway Employee including raid, arrest & bail by local Police, CBI & other LEAs.**(EC)**
- xix)** Arrest of RPF Personnel by Local Police, CBI, Vigilance and Suspension thereof. **(EC)**
- xx)** Involvement of RPF Personnel in any type of Malpractices/Corruption Cases and Cybercrime. **(C)**

- xxi)** Assault Cases, serious incidents of Indiscipline, Misconduct between Senior & Junior Personnel. **(EC)**
- xxii)** Murder of RPF Personnel. **(EC)**
- xxiii)** Suicide committed by RPF Personnel. **(EC)**
- xxiv)** Incidents of Fratricide. **(EC)**
- xxv)** Attempt to suicide by RPF Personnel. **(EC)**
- xxvi)** Accidental/Unnatural Death of RPF Personnel. **(C)**
- xxvii)** Natural Death of RPF Personnel.
- xxviii)** Death of RPF Personnel while On Duty. **(EC)**
- xxix)** Involvement of RPF Personnel in Rape, Molestation, or Sexual Harassment Cases. **(EC)**
- xxx)** Deliberate/Accidental Firing by RPF Personnel. **(EC)**
- xxxi)** Loss of Official Documents, Service Documents, Govt. Property.
- xxxii)** Road Accidents involving On Duty RPF Personnel or RPF Vehicles. **(EC)**
- xxxiii)** RPF Personnel under treatment of HIV/AIDS/**COVID 19 virus or any other Pandemic caused by any Micro Organism.**
- xxxiv)** Death of railway employee on duty or Contractual Worker while working in the Railway Premises
- xxxv)** Death of Dog of RPF Dog Squad **(C)**
- xxxvi)** Loss of I/Card by RPF Personnel
- xxxvii)** Immediate Relief and Rescue Operations extended by RPF Personnel to the Local Administration in the event of Major Disasters
- xxxviii)** Good work/extra ordinary work done by RPF Personnel as well as their Wards which has brought good name to the Force
- xxxix)** Visit of VVIPs/VIPs including Hon. MP/MLA and important Political Leaders and Related Issues.
- xl)** Visit of Senior Dignitary in the Divisional Unit and Related Issues
- xli)** Visits of Senior Officers of the Divisional Unit to the Zonal Headquarters
- xlii)** Meeting of the Divisional Management with the Local Police & Local Administration etc.

8.0 SELECTION, TRAINING AND TENURE OF SW PERSONNEL.

8.1 SELECTION OF SW PERSONNEL.

The vacancies arising in future will be filled after screening mentioned in succeeding Paragraphs.

The vacancies, except the vacancies in the rank of Intelligence Officer, will be filled up after short listing and subsequent screening to be conducted by the PCSCs of the concerned Zones in consultation with Intelligence Cell of Railway Board.

a) Short listing for screening:

PCSC will shortlist candidates at least 3 times the number of vacancies in each rank in SW of the concerned Zone. The following RPF personnel will be eligible to be shortlisted:

Designation	Maximum age of Eligibility
Watcher	40 years
Security Assistant (SA)	45 years
Assistant Intelligence officer (AIO)	50 years
Deputy Intelligence officer (DIO)	55 years

- (i)** The minimum length of service to be eligible to be shortlisted for screening against a vacancy in SW will be TWO (2) years after completion of Initial Training for direct recruits in Constable/ Sub Inspector.
- (ii)** Posting of Intelligence Officers (IPFs) will be done by PCSCs. However, IPFs with unblemished antecedents shall be chosen for posting in SW. IPFs, so chosen for posting in SW, will have to undergo Induction training within three (3) months of getting posted in SW.
- (iii)** The shortlisted candidates should be free from DAR proceedings/vigilance/ criminal cases and should not be undergoing any penalty. They should have clean record of service for the past 10 years. If service length of the applicant is less than 10 years, then he/she should have clean record for his Entire Service.
- (iv)** The short listing for the vacancies arising during the whole year will be done on or before 26th January of that Year. In case of any departure from this

timeline, PCSCs may seek and obtain approval of DG RPF citing cogent reasons.

b) Screening

Post short listing, the candidates will be put through the process of screening to identify most suitable personnel for SIB.

i) Screening may be done to adjudge the suitability of a Candidate based on the following Traits:

- Having flair for Intelligence Gathering,
- Good Inter Personal Skills,
- Proficiency in Local Language and Customs,
- Contacts in the Local Population
- Inquisitiveness and attentive to Details
- Perceptiveness and possession of Ingenuity
- Being a good Listener and knowledge of how to keep Silent
- Ability to express clearly and interestingly
- Passion for Anonymity
- Possession of Great Patience
- Quick Thinking
- Inconspicuousness in appearance

ii) A Screening Committee will be constituted by PCSC consisting of three officers of or above the rank of Security Commissioner. In the event of absence of an officer of requisite rank in the Zone, an officer of the rank of Assistant Security Commissioner will be nominated.

iii) An Officer nominated by IB/ State Intelligence/ any other sister security/intelligence agency will be co-opted in the committee as 'Technical Member'. If service of technical member from above agencies could not be obtained, PCSC will request DG/RPF for nomination of a suitable technical officer giving cogent reasons.

iv) An Observer will be nominated by DG/RPF as his representative to be present during the process of screening and submit his/her report to DG/RPF after completion of screening.

v) The following will be the stages of Screening:

(a) Psychological Test: based on a standard questionnaire. It will be of 40 Marks. The Standard Questionnaire duly filled up by the Candidates will be

handed over to the Observer. He will submit the filled up questionnaire to Intelligence Cell, Railway Board who will get them evaluated and submit the list of marks to the Committee after obtaining the approval of DG/RPF. **The Questionnaire may be designed by IG HQ and approved by DG RPF before using it for Psychological Test.**

- (b) Test of Proficiency in speaking Local Language:** 10 marks will be evaluated by the committee. Zones, where more than one language is spoken, proficiency will be tested in any of the languages spoken. Bonus 10 marks will be awarded if the candidate is able to speak all but not less than four languages with proficiency. Bonus 5 marks will be awarded if he/she is able to speak more than two languages with proficiency.
- (c) Proficiency in IT/Computer Applications:** 50 marks will be evaluated by the committee.
- (d) Test of driving a Four Wheeler:** 10 marks will be evaluated by the Committee.
- (e) Record of Service:** 20 marks will be evaluated by the committee provided that for calculating the marks of Record of Service, the marks obtained by candidates having less than 5 years service may be extrapolated with reference to full 20 marks.
- (f) Test of Proficiency in Intelligence Trade Craft:** 50 marks will be evaluated by the technical member and he will submit the list of marks to the committee.
- (g)** The Candidates obtaining 60% marks (minimum 108 marks out of full marks 180) will be declared to have qualified. The Candidates declared to have qualified will be included in the merit list and subsequently posted to the extent of vacancies on the basis of their merit.

8.3 TRAINING:

- (i)** A two week long course on “**Intelligence Trade Craft**” will be conducted by concerned PCSCs in Zonal RPF Training Centres for every RPF personnel on his initial posting in SW wing after screening. The training module already been circulated by Railway Board, is enclosed as **Annexure 9**. PCSCs may coordinate with concerned Joint Directors SIB of the concerned States to help

them in training by making available the services of experienced IB Personnel as Trainers.

The Services of 60 in-house Trainers (trained by IB in TOT courses conducted from 2018 to 2021) and 100 other RPF Officers trained by IB in May & Sep 2019 may also be utilised for training.

PCSCs may also approach State Police and Other Security Agencies to avail of the services of reputed Intelligence Experts as Trainers.

- (ii) Director/JJR RPF Academy will coordinate with Addl. Director/Training, IB and organise “**Training of Trainers**” courses on Intelligence Trade Craft at least twice every year to develop sufficient number of in-house Trainers.
- (iii) A weeklong refresher course on “**Intelligence Working**” will be conducted by PCSCs every year for the RPF Personnel working in SW wing. Trainers within and outside RPF may be utilized for the Course. The syllabus of the refresher training is enclosed as **Annexure 10**.
- (iv) IG Tech will set up a Social Media Analytics Lab at a suitable location under TOP ARC. Director JJR RPF Academy will arrange to impart weeklong training to 64 RPF (4 per zone) personnel posted in SW across the zones per annum. He will work in coordination with IG Tech and may engage experts within and outside the Government for imparting this training. In addition, specialised software related to training, particularly in cyber surveillance and use of social media analysis tools may be organized by the Zonal railways on regular basis for their Intel operatives.
- (v) Concerned PCSCs will procure and operationalize Social Media Analysis Software and get suitable RPF Staff posted in SW trained for utilizing the Software.

8.4 TENURE

Although the tenure of RPF Personnel in SW will be 5 years, the provisions of **Establishment Manual and other guidelines** regarding tenure transfer will not be applicable on the RPF Personnel working in SW. The restriction of 10 years’ service in continuous spells or 15 years service in broken spells or 2 consecutive tenures in a division will also not be applicable for RPF Personnel posted in Special Wing.

However, if an RPF Personnel has completed 10 years at a Place while working in SW, he/she may be transferred and posted to some other Place within SW of the Zone. Further, the administration reserves the right to transfer any RPF Personnel working in SW to any other location within the SW of the Zone in the exigencies of Service or for administrative reasons or to avoid local entanglements of such Personnel or for any such other Consideration. Such an action by the concerned Competent Authority should be recorded with adequate reasons and a detailed report should be submitted to the IG/ HQ by the Zone within a fortnight from the date of initiation of such an action.

8.5 POSTING OUT OF SPECIAL WING

DG/RPF reserves the right to post any RPF staff out of SW without assigning any reason.

- (i)** Ordinarily, RPF Personnel working in SW wing may not be posted out of SW prior to completion of tenure. Exceptional cases will be dealt on case to case basis with approval of DG/RPF. In such cases, PCSC concerned will send a proposal to DG/RPF with detailed reasons mentioned therein.
- (ii)** RPF Personnel posted in SW may be posted out of SW after completion of tenure on receipt of his/her option in writing. If the concerned staff opts to continue in SW, he/she may not be posted out and the period subsequent to the completed tenure will be treated as a fresh tenure.
- (iii)** However, if the Staff gets promoted to a higher rank, he/she will be posted out of SW only in the event of vacancy not being available in SW anywhere in the zone in that Rank.
- (iv)** In case he/she wants to come back to SW after having left SW on his own option/due to vacancy not available in the promoted rank, he/she will have to clear the screening test in his/her new rank afresh except in case of promotion to the rank of IPF.

8.6 WRITING OF APARs

The following channel for writing APARs of RPF Personnel posted in SW wing will be followed in terms of rule 31 read with rule 17.5 of RPF rules 1987:

Designation	Initiating Officer	Reviewing Officer	Accepting officer
Watcher	Intelligence Officer	Gazetted Officer (IC) of SW in the Zone	PCSC
Security Assistant (SA)	Intelligence Officer	Gazetted Officer (IC) of SW in the Zone	PCSC
Assistant Intelligence officer (AIO)	Intelligence Officer	Gazetted Officer (IC) of SW in the Zone	PCSC
Deputy Intelligence officer (DIO)	Intelligence Officer	Gazetted Officer (IC) of SW in the Zone	PCSC
Intelligence Officer (IO)	Gazetted Officer (IC) of SW in the Zone	PCSC	IG/ HQ
Gazetted Officer (IC) of SW in the Zone (in Junior Scale)	As per the circular issued by Confidential Cell, Railway Board from time to time		

IG/HQ will exercise Powers to write APARs as Representatives of the office of DG/RPF.

8.7 COMMAND AND CONTROL

The following channel of Command and Control will be adhered to:

- (i)** Administrative Control: The salary, wages, leave, TA and other administrative authority will be exercised as per the existing procedure in vogue in the zone.

(ii) Disciplinary Control over NON Gazetted personnel posted in SW: The Gazetted Officer In-charge of **SW** will exercise disciplinary control over NG RPF personnel posted in **SW** as per the schedule of powers prescribed in the RPF rules 1987. Where the Gazetted Officer (IC) of **SW** is in Junior Scale, the powers of disciplinary authority in a higher rank over NG staff posted in SW will be exercised by an officer of appropriate rank posted in the Zone nominated by the PCSC by notification in this regard. The powers of Appellate Authority will be exercised by CSC and that of Revisioning Authority will be exercised by IG/ HQ as representative of the office of DG/RPF in terms of rule 31 read with rule 17.5 of RPF rules 1987.

9. Reports, returns and documentation:

Whereas in the RPF regulations the format for registers pertaining to crime, establishment and others has been prescribed, no particular mention has been made regarding records and registers for SW. The following registers as per format indicated are hereby suggested:

a) Open Source (Print/Electronic/Social Media) Information Register- DS 1 (includes information received from contacts).

Sl No	Date	Name of the source (information received)	Details of the information	Action taken	Result/ Remarks

Note: information received from closed sources should be recorded confidentially and kept in personal custody of the Intelligence Operative. The names of closed sources may be camouflaged by keeping pseudonyms that are not used traditionally for naming humans like “Sunrise”, “Red rose”, “Ivory”, “Sapphire” etc.

b) Current month forecast Register- DS 2

Sl. No	Date	Details of the information	Action taken	Results/ Remarks

Report of daily forecasts to be sent by SIB (IC) of the Zone to Intelligence Cell, Railway Board.

c) Register for outsiders involved in subversive/ nefarious activities - DS 3.

Sl. No	Details of the person	Details of the activities	Name of associates	Police registration particulars, if any	Area of activity	Remark

d) Dossier format for railway employees and non railway workers working in railway system who indulged in undesirable activities - DS 4.

1.	Name of the worker	
2.	Railway or Non Railway (name of firm in case of non railway)	
3.	Parentage	
4.	Place of residence	
5.	Affiliation/ leaning with political parties (present/ past) if any	
6.	Date of birth	
7.	Date of joining service in initial capacity	
8.	Present designation	
9.	Place of working	
10.	Brief details of objectionable activities	
11.	Any adverse trait e.g. corrupt, alcoholic, gambler, running huge debt, womanizer, loan shark, criminal, extortionist,	
12.	Any objectionable activities of the union/association of etc to which he belongs.	
13.	Financial position/ assets of the employee (whether commensurate with known sources of income)	
14.	Any other specific information	

A monthly report with a list of such employees with the details of undesirable activities they are indulging in shall be submitted by the GO (IC) of SIB in the Zone to the IG/HQ.

e) Register for daily interaction with sister Intelligence/security agencies by IPF/SI (IC)/SIBs of Division to SIB/ Zonal Railway:- (DS-5): A weekly report of the interaction must be submitted to the GO (IC) of SIB in the Zone. The GO (IC) of SW in the Zone shall submit the monthly gist of these weekly reports to IG/HQ.

Div.	Date	Time	Through phone or through personal meeting	Name of person interacted	Designation	Agency to which the person belongs	Gist of information exchanged, etc	Remarks, if any.

f) Village profile register: Annexure 2. (DS-6)

g) Register for the forecasts for the next month. (DS-7), a report to be submitted by SIB (IC) of the Zone to Intelligence Cell, Railway Board every month.

h) Register for unusual/suspicious activity in the area of responsibility: (DS-8), A report in respect of each entry must be submitted to the GO (IC) of the SIB of the zone by the concerned divisional SIB (IC).

i) Register for undesirable activities of RPF/RPSF personnel: (DS-9), the following data for RPF/RPSF personnel of each post/unit will be maintained

- (i) Name of RPF/RPSF unit
- (ii) Morale of the force
- (iii) Grievances of the members of the force which, if remained un-addressed, are likely to result in disruption of smooth functioning of the force.
- (iv) Discipline in the post
- (v) Information regarding acts of indiscipline among officers or non gazetted personnel which has potential to cause disruption in smooth functioning of RPF/RPSF.
- (vi) Rotation of staff on sensitive duties.
- (vii) Staff performing duties in civil dress.
- (viii) Staff & Officers indulging in corrupt/criminal/objectionable activities like money lending, operating gambling (satta/jua), having other remunerative occupation, using fear of uniform for extraneous purposes, misusing government accommodation for running business etc.
- (ix) Any kind of groupism among members of the force on the basis of caste, creed, region, religion, gender etc which is likely to cause disharmony or disaffection among members of the force.
- (x) Any behaviour of the members of the force which is detrimental to safety, security and general well being of the member her/himself or others, for example excessive alcoholism, drug addiction, mental disturbance, depression, radicalisation etc.
- (xi) Any other information related to member of the force or outsider requiring immediate attention and action on the part of the administration.

A report in this regard will be sent to GO (IC) of SIB in the Zone. Every month GO (IC) of SIB will submit report directly to IG/HQ in the same format post wise. GO (IC) of SIB will submit report regarding undesirable activities of RPSF to IG RPSF too in addition to IG/ HQ and PCSC of the zone concerned in compliance to L.No. 2018/Sec. (ABE)/TR/6/48 dated 20.11.2018.

j) Register of action taken on threat calls received: (DS-10) Format enclosed as Annexure- 3.

k) **Database of inputs/alerts received/generated and occurrences (DS-11)** in MS excel/MS-access. Format enclosed as **Annexure 4**. Occurrences include bomb blast, arson, damage and destruction of railway property, confirmed sabotage, suspected sabotage, track tampering, placing of foreign material on track, explosive recovery, kidnapping of railway employees, train hijack, other activities of terrorists/LWE activists/insurgents like pasting of posters, banners, recovery of pamphlets, graffiti, threatening of railway employees etc. The same database will include the details of inputs received/outputs (alerts/advisories) generated. The database once populated will come in handy for analysis.

The data collected in registers will be analysed regularly and any pattern observed will be shared with executive branch of RPF endorsing a copy to Intelligence Cell, Railway Board.

All registers will be maintained and updated in soft copy (in MS-Excel). The communication to Intelligence Cell, Railway Board will be made strictly through SIB module of RSMS.

10. Report Writing:

Report is a Permanent Record and should always be preserved for future reference. The report should touch all points of Enquiry. **EVERY SOURCE REPORT SHOULD CONTAIN GRADING -A1, B4, C3 ETC.** The report must mention about requirement of further verification on those points on which the Intel Operative is no sure. Retrospection should be done and difficulties encountered should be clearly mentioned in the Report.

A standard report writing format may be designed & implemented in all Zonal Railways in order to ensure uniformity and indexing in the Centralized Data Bank. The committee of CSC RDSO and Sr.SC MAS may design and propose the standard report writing format. The format will be circulated to the Zones after finalization in due course.

11. Infrastructure and resources:

As far as possible, the location of the SW office should be in isolation in order to protect the identity of the sources & their sub handler from other railway personnel.

- The PCSCs shall coordinate with the concerned DRMs to allot a type III/IV quarter in the railway colony earmarked for operationalising it as the SW Office.
- The identity of the SW office and its occupants should not be revealed through any office board/name plate.

- Subject to the availability of space, a room should be earmarked for briefing/debriefing of the individual source.
- The concerned PCSCs and Sr. DSCs/DSCs shall earmark atleast 25% of their SSF immediately after receipt for distribution to ASCs/SIB and IsPF/ SIs of SIB units. An annual internal audit about proper accountal/utilisation of the fund shall be conducted by the concerned SC/ASC Intelligence at the Zonal Headquarter and a detailed audit report shall be sent to the IG/ HQ in the first week of January, every year. The Auditing Officer should record details about proper utilisation of the fund through parameters like amount spent, number of sources developed during the year, number of high-value Intel inputs generated etc.
- Additional SS funds as per need must be made available to SW by the concerned Divisional Head (Sr.DSC/DSC) and PCSC.
- Imprest of Rs 5000/- or more should be sanctioned for monthly petty expenses of the SIB (IC) of the division. The imprest amount may be more based on the workload, jurisdiction, sensitivity of the area, operational need among other factors.
- Provision of adequate tech Gadgets in the field units shall be ensured by all the PCSCs. Some of the technological gadgets recommended are as under:
 - i. Smart Phones with CUG SIM Cards to all SIB personnel
 - ii. Hidden/Spy cameras
 - iii. Night vision devices
 - iv. CDR Analysis software to analyze CDR/SDR/TDD
 - v. GSM live voice recorder
 - vi. GSM live video recorder
 - vii. Pocket pen voice/ video recorder,
 - viii. Wireless video camera with laptop recorder,
 - ix. Audio/video transmitters that can be concealed
 - x. Audio/video bugs concealed in button/spectacle frame
 - xi. Wide band video UHF link, Laser listening device, video bugs in spectacles, video bugs in tie pins, digital audio miniature bugs, video bug in button etc.

The list is only indicative and not exhaustive. In addition, software/IT application for social media analysis will also be procured for collecting OST (open source Intelligence). While procuring the Gadgets/Software, the Zonal PCSCs shall ensure that mandatory condition of short duration training by the vendor while inviting tenders related to procurement of tech Gadgets/Software should be a part of the tender document.

- Computers with scanners, printers and internet connection should be provided with SW along with fax, video cameras, digital cameras and photo copiers. LCD/ LED TVs and News Papers should also be provided at all SW units.
- One four wheeler and one two wheeler at the divisional level SW and one motorcycle to each sub unit of SW should be provided. Hiring arrangements of four wheelers should be processed immediately at Zonal levels. Proposal for two wheelers should be processed by Zones for procurement.
- The PCSCs shall ensure that SIB Personnel should be given priority in allotment of railway residential accommodation from the RPF quarter pool by the concerned Sr. DSC/DSC.

12. STRIKE/MODEL PROTECTION SCHEME.

As per instructions received from MHA, the Model Protection Schemes are drawn by the Management in consultation with the Local Authorities and with the approval of the State Govt. for meeting any contingency arising out of Strikes, Lockouts and Natural Calamities:

The Railway Management will depend on the RPF and the Local Police/Magistrate to provide adequate Security and Law and Order arrangements and other Agencies of the Local Govt. viz. Fire Brigade, Medical etc. during such Periods. It is obvious that the Management and other co-related Agencies handling supplies like water, electricity, edible stuff etc. have to work in close coordination which would only be possible if the Strike/Protection schemes are drawn up by the Management in consultation with the Local Authorities and with the approval of the State Govt.

The Model Protection Schemes will be enforced under the orders of the Dy. Commissioner District Magistrate. PCSC of the Zonal Railway (in respect of all Railway Divisions under their Jurisdiction) & Senior most Officer of the Railway PU(s) shall ensure that Strike Protection Scheme are drawn up expeditiously by the concerned Railway Management.

13. QUARTERLY SURPRISE SECURITY CHECK.

The Zonal SW In-charge shall conduct surprise security check in the Field SW Units on Quarterly Basis and send Report thereon as per the Performa prescribed at **Annexure - 8**. The Report in duplicate on the subject must reach to the Competent Authority latest by 10th of the month following the Quarter for which it pertains:

Period of Quarter	Due Date
April to June	10th July
July to Sept.	10th Oct.
Oct to Dec.	10th Jan.
Jan to March	10th April

14. YEARLY REPORT ON STATUS OF EMPLOYEES.

This shall be prepared on 1st Jan of each year so as to reach Force HQrs by 31st January in the format given at **Annexure – 5**, each year and a copy of this shall be endorsed to the respective Divisional Head of the RPF.

15. INFORMATION RELATING TO RAILWAY UNIT AT A GLANCE.

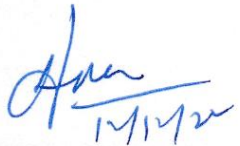
This shall be prepared by the Unit Commanders on the format at **Annexure 6** with a copy to PCSC of the Zonal Railway & Zonal In-charge of the SW Wing in the first week of January each year. Subsequent changes, if any occurred in the information may be reported promptly to the concerned Competent Authorities.

16. SECURITY CLEARANCE OF FOREIGNERS COMING TO INDIA AND VISITING THE RAILWAY UNIT:

The Unit Head shall send a detailed report to Security Directorate Intelligence Branch in respect of foreigners who visited the Unit immediately after the visit and shall follow/adhere to the instructions contained in **Appendix – 4**.

17. Powers to relax, modify or withdraw:

The Director General/RPF reserves the right to relax, modify or withdraw any or all provisions of this Chapter.



(Sanjay Chander)
Director General/ RPF

ANNEXURE – 1

(Refer Para 4)

MAC MATRIX FOR EVALUATION OF INFORMATION RELIABILITY OF A SOURCE

ALPHABET	RELIABILITY	DESCRIPTION
A	Completely Reliable	No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability.
B	Fairly Reliable	Minor doubt about authenticity, trustworthiness, or competency: has a history of valid information most of the time.
C	Reliability Cannot be Judged	Authenticity, trustworthiness, or competency cannot be judged regarding the input, but has provided valid information in the past.
D	Unreliable	Significant doubt about authenticity, trustworthiness, or competency. History of invalid information in the Past.
E	Untested Source	First time Information/ Causal contact.

CREDIBILITY OF INFORMATION

ALPHABET	RELIABILITY	DESCRIPTION
1	Confirmed	Confirmed by other independent sources; logical in itself; consistent with other information on the subject.
2	Likely	Not confirmed; logical in itself; consistent with other information on the subject.
3	Unsupported but probably considered True	Not confirmed; but reasonably logical in itself.
4	Unlikely	Not confirmed, not logical in itself, contradicted by other information on the subject.
5	Probability of the Report Cannot be Judged	First Information provided by the source/ Causal contact.

THREAT ASSESSMENT
<input type="checkbox"/> Is the threat credible? <input type="checkbox"/> Is the threat corroborated? <input type="checkbox"/> Is the threat specific and/or imminent? <input type="checkbox"/> How grave is the threat? <input type="checkbox"/> Background Information <input type="checkbox"/> Assessment <input type="checkbox"/> Course of Action <input type="checkbox"/> The cost of action will be great, but the price of inaction will be far greater?

WHAT WE LOOK FOR - ADD TIPP

- **ASSET SPECIFICITY**
- **DOMAIN SPECIFICITY**
- **DISAMBIGUATION**
- **TIMELINE BUILDING**
- **INTEGRITY OF CONTENT**
- **PRECISION OF LANGUAGE**
- **PATTERN RECOGNITION**

Annexure- 2

VILLAGE PROFILE

Name of village:

Tehsil:

Thana with name and number of SHO:

Sub division:

District:

Distance from railway track: (UP/DOWN)

Name and mobile numbers of elected officials:

1.	Population		14.	Any history of communal violence or caste conflict with names of persons suspected to be involved in inciting violence	
2.	Male Population		15.	Information about animosity between two individuals or families or groups	
3.	Female Population		16.	Information about any resentment against railway	
4.	Adult Literacy		17.	No of unemployed youth	
5.	Main occupation		18.	Information about any unusual gathering of people or mela in the village or nearby area	
6.	Names of rich persons with their occupation				
7.	Names of persons living abroad with details of foreign countries where they are living		19.	Any unusual movement of strangers noticed in the area	
8.	Names and mobile numbers of persons		20.	Names and mobile number of persons from that village that	

	radicalised			can be utilised as informers	
9.	Names of persons with criminal antecedents and info about their modus operandi		21.	Name of Village Chowkidar and his mobile no, if any	
10.	Names of persons with LWE leaning (activists/sympathisers)		22.	Names of persons working with police or Homeguard with their mobile nos	
11.	Names of persons in jail		23.	Names and mobile numbers of respected persons	
12.	Name of persons with criminal antecedents presently absconding		24.	Names and mobile numbers of persons of other villages/towns commuting to this village for work	
13	Names of persons working in railways with their mobile numbers.		25.	Names and mobile numbers of persons of this village commuting to other villages/towns daily for work	
26	Name of NGO with contact details of key person active in the area:				

Annexure 3

DETAILS OF THREAT CALLS/ THREAT LETTERS

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.
Sl. No.	Rail way	Division	State	District	Date of receipt of Threat Call/ Letter/ email/ social media msg /SMS	Telephone no. of caller	Tel. No. of recipient	Time of receipt of call	Address of letter/ email sender	Identity of person making threat	Identity of recipient of Call/ Letter/ email/ social media msg /SMS	Summary of Threat Call/ Letter/ email/ social media msg /SMS	Crime Case No and Date	Status of Investigation

Database of inputs/alerts received/generated and occurrences (DS-11)																						Annexure 4												
Sl. No.	Date	Time	Theatre	State	District	Activity	Input/ Output/ Occurrence						Train / Station / Others	Name of Suspect/ Arrested Person	Name of Organisation taking responsibility/ Suspected to be involved	Name of Dead/ Injured/ Victim			Recovery Details	Trains affected	Time taken to restore normalcy	Criminal cases registered	Brief of Input/ Alert/ Occurrence	Follow up action	Remarks									
							Input (Information)		Output (Alert)		Occurrence (Event)					Dead	Injured	Victim																
							Input No.	Received From	Output No.	Seen	Zone	Division																						
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25										
Theatre (Column 4) will include data regarding: - (a) J&K, (b) LWE, (c) North East, (d) Others																																		
Activity (Column 5) will include: - a) Sabotage, (b) Shoot Out, (c) Attack on Security Forces, (d) Bomb Blast, (e) Recovery of Explosives, (f) Damage to Railway Property, (g) Tampering of Track, (h) Obstruction to track, (i) Recovery of A/A, (j) Kidnapping of Railway Employee, (k) Pasting / distribution/ recovery of posters/ sighting banners/ Pamphlet, Graffiti, (l) Threat Call/ Letters/ Telephone Calls, (m) Law and Order disturbance, (n) rail roko/dharna/agitation (o) Heavy Crowd in Station/ Trains, (p) Hijacking of train, (q) Arrest of terrorist/ suspected terror activist/ LWE Cadre/ Insurgent, (r) Recovery of Narcotic/ FICN, (s) Movement of Terrorist/ LWE/ Insurgent (t) Any Other Input/ Output/ Incident																																		

ANNEXURE – 5

YEARLY REPORT ON STATUS OF THE EMPLOYEES

Name _____ of _____ the _____ Railway
Unit.....No.....Date.....

SUBJECT: Yearly report of State of Employees of the Railway Unit as on 1st
January.....

The state of employees etc. of this unit as on 1st day of
January.....is furnished as under.

Category	Indian Nationals	Foreign Nationals	Grand Total
	Male/Female Total	Male/Female Total	Male/Female

- a) Total Railway Employees
- b) Permanent
- c) Temporary
- d) Casual or daily wages
- e) Trainees
- f) Others (Contractual Employees)
- g) Total

.....
A) In case of Foreign Nationals, details of their countries and terms of
engagement etc., are to be enclosed in a separate sheet.

B) Contractor's Workers showing names of each Contractor with comments
on status of their police Verification

C) Details of Private Security Personnel etc. if any, rank and category wise
showing deployment and duty point.

D) Details of any other Agencies like Police, Home Guard looking after
security duties of the Railway Unit & their deployment locations etc.

E) Any ether relative information considered essential for Difficulties and
Suggestions.

ANNEXURE - 6

RAILWAY UNIT AT A GLANCE

1. Name of the Railway Unit and its location
2. Location of the Unit Headquarter
3. Date on which the Railway Unit came into existence.
4. Date of induction of RPF in the concerned Unit
5. Nearest Railway Station and distance in Kms from the unit, with telephone numbers
6. Nearest Police Station with Telephone No. and address.
7.
 - a) Head of the Railway Unit
 - b) Other important Railway Officers like Medical, Safety Departments of the Railway Unit.
 - c) Dist. Magistrate.
 - d) Sr. Supdt. of Police/Supdt. of Police.
8. Security Category, if any (based on whether Industrial Security Team of the IB has done Security Audit).

ANNEXURE - 7

STRIKE/PROTECTION SCHEME OF THE RAILWAY UNIT

Zone

Divisional

Unit.....

.....

.....

.....

.....

Sl. No	Name of the Divisional Unit	Name of the GO/ RPF	Whether Strike scheme have been drawn or not	Who prepared the scheme	Has Management approved it	Has it been vetted by State Govt. or not
(1)	(2)	(3)	(4)	(5)	(6)	(7)

If, answer to Col. 7 is negative state any other Remark	Competent authority who has vetted the Scheme.	If not vetted by any Competent Authority, what further action is being taken to get it vetted
(8)	(9)	(10)

ANNEXURE – 8

QUARTERLY REPORT ON SECURITY CHECK OF SW DIVISIONAL UNIT FOR THE QUARTER ENDING.....

- i.** Name of the Office.
- ii.** Name of the Branch/Section checked.
- iii.** Are any improvements necessary in the Security of the Building?
- iv.** Are arrangements for security for duplicates keys satisfactory?
- v.** Is provision of Locks, Steel Almirahs are satisfactory?
- vi.** Are seals numbered and accounted for?
- vii.** Is The Procedure for copying printing of document is safe?
- viii.** Are the Classified Registers properly maintained?
- ix.** Are the computers system of the office safe in view of data/documents as well as cyber threats?
- x.** Are the Classified Waste Materials burnt under supervision?
- xi.** Is an account of note books kept and their issue and destruction done properly?
- xii.** Are the new hands briefed about security regulations in the SW Wing?
- xiii.** Has there been any case of breach of security during the quarter? If so, give details.
- xiv.** General Remarks, if any

Signature of inspecting Officer

Name & Designation

Station:

Place

Annexure 9

Syllabus for induction course (2 weeks) for RPF staff screened for SIB:

THE ART AND CRAFT OF INTELLIGENCE

Chanakya: “ A greedy person can be cultivated by gift, a gentleman by bestowing honour, a scholar by intelligent discussion, a weak person by thrashing or lackmail”

COURSE CONTENT FOR INTELLIGENCE MODULE

(DURATION: 02 WEEKS)

Intelligence: An Introduction

- 1- Definition of Intelligence
 - 2- Difference between Intelligence and Information
 - 3- Intelligence as Information (To enable the Railways to formulate and implement its policies against internal/ external security threats) and as activities.
 - 4- 4 D's of Intelligence Process (Detecting, Differentiating, Distinguishing and Disseminating)
 - 5- Structure of Intelligence set up at National level and state level
 - 6- Structure of Intelligence set up in the RPF
 - 7- Qualities of Intelligence Officer/ Staff
 - 8- Aids in Interrogation:
 - a. Human Aids
 - b. Chemical Aids
 - c. Scientific Aids
 - d. Psychological Aids
 - 9- Pit Falls to be avoided during Interrogation
 - 10- Documentation of Interrogation
 - 11- **Role Playing Exercise of Interrogation** in which each participant will interrogate a suspect by utilizing anyone type of interrogator role play among sympathetic or benign, School Master or idiotic types of interrogator
- Home Assignment: Interrogation report writing by each** participant in the prescribed format

Objectives of Intelligence Collection

Objectives:

- a. Survival needs of the Organisation,
- b. Understanding the enemy,
- c. Safeguarding various constitutional orders,
- d. Protecting the organization from elements of surprise,
- e. Ensuring the welfare of state and the public order,
- f. Monitoring performance of various wings of the Railways

Types of Intelligence

- 1- Tactical Intelligence (For short term objectives).
- 2- Operational Intelligence (For providing detailed and enhance understanding)
- 3- Strategic Intelligence (For long term objectives)
- 4- Defensive Intelligence (2 D's: Detect and Deter)
- 5- Black Intelligence (Covert Intelligence)
- 6- White Intelligence (Overt Intelligence)
- 7- Hard Intelligence
- 8- Soft Intelligence

Steps of Intelligence Process

- 1- Planning
- 2- Collection (Types of Sources (Open Sources and Covert Sources (HUMINT, SIGINT, IMINT, PHOTINT, ELINT, NUCINT, RADINT, MASINT, TECINT))
- 3- Evaluation (Evaluation Criteria for Validity of Data and Reliability of the Sources based on Grading A1, B2, C3 etc.)
- 4- Collation (Different Methods of Collation)
- 5- Analysis (5 W's: Who, What, When, Where and How, Data Integration and Clarification, Inference development, Inference testing, Finalising relevant and meaningful inferences fro the user etc.)
- 6- Dissemination
- 7- Review/ Feedback (Importance of Review/ Feedback Mechanism, Different types of feedback Mechanisms)

Intelligence Trade Craft

- 1- Intelligence terminology
- 2- Definition of Trade Craft
- 3- Trade Craft Terminology:
 - a. Secret Enquiry
 - b. Surveillance
 - c. Agent Running
 - d. Cover and Alibi
 - e. Communication
 - f. Search and Concealment
 - g. Interrogation

Secret Enquiry

- 1- Secret Enquiry: An Introduction (Anatomy of the Secret Enquiry)
- 2- Essential Components of Secret Enquiry
- 3- Scope and utility (Short term/ Long term)
- 4- Principals of Secret Enquiry
- 5- Process of Secret Enquiry:
 - a. Preparation/ Planning:

- Understanding the task,
- Channels/ Sequencing
- Record Checking,
- Selection of Sources,
- Selection of appropriate cover and alibi for different situations,
- Methodology,
- Adopted/ channels to be used, time setting,
- Assessment of risks or the eventualities,
- Damage control, briefing/ debriefing),
- b. Field operation (steps involved, utility of the time factor, creation of suitable situations)
- c. Repertoire (Format of the report, interim report and final report)
- Field exercise involving live situation.

Surveillance

- 1- Definition
- 2- Surveillance Terminology (Pick up, rendezvous etc.)
- 3- Objectives of Surveillance
- 4- Principles of Surveillance
- 5- Types of Surveillance: (General and Technical):
 - a. General Surveillance: Static (Fixed Area and Fixed Point) and Mobile Surveillance (Foot and Vehicular Surveillance)
 - b. Technical Surveillance:
Visual and Audio Surveillance including bugging
- 6- Process of Surveillance:
 - a. Planning
 - b. Briefing
 - c. Pick-Up
 - d. Follow
 - e. Housing
 - f. Reporting
 - g. Debriefing
 - h. Report writing
- 7- Mobile Surveillance:
 - a. Foot Surveillance:
Straight Line System,
Parallel or T System,
ABC Position,
Lead, Back Up, Rover,
Lead Watcher, Back Up Watcher etc.
 - b. Vehicular Surveillance:
Role of footman,
Qualities of driver,
Caravan System and Parallel System
- 8- Static Surveillance:
 - a. Utility and scope
 - b. Methodology
 - c. Static Surveillance in covered spaces and open public areas
 - d. Process:

Planning and preparation,

Briefing to the watchers,
Pick-Up,
Deployment of teams at the rendezvous,
Identification of the Suspect,
Rotation of Teams,
Housing,
Debriefing,
Report Writing (Format and essential ingredients of Report Writing)

- e. Equipments
- f. Do's and Don'ts

9- Field Exercise (Operation SSX: Mix of Static, Foot Mobile Surveillance, Contact Meeting by suspect will take anti-surveillance)

10- Field Exercise (Operation SSX: Mix of Static, Foot Mobile Surveillance, Contact Meeting by suspect will take anti-surveillance)

11- Home Assignment:

Report Writing by each participant about the above mentioned operation SSX as per the prescribed format.

Field exercise related to vehicular surveillance:

Participants may be provided with the necessary equipments, two wheeler/ four wheeler vehicles along with drivers.

Participants may be divided in group of three participants.

Home Assignment: Report writing by each group of participants about the above mentioned vehicular surveillance exercise in the prescribed format.

Agent Running

- 1- Meaning and Scope
- 2- Terminology Used in Agent Running Ops.
- 3- Difference between context, sources and agents
- 4- Types of agents:
 - Resident agent,
 - Illegal resident,
 - Sleeper agent,
 - Agent of influence,
 - Honorary Agent
- 5- Qualities of an agent
- 6- Types of motivation
- 7- Recruitment Process and techniques of agent running:
 - a. Target
 - b. Talent Spotting
 - c. Approval
 - d. continuation
 - e. Motivation
 - f. Training
 - g. Handling
 - h. Payment
- 8- Evaluation: 5 W's (Who, What, When, Where, Why and How)

- 9- Handling over of an agent to a new handler
- 10- Role Playing Exercise by each participant about handling a contact meeting with an agent at a Public Rendezvous.

Please note: The dummy agent will be provided by the Trainer.

Home Assignment:

Report Writing by each participant about the above mentioned role playing exercise in the prescribed format.

Communication

- 1- Definition
- 2- Components:
 - a. Sender
 - b. Receiver
 - c. Information
 - d. Media
 - e. Transmission
 - f. Reception
 - g. Response
- 3- Needs of Communication
- 4- Channels of Communication:
 - a. Normal Channel
 - b. Alternate Channel
 - c. Emergency Channel
- 5- Components of Secret Communication (Requisites, Choice Factors)
- 6- Techniques of Secret Communication by using overt and covert channels
- 7- Terminology used in Secret Communication:
 - a. Dead Letter Box (DLB)
 - b. Portable DLB
 - c. Cut Out
 - d. Courier
 - e. Dead Courier
 - f. Live Courier
 - g. General Courier
 - h. Live Letter Box
- 8- Different types of personal meetings:
 - a. Safehouse meetings
 - b. Meeting on the Move
 - c. Mobile Meeting
 - d. Brush Meeting
 - e. Floating Meeting
 - f. Cover advertisement
- 9- Precautions to be taken during personal meetings
- 10- Do's and Don'ts

Cover and Alibi

- 1- Meaning and Scope

- 2- Difference between cover and Alibi
- 3- Utility of acquiring a suitable cover
- 4- Types of cover:
 - a. Legal Cover
 - b. Illegal Cover
 - c. Short Term Cover
 - d. Long Term Cover
 - e. Official Cover
 - f. Non Official Cover
- 5- Requisites of a Suitable Cover
- 6- Living up a cover
- 7- Preparation of a Cover:
 - a. Change in the Bio-graphical profile
 - b. Change in the Life History
 - c. Training (In Trade Craft, Secret Communications, Handling of difficult unforeseen situations, Local Area Language Training, Knowledge about chemicals used for secret surveillance, Gaining knowledge about History, Geography, Environment, Infrastructure, Cultural Traditions of the target area)
 - d. Finalization of essential equipments, their handling and concealment
 - e. Field Training and Emergency Needs
 - f. Rescue and escape techniques and routes
- 8- Rehearsals, Testing and Modifications
- 9- Requisites of a good Alibi:
- 10- Uses of Alibi
- 11- Types of Alibi:
 - a. Original Alibi
 - b. Alternative Alibi
 - c. Emergency Alibi

Gadgets

- 1- Uses of GPS Technology
- 2- Utility of Data Fusion
- 3- Cryptography and Cryptanalysis
- 4- Virtual and enhanced reality environment and analysis
- 5- Cellular Intercept System
- 6- Surveillance Gadgets:
 - a. Shoe Bugs
 - b. Water cooler sensors
 - c. Peep hole reverser
 - d. Video Camera Pen
 - e. Call Interceptor Software for GSM Mobile Phones
 - f. Body-Worn, Miniature Cameras,
 - g. Dissolving Paper
 - h. Envelope X-ray Spray
- 7- Stingray
- 8- Gossamer
- 9- Hackers Tool Kit

- 10- War Driving
- 11- Phone Cloning Equipments
- 12- MSTDS**
- 13- Steganography
- 14- **Hands on experience** of using the hacker's tool kit in the computer lab for surveillance purposes

Development of Sources

- 1- Meaning of Sources
- 2- Types of Sources:
 - a. Casual Sources
 - b. OBS (Observer Sources)
 - c. Regular Sources
- 3- Level of Sources:
 - a. Local Sources
 - b. District Level Sources
 - c. State Level Sources
 - d. National Level Sources
- 4- Handling of Sources:
 - a. Selection of Safe House
 - b. Signals Involved in identifying the source
 - c. Alternate rendezvous
 - d. Tasking of Source
 - e. Protecting the Identity of the Source
 - f. Preparing his index
 - g. Payment to the Sources
 - h. Source Reports and different grading of reliability
- 5- Source Review

Security Verification in an Organisation

- 1- Meaning and Scope
- 2- Types of Organisational Security:
 - a. Departmental Security:
 - Subversion,
 - Sabotage,
 - Expionage,
 - Negligence,
 - Leakage
 - b. Personnel Security
 - c. Document Security (Category wise Classification of Documents)
 - d. Physical Security (Static Protective Measures, Access Control)
 - e. Electronic Security (Hazard Protection, Hardware Security, Numbering of DVD's, De-gaussing of Hardware components, Precautions to be taken while using the Internet)
 - f. Precautions to be taken while the Internet) along with hands on training in the computer lab

	Monday First Week
10.00-10.40 am	<p align="center">Intelligence: An Introduction</p> <ol style="list-style-type: none"> 1. (Definition of Intelligence) 2. Difference between Intelligence and Information 3. Intelligence as Information (To enable the Railways to formulate and implement its policies against internal/ external threats) and as activities. 4. D's of Intelligence Process (Detecting, Differentiating, Distinguishing and Disseminating)
10.45-11.25 am	<p align="center">Intelligence: An Introduction</p> <ol style="list-style-type: none"> 1. (Structure of Intelligence set up at National level and state level) 2. Structure of Intelligence set up in the RPF 3. Qualities of Intelligence Officer/ Staff)
12.15-12.55 pm	Types of Intelligence
13.00-13.40 pm	<ol style="list-style-type: none"> 1. Tactical Intelligence (For short term objectives). 2. Operational Intelligence (For providing detailed and enhance understanding) 3. Strategic Intelligence (For long term objectives) 4. Defensive Intelligence (2 D's: Detect and Deter) 5. Black Intelligence (Covert Intelligence) 6. White Intelligence (Overt Intelligence) 7. Hard Intelligence 8. Soft Intelligence
15.00-15.40 pm	Steps of Intelligence Process
15.45-16.25 pm	<ol style="list-style-type: none"> 1. Evaluation (Evaluation Criteria for Validity of Data and Reliability of the Sources based on Grading A1, B2, C3 etc.)
16.30-17.10 pm	<ol style="list-style-type: none"> 2. Collation (Different Methods of Collation) 3. Analysis (5 W's: Who, What, When, Where and How, Data Integration and Clarification, Inference development, Inference testing, Finalising relevant and meaningful inferences for the user etc.) 4. Dissemination 5. Review/ Feedback (Importance of Review/ Feedback Mechanism, Different types of feedback Mechanisms)

Time Schedule	Tuesday First Week
10.00-10.40 am	Intelligence Trade Craft
10.45-11.25 am	<ol style="list-style-type: none"> 1. Intelligence terminology 2. Definition of Trade Craft 3. Trade Craft Terminology: <ol style="list-style-type: none"> a. Secret Enquiry b. Surveillance c. Agent Running d. Cover and Alibi e. Communication f. Search and Concealment g. interrogation
11.30am-12.10 pm	<p style="text-align: center;">Secret Enquiry</p> <ol style="list-style-type: none"> 1. Secret Enquiry: An Introduction (Anatomy of Secret Enquiry) 2. Essential Components of Secret Enquiry 3. Scope and utility (Short term/ Long term) 4. Principals of Secret Enquiry
12.15-12.55 pm	<p style="text-align: center;">Secret Enquiry</p> <p style="text-align: center;">Process of Secret Enquiry:</p> <ol style="list-style-type: none"> a. Preparation/Planning (Understanding the task, Channels/Sequencing , Record Checking ,Selection of Sources , Selection of appropriate cover and alibi for different situations , methodology adopted/channels to be used , time setting, assessment of risks of the eventualities damage control, briefing /debriefing) b. Field Operation (steps involved , utility of the time factor, creation of suitable situation). c. Reportoire (Format of the report, interim report and final report)
13.00-13.40pm	Field Exercise involving secret enquiry of an unknown suspect
15.00-15.40pm	
15.45-16.25pm	
16.30-17.10pm	<p style="text-align: center;">Secret Enquiry</p> <p>Reportoire (Format of the report , interim report and final report)</p>

	Home Assignment
	Detailed Report writing by each participant related to the secret enquiry done by him of an unknown suspect.

Time Schedule	Wednesday First Week
10.00-10.40 am	Surveillance 1. Definition 2. Surveillance Terminology (Pick up, rendezvous etc.) 3. Objectives of Surveillance 4. 4- Principles of Surveillance
10.45-11.25 am	Surveillance Types of Surveillance (General and Technical) a. General Surveillance: Static (Fixed Area and fixed Point) and Mobile Surveillance (Foot and Vehicular Surveillance) b. Technical Surveillance: (Visual and Audio Surveillance including bugging)
11.30am-12.10 pm	Surveillance Process of Surveillance
12.15-12.55 pm	a. Planning b. Briefing c. Pick-Up d. Follow e. Housing f. Reporting g. Debriefing h. Report Writing
13.00-13.40 pm	Surveillance Mobile Surveillance a. Foot Surveillance (Straight Line system, Parallel or T System, ABC Position, Lead, Back Up, Rover, lead Watcher, Back Up Watcher etc.)
15.00-15.40 pm	Surveillance

	<p style="text-align: center;">Mobile Surveillance</p> <p>a. Vehicular Surveillance (Role of footman, Qualities of driver, Caravan System and Parallel System)</p>
<p style="text-align: center;">15.45-16.25 pm</p>	<p style="text-align: center;">Surveillance</p> <p style="text-align: center;">Static Surveillance</p> <p>a. Utility and scope</p> <p>b. Methodology</p> <p>c. Static Surveillance in covered spaces and open public areas</p> <p>d. Process (Planning and preparation, Briefing to the watchers, Pick-Up, Deployment of teams at the rendezvous, Identification of the Suspect, Rotation of Teams, Housing, Debriefing, Report Writing (Format and essential ingredients))</p> <p>e. Equipments</p> <p>f. Do's and Don'ts</p>

Time Schedule	Thursday First Week
10.00-10.40 am	<p style="text-align: center;">Surveillance</p> <p>a. Field Exercise (Operation SSX: Mix of Static, Foot Mot Surveillance, Contact Meeting by suspect who will take and surveillance measures)</p> <p>b. Home Assignment:</p> <p>Report Writing by each participant about the above mentioned operation SSX as per the prescribed format.</p>
10.45-11.25 am	
11.30am-12.10 pm	
12.15-12.55 pm	
13.00-13.40 pm	
15.00-15.40 pm	<p style="text-align: center;">Surveillance</p> <p>a. Debriefing</p> <p>b. Report Writing by each participant about the above mentioned operation SSX as per the prescribed format (Time allowed: 40 Minutes).</p>
15.45-16.25 pm	
16.30-17.10 pm	

Time Schedule	Friday First week
10.00 -10.40 am	<p style="text-align: center;">Agent Running</p> <ol style="list-style-type: none"> 1. Meaning and Scope 2. Terminology Used in Agent Running Ops. 3. Difference between context, sources and agents 4. Types of agents (Resident agent, Illegal resident, Sleeper agent, agent of Influence, Honorary Agent) 5. Qualities of an agent 6. Types of motivation
10.45-11.25 am	
11.30am-12.10 pm	<p style="text-align: center;">Agent Running</p> <p>Recruitment Process and techniques of agent running</p> <ol style="list-style-type: none"> a. Target b. Talent Spotting c. Approval d. Continuation
12.15-12.55 pm	

	<ul style="list-style-type: none"> e. Motivation f. Training g. Handling h. payment
13.00-13.40 pm	<p style="text-align: center;">Agent Running</p> <ol style="list-style-type: none"> 1. Evaluation: 5 W's (Who, What, When, Where, Why and How) 2. Handling over of an agent to a new handler
15.00-15.40 pm	<p style="text-align: center;">Agent Running</p>
15.45-16.25 pm	<p>Role Playing Exercise by each participant about handling a contact meeting with an agent at a Pulic Rendezvous. Please note: The dummy agent will be provided by the Trainer.</p>
16.30-17.10 pm	
	<p>Home Assignment:</p> <p>Report Writing by each participant about the above mentioned role playing exercise in the prescribed format.</p>

Time Schedule	Saturday First week
10.00–10.40am	<p style="text-align: center;">Development of Sources</p> <ol style="list-style-type: none"> 1. Meaning of Sources 2. Types of Sources <ul style="list-style-type: none"> a. Casual Sources b. OBS (Observer Sources) c. Regular Sources 3. Level of Sources: <ul style="list-style-type: none"> a. Local Sources b. District Level Sources c. State Level Sources d. National Level Sources

10.45-11.25am	Development of Sources
11.30am-12.10 pm	<ol style="list-style-type: none"> 1. Handling of Sources <ol style="list-style-type: none"> a. Selection of Safe House b. Signals Involved in identifying the source c. Alternate rendezvous d. Tasking of Source e. Protecting the Identity of the Source f. Preparing his index g. Payment to the Sources h. Source Reports and different grading of reliability 2. Source Review
13.00-13.40pm	
15.00-15.40pm	<p style="text-align: center;">Cover and Alibi</p> <ol style="list-style-type: none"> 1. Meaning and Scope 2. Difference between cover and Alibi 3. Utility of acquiring a suitable cover 4. Types of Cover: <ol style="list-style-type: none"> a. Legal Cover b. Illegal Cover c. Short Term Cover d. Long Term Cover e. Official Cover f. Non Official
15.45-16.25pm	<p style="text-align: center;">Cover and Alibi</p> <ol style="list-style-type: none"> 1. Requisites of a Suitable Cover 2. Living up a Cover
16.30-17.10pm	<p style="text-align: center;">Cover and Alibi</p> <ol style="list-style-type: none"> 1. Preparation of a Cover <ol style="list-style-type: none"> a. Change in Bio-graphical profile b. Change in Life History

	<p>c. Training (In Trade Craft, Secret Communications, handling of difficult unforeseen situations, Local Area Language Training, Knowledge about chemical used for secret surveillance, Gaining Knowledge about History, Geography, Environment, Infrastructure, Cultural Traditions of the target area)</p> <p>d. Finalisation of essential equipments, their handling and concealment</p> <p>e. Field Training and Emergency Needs</p> <p>f. Rescue and escape techniques and routes</p>
--	---

Sunday
<p>Field exercise related to the vehicular surveillance</p> <p>Participants may be provided with the necessary equipments, two wheeler/ four wheeler vehicles along with drivers.</p> <p>Participants may be divided in group or three participants.</p> <p>Home Assignment: Report writing by each group of participants about the above mentioned vehicular surveillance exercise in the prescribed format.</p>

Time Schedule	Monday Second week
10.00-10.40 am	<p style="text-align: center;">Cover and Alibi</p> <ol style="list-style-type: none"> 1. Requisites of a Good Alibi 2. Uses of Alibi 3. Types of Alibi <ol style="list-style-type: none"> a. Original Alibi b. Alternative Alibi c. Emergency Alibi
10.45-11.25am	Communication

	<ol style="list-style-type: none"> 1. Definition 2. Components: <ol style="list-style-type: none"> a. Sender b. Receiver c. Information d. Media e. Transmission f. Reception g. Response
11.30am-12.10pm	Communication
12.15-12.55pm	<ol style="list-style-type: none"> 1. Need of Communication 2. Channels of Communication <ol style="list-style-type: none"> a. Normal Channel b. Alternate Channel c. Emergency Channel 3. Components of Secret Communication (Requisites, Choice Factors) 4. Techniques of Secret Communication by using overt and covert channels
13.00-13.40 pm	Communication
	<ol style="list-style-type: none"> 1. Terminology used in Secret Communication: <ol style="list-style-type: none"> a. Dead Letter Box (DLB) b. Portable DLB c. Cut Out d. Courier e. Dead Courier f. Live Courier g. General Courier h. Live Letter Box
15.00-15.40 pm	Communication
15.45-16.25 pm	<ol style="list-style-type: none"> 1. Different types of personal meetings <ol style="list-style-type: none"> a. Safe house meetings b. Meeting on the Move c. Mobile Meeting d. Brush Meeting e. Floating Meeting f. Cover advertisement 2. Precautions to be taken during personal meetings
16.30-17.10 pm	

Time Schedule	Tuesday Second week
10.00-10.40am	Interrogation
10.45-11.25am	<ol style="list-style-type: none"> 1. Meaning and Scope 2. Types of Interrogation <ol style="list-style-type: none"> a. Preliminary Interrogation b. Detailed Interrogation 3. Categories of Interrogates 4. Types of Interrogators <ol style="list-style-type: none"> a. Bully b. Sympathetic or Benign c. School Master d. Human Vulture e. Idiotic
11.30am-12.10pm	Interrogation
12.15-12.55pm	<ol style="list-style-type: none"> 1. Qualities of an Interrogator 2. Planning an Interrogation 3. Techniques of Interrogation 4. Aids in Interrogation <ol style="list-style-type: none"> a. Human Aids b. Chemical Aids c. Scientific Aids d. Psychological Aids 5. Pit Falls to be avoided during Interrogation 6. Documentation of Interrogation
13.00-13.40pm	
15.00-15.40Pm	Role Playing Exercise of Interrogation in which each participant will interrogate a suspect by utilizing anyone type of interrogator role play among sympathetic or benign, School Master or idiotic types of Interrogator
15.45-16.25pm	
16.30-17.30pm	Home Assignment: Report writing by each participant in the prescribed format about the Role Playing Exercise of Interrogation in which each participant will interrogate a suspect by utilizing say one type of interrogator role play among the sympathetic or benign, School Master or idiotic types of interrogator.

Time Schedule	Wednesday Second Week
10.00-10.40 am	Security Verification in an Organization
10.45-11.25 am	<ol style="list-style-type: none"> 1. Meaning and Scope 2. Types of Organizational Security: <ol style="list-style-type: none"> a. Departmental Security (Subversion, Sabotage, Expionage, Negligence, Leakage)

	b. Personnel Security
11.30-12.10 pm	Security Verification in an Organisation Document Security (Category wise Classification of Documents)
12.15-12.55 pm	Security Verification in an Organisation
13.00-13.40 pm	Physical Security (Static Protective Measures, Access Control)
15.00-15.40 pm	Security Verification in an Organisation
15.45-16.25 pm	
16.30-17.10 pm	Electronic Security (hazard Protection, Hardware Security, Numbering of DVD's, De-gaussing of Hardware components, Precautions to be taken while using the Internet) along with hands on training in the computer lab

Time Schedule	Thursday Second week
10.00-10.40am	Gadgets 1. Uses of GPS Technology 2. Utility of Data Fusion
10.45-11.2Sam	Gadgets 1. Cryptography and Cryptanalysis 2. Virtual and enhanced reality environment and analysis
11.30am-12.10pm	Gadgets Cellular Intercept
12.15-12.55pm	Gadgets Surveillance Gadgets a. Shoe Bugs b. Water cooler sensors c. Peep hole reverser d. Video Camera Pen

13.00-13.40pm	<p style="text-align: center;">Gadgets</p> <ul style="list-style-type: none"> a. Call Interceptor Software for GSM Mobile Phones b. Body-Worn, Miniature Cameras
15.00-15.40pm	<p>Role playing exercise of covering a meeting by using body worn miniature camera, along with creation of a DVD of the recorded evidence in the computer lab.</p> <p>Home Assignment: Report writing about the above mentioned role playing exercise in the prescribed format.</p>
15.45-16.25pm	
16.30-17.10pm	

Time Schedule	Friday Second Week
10.00-10.40 am	Gadgets
10.45-11.25 am	<ul style="list-style-type: none"> a. Dissolving Paper b. Envelope X-ray Spray <ul style="list-style-type: none"> 1. Stingray 2. Gossamer
11.30am-12.10 pm	Gadgets
12.15-12.55 pm	<ul style="list-style-type: none"> 1. War Driving 2. Phone Cloning Equipments 3. Hands on experience about the phone cloning equipments
13.00-13.40 pm	Gadgets
	<ul style="list-style-type: none"> 1- MSTDS 2- Steganography
15.00-15.40 pm	Gadgets
	Hacker's Tool Kit
15.45-16.25 pm	Gadgets
16.30-17.10 pm	Hands on experience of using the hacker's tool kit in the computer lab for surveillance purposes.

Time Schedule	Saturday Second week
10.00-10.40am	Review Session
10.45-11.25am	
11.30am-12.10pm 12.15 - 12.55pm 13.00 - 13.40	Valediction

Report Writing Exercise in the prescribed formats

Secret Enquiry

Detailed Report writing by each participant related to the secret enquiry done by him of an unknown suspect.

Format will be provided by the trainer.

Surveillance

Report writing by each participant about operation SSX as per the prescribed format.

Format will be provided by the trainer.

Agent Running

Report writing by each participant in the prescribed format about handling a contact meeting with agent at a Public Rendezvous.

Format will be provided by the trainer.

Interrogation

Report writing by each participant in the prescribed format about the Role Playing Exercise Interrogation in which each participant will interrogate a suspect by utilizing any one type interrogator role play among the sympathetic or benign, School Master or idiotic types of interrogator.

Field Exercise, Role Playing Exercise and Hands On Experiences

Secret Enquiry

Field Exercise involving secret enquiry of unknown suspect.

Surveillance

Field Exercise (Operation SSX: Mix of Static, Foot Mobile Surveillance, Contact Meeting by suspect who will take anti-surveillance, measures)

Agent Running

1. Role Playing Exercise by each participant about handling a contact meeting with agent at a Public Rendezvous.

Please Note: The dummy agent will be provided by the Trainer.

2. Role playing exercise of covering a meeting by using body worn miniature camera, along with creation of a DVD of the recorded evidence in the computer lab.

Interrogation

Role Playing Exercise of interrogation in which each participant will interrogate a suspect by utilizing any one type interrogator role play among the sympathetic or benign, School Master or idiotic types of interrogator.

Gadgets

Hands on experience of using the hacker's tool kit in the computer lab for surveillance purposes.

ANNEXURE-10

Syllabus for refresher course (one week) for RPF staff working in SIB:

Intelligence: An Introduction

1. Definition of Intelligence
2. Difference between Intelligence and Information
3. Intelligence as Information (To enable the Railways to formulate and implement its policies against internal /external security threats) and as activities.
4. 4 D's of Intelligence Process (Detecting, Differentiating, Distinguishing and Disseminating)
5. Structure of Intelligence set up at National level and state level
6. Structure of Intelligence set up in the RPF
7. Qualities of Intelligence Officer/Staff

Objectives of Intelligence Collection

Objectives:

Safeguarding various constitutional orders,
Protecting the organization from elements of surprise,
Ensuring the welfare of state and the public order,
Monitoring performance of various wings of the Railways

Types of Intelligence

- 1- Tactical Intelligence (For short term objectives).
- 2- Operational Intelligence (For providing detailed and enhance understanding)
- 3- Strategic Intelligence (For long term objectives)
- 4- Hard Intelligence
- 5- Soft Intelligence

Steps of Intelligence Process

- 1- Planning
- 2- Collection (Types of Sources (Open Sources and Covert Sources (HUMINT, SIGINT, IMINT, PHOTINT, ELINT, NUCINT, RADINT, MASINT, TECINT))

3- Evaluation (Evaluation Criteria for Validity of Data and Reliability of the Sources based on Grading A 1, 82, C3 etc.)

4- Collation (Different Methods of Collation)

5- Analysis (5 W's: Who, What, When, Where and How, Data Integration and Clarification, Inference development, Inference testing, Finalising relevant and meaningful inferences for the user etc.)

6- Dissemination

7- Review/ Feedback (Importance of Review/ Feedback Mechanism, Different types of feedback Mechanisms)

Intelligence Trade Craft

1. Intelligence Terminology
2. Definition of Trade Craft
3. Trade Craft Terminology:
 - a. Secret Enquiry
 - b. Surveillance
 - c. Cultivation of Sources
 - d. Cover and Alibi
 - e. Communication
 - f. Gadgets

Secret Enquiry

- 1- Secret Enquiry: An Introduction (Anatomy of the Secret Enquiry)
- 2- Essential Components of Secret Enquiry
- 3- Scope and utility (Short term/Long term)
- 4- Principals of Secret Enquiry
- 5- Process of Secret Enquiry:

Preparation/ Planning:

Understanding the task
Channels/Sequencing
Record Checking
Selection of Sources
Selection of appropriate cover and alibi for different situations
Methodology

Adopted/channels to be used, time setting
Assessment of risks or the eventualities
Damage Control
Briefing / Debriefing

- a. **Field Operation** (steps Involved, utility of the time factor, creation of suitable situations)
- b. **Repertoire** (Format of the Report, Interim Report and Final Report)

Field Exercise Involving Live Situation

Surveillance

- 1- Definition
- 2- Surveillance Terminology (Pick up, Rendezvous etc.)
- 3- Objectives of Surveillance
- 4- Principles of Surveillance
- 5- Types of Surveillance: (General and Technical):
 - a. General Surveillance:
Static (Fixed Area and Fixed Point) and
Mobile Surveillance (Foot and Vehicular Surveillance)
 - b. Technical Surveillance:
Visual and Audio Surveillance including bugging
- 6- Process of Surveillance:
 - a. Planning
 - b. Briefing
 - c. Pickup
 - d. Follow
 - e. Housing
 - f. Reporting
 - g. Debriefing
 - h. Report Writing
- 7- **Mobile Surveillance:**
 - a. **Foot Surveillance:**
Straight Line System,

Parallel or T System,

ABC Position,

Lead, Back Up, Rover,

Lead Watcher, Back Up Watcher etc.

b. Vehicular Surveillance:

Role of footman, Qualities of driver, Caravan System and Parallel System.

8- Static Surveillance:

- a. Utility and scope
- b. Methodology
- c. Static Surveillance in Covered Spaces and Open Public Areas
- d. Process:
Planning and preparation, Briefing to the watchers, Pick-Up, Deployment of teams at the Rendezvous, Identification of the Target, Rotation of Teams, Housing, Debriefing, Report Writing (Format and essential ingredients of ReportWriting)
- e. Equipment's
- f. Do's and Don'ts

9- Field Exercise (Operation SSX: Mix of Static, Foot Mobile Surveillance, Contact Meeting by suspect will take anti-surveillance measures)

10. Home Assignment:

Report Writing by each participant about the above mentioned operation SSX as per the prescribed format.

Field exercise related to vehicular surveillance:

Participants may be provided with the necessary equipment's, two wheeler/four wheeler vehicles along with drivers.

Participants may be divided in group of three participants.

Home Assignment: Report writing by each group of participants about the above mentioned vehicular surveillance exercise in the prescribed format.

Development of Sources

1. Meaning of Sources
2. Types of Sources:
 - a. Casual Sources
 - b. OBS (Observer Sources)
 - c. Regular Sources
3. Level of Sources:
 - a. Local Sources
 - b. District Level Sources
 - c. State Level Sources
 - d. National Level Sources
4. Handling of Sources:

- a. Selection of Meeting Place
- b. Signals Involved in identifying the Source
- c. Alternate Rendezvous
- d. Tasking of Source
- e. Protecting the Identity of the Source
- f. Preparing his index
- g. Payment to the Sources
- h. Source Reports and different grading of Reliability

5. Source Review

Communication

1- Definition

2- Components:

- a. Sender
- b. Receiver
- c. Information
- d. Media
- e. Transmission
- f. Reception
- g. Response

3- Needs of Communication

4- Channels of Communication:

- a. Normal Channel
- b. Alternate Channel
- c. Emergency Channel

5. Terminology used in Secret Communication:

- a. Dead Letter Box (DLB)
- b. Portable DLB
- c. Courier
- d. Dead Courier
- e. Live Courier
- f. General Courier

6. Different types of Personal Meetings:

- a. Meeting on the Move
- b. Open Areas Meetings
- c. Mobile Meeting
- d. Brush Meeting
- e. Floating Meeting

7. Precautions to be taken during Personal Meetings

8. Do's and Don'ts

Gadgets

1. Uses of GPS Technology
2. OSINT Techniques for Intel Collection
3. SOCINT Techniques for Surveillance Work
4. **Surveillance Gadgets:**
 - i. Smart Phones with CUG SIM Cards to all SIB personnel
 - ii. Hidden/Spy cameras
 - iii. Night vision devices
 - iv. CDR Analysis software to analyze CDR/SDR/TDD
 - v. GSM live voice recorder
 - vi. GSM live video recorder
 - vii. Pocket pen voice/ video recorder,
 - viii. Wireless video camera with laptop recorder,
 - ix. Audio/video transmitters that can be concealed
 - x. Audio/video bugs concealed in button/spectacle frame
 - xi. Wide band video UHF link, Laser listening device, video bugs in spectacles, Video bugs in tie pins, digital audio miniature bugs, video bug in button etc.

**Daily Time
Table**

Time Schedule	Monday
10.00 am - 10.40 am	<p style="text-align: center;">Intelligence: An Introduction</p> <ol style="list-style-type: none"> 1. Definition of Intelligence 2. Difference between Intelligence and Information 3. Intelligence as Information (to enable the Railways to formulate and implement its policies against internal / external threats) and as activities. 4. 4D's of Intelligence Process (Detecting, Differentiating, Distinguishing and Disseminating) 5. Structure of Intelligence set up at National level and State Level] 6. Structure of Intelligence Setup in the RPF 7. Qualities of Intelligence Officer/Staff
10.00 am - 10.40 am	<p style="text-align: center;">Objectives of Intelligence Collection</p> <p>Various Objectives (Survival needs of the Organization, understanding the Motives of the Target, safeguarding various Constitutional Orders, protecting the organization from elements of surprise, ensuring the welfare of State and the Public Order, monitoring performance of various wings of the Organisation)</p>
10.45 am - 11.25 am	<p style="text-align: center;">Types of Intelligence</p> <ol style="list-style-type: none"> 1. Tactical Intelligence (For Short Term Objectives). 2. Operational Intelligence (For providing detailed and enhance understanding) 3. Strategic Intelligence (For Long Term Objectives) 4. Hard Intelligence 5. Soft Intelligence

	Steps of Intelligence Process
11.30 am – 12.10 pm	<ol style="list-style-type: none"> 1. Evaluation (Evaluation Criteria for Validity of Data and Reliability of the Sources based on Grading A1, 82, C3 etc.) 2. Collation (Different Methods of Collation) 3. Analysis (5 W's: Who, What, When, Where and How, Data Integration and Clarification, Inference development, Inference testing, Finalising relevant and meaningful inferences for the user etc.) 4. Dissemination 5. Review/ Feedback (Importance of Review/ Feedback Mechanism, Different types of feedback Mechanisms)
12.15 pm - 12.55 pm	Intelligence Trade Craft
	<ol style="list-style-type: none"> 1. Intelligence Terminology 2. Definition of Trade Craft 3. Trade Craft Terminology: <ol style="list-style-type: none"> a. Secret Enquiry b. Surveillance d. Development & Running of Sources e. Communication
13.00 pm - 13.40 pm	Secret Enquiry
	<ol style="list-style-type: none"> 1. Secret Enquiry: An Introduction (Anatomy of Secret Enquiry) 2. Essential Components of Secret Enquiry 3. Scope and Utility (Short term/Long term) 4. Principles of Secret Enquiry <p style="text-align: center;">Process of Secret Enquiry:</p> <ol style="list-style-type: none"> a. Preparation/Planning (Understanding the task, Channels/Sequencing, Record Checking, Selection of Sources, Selection of appropriate cover and alibi for different situations, methodology adopted/ channels to be used, time setting, assessment of risks of the eventualities, damagecontrol, briefing/ debriefing) b. Field Operation (steps involved, utility of the time factor, creation of suitable situation). <p style="text-align: center;">Repertoire (Format of the Report, Interim Report and Final Report)</p>
15.00 pm - 15.40 pm	Field Exercise involving Secret Enquiry of a Target

<p>15.45 pm - 16.25 pm</p> <p>16.30 pm - 17.10 pm</p>	<p style="text-align: center;">Home Assignment</p> <p>Detailed Report writing by each Participant related to the secret enquiry done by him of a Target</p>
<p style="text-align: center;">Day 2</p>	
<p>Time Schedule</p>	<p style="text-align: center;">Tuesday</p>
<p>10.00 am - 10.40 am</p>	<p style="text-align: center;">Surveillance</p> <ol style="list-style-type: none"> 1. Definition 2. Surveillance Terminology (Pick up, rendezvous etc.) 3. Objectives of Surveillance 4. Four Principles of Surveillance <p style="text-align: center;">Surveillance</p> <p style="text-align: center;">Types of Surveillance (General and Technical)</p> <ol style="list-style-type: none"> a. General Surveillance: Static (Fixed Area and Fixed Point) and b. Mobile Surveillance (Foot and Vehicular Surveillance) <p>Technical Surveillance: (Visual and Audio Surveillance including Bugging)</p>
<p>10.45 am - 11.25 am</p>	<p style="text-align: center;">Surveillance Process of Surveillance</p> <ol style="list-style-type: none"> a. Planning b. Briefing c. Pickup d. Follow e. Housing f. Reporting g. Debriefing h. Report Writing

<p>11.30 am – 12.10 pm</p>	<p style="text-align: center;">Surveillance Mobile Surveillance</p> <p>a. Foot Surveillance:</p> <ul style="list-style-type: none"> • Straight Line System • Parallel or T System • ABC Position, Lead • Backup • Rover • Lead Watcher • BackUp Watcher etc. <p style="text-align: center;">Mobile Surveillance</p> <p>a. Vehicular Surveillance:</p> <ul style="list-style-type: none"> • Role of Footman • Qualities of Driver • Caravan System and Parallel System
<p>12.15 pm - 12.55 pm</p>	<p style="text-align: center;">Static Surveillance</p> <p>a. Utility and scope</p> <p>b. Methodology</p> <p>c. Static Surveillance in Covered Spaces and Open Public Areas</p> <p>d. Process:</p> <ul style="list-style-type: none"> • Planning and Preparation • Briefing to the Watchers • Pickup • Deployment of teams at the Rendezvous • Identification of the Target • Rotation of Teams • Debriefing • Report Writing (Format and Essential Ingredients) <p>e. Equipment</p> <p>f. Do's and Dont's</p>
<p>13.00 pm - 13.40 pm</p>	<p>Lunch Break followed by Field Exercise - Operation</p>
<p>15.00 pm - 15.40 pm</p>	<p>SSX: Mix of Static Foot Mobile Surveillance, Contact Meeting by Dummy Target who will take Anti-Surveillance Measures)</p>
<p>15.45 pm - 16.25 pm</p>	

16.30 pm - 17.10 pm	<ul style="list-style-type: none"> a. Debriefing b. Report Writing by each Participant about the above mentioned Operation SSX as per the prescribed format (Time allowed: 40 Minutes)
Day 3	
Time Schedule	Wednesday
10.00 am - 10.40 am	<p>Cultivation of Sources:</p> <ul style="list-style-type: none"> 1. Meaning of Sources 2. Types of Sources: <ul style="list-style-type: none"> a. Casual Sources b. OBS (Observer Sources) c. Regular Sources 3. Level of Sources: <ul style="list-style-type: none"> a. Local Level Sources b. State Level Sources d. National Level Sources
10.45 am - 13.40 pm	<p>Handling of Sources:</p> <ul style="list-style-type: none"> a. Signals Involved in identifying the Source b. Selection of Tasking Location c. Alternate Rendezvous d. Tasking of Source e. Protecting the Identity of the Source f. Preparing his Index g. Payment to the Sources h. Source Reports and different grading of Reliability 2. Source Review
15.00 pm - 15.40 pm	Simulated Exercise on Source Cultivation including RolePlay
15.45 pm - 16.25 pm	
16.30 pm - 17.10 pm	Debriefing Interaction
Day 4	
Time Schedule	Thursday

<p>10.00 am - 10.40 am</p>	<p style="text-align: center;">Communication with Sources</p> <ol style="list-style-type: none"> 1. Definition 2. Components: <ol style="list-style-type: none"> a. Sender b. Receiver c. Information d. Media e. Transmission f. Reception g. Response
<p>10.45 am - 11.25 am</p>	<p style="text-align: center;">Communication</p> <ol style="list-style-type: none"> 1. Need of Communication 2. Channels of Communication <ol style="list-style-type: none"> a. Normal Channel b. Alternate Channel c. Emergency Channel
<p>11.30 am - 12.10 pm</p>	<p style="text-align: center;">Communication</p> <ol style="list-style-type: none"> 1. Brief Exposure to Terminology used in Secret Communication: <ol style="list-style-type: none"> a. Dead Letter Box (DLB) b. Portable DLB d. Courier e. Dead Courier f. Live Courier g. General Courier h. Live Letter Box
	<p style="text-align: center;">Communication</p> <ol style="list-style-type: none"> 1. Different types of Personal Meetings <ol style="list-style-type: none"> a. Meeting on the Move b. Mobile Meeting c. Brush Meeting d. Floating Meeting 2. Precaution to be taken during Personal Meetings

12.15 pm - 12.55 pm & 13.00 pm - 13.40 pm	Simulated Exercise of holding Meeting with the Source in an Open Area Debriefing interaction
15.00 pm - 15.40 pm	<p>Cover and Alibi for Secret Enquiry/ Surveillance</p> <ol style="list-style-type: none"> 1. Cover and Alibi - Meaning and Scope 2. Difference between Cover and Alibi 3. Utility of acquiring a suitable Cover 4. Requisites of a Good Alibi 5. Uses of Alibi <p>3. Types of Alibi:</p> <ol style="list-style-type: none"> a. Original Alibi b. Alternative Alibi c. Emergency Alibi
15.45 pm - 16.25 pm	<ol style="list-style-type: none"> 1. Requisites of a Suitable Cover 2. Living up a cover
16.30 pm - 17.10 pm	<p style="text-align: center;">Cover and Alibi</p> <ol style="list-style-type: none"> 1. Preparation of a Cover <ul style="list-style-type: none"> • Handling of difficult unforeseen Situations • Local Area Language Training • Finalization of Essential Equipment's, their handling and Concealment • Emergency Needs • Escape Techniques and Routes
Day 5	
Time Schedule	Friday
10.00 am - 10.40 am	<p style="text-align: center;">Gadgets</p> <ol style="list-style-type: none"> 1. Uses of GPS Technology 2. Social Profile based SOCINT Techniques
10.45 am - 11.25 am	<p style="text-align: center;">Gadgets</p> OSINT Techniques

<p>11.30 am – 12.10 pm</p>	<p style="text-align: center;">Surveillance Gadgets</p> <ul style="list-style-type: none"> • Shoe Bugs • Peep Hole Reverser • Video Camera Pen • Body Worn, Miniature Cameras
<p>12.15pm-12.55 pm & 13.00 pm-13.40 pm</p>	<p style="text-align: center;">Gadgets</p> <ol style="list-style-type: none"> i. Smart Phones with CUG SIM Cards to all SIBpersonnel ii. Hidden/Spy cameras iii. Night vision devices iv. CDR Analysis software to analyze CDR/SDR/TDD v. GSM live voice recorder vi. GSM live video recorder vii. Pocket pen voice/ video recorder, viii. Wireless video camera with laptop recorder, ix. Audio/video transmitters that can be concealed x. Audio/video bugs concealed in button/spectacle frame xi. Wide band video UHF link, Laser listening device, video bugs in spectacles, video bugs in tie pins, digital audio miniature bugs, video bug in button etc.
<p>15.00 pm - 15.40 pm</p>	<p>Role Playing Exercise of covering a meeting by using body worn miniature camera, along with creation of a Recording of the evidence in the computer lab.</p> <p>Home Assignment: Report writing about the above mentioned Role Playing Exercise</p>
<p>15.46 pm - 16.25 pm</p>	
<p>16.30 pm - 17.10 pm</p>	
<p>Day 6</p>	
<p>Time Schedule</p>	<p>Saturday</p>
<p>10.00 am-10.40 am</p>	<p>Review Session</p>
<p>10.45 am-11.25 am</p>	<p>Syndicate Group Activity on Cultivation of</p>

	Sources
11.30 am-12.10 pm	Role Playing Activity related to Secret Enquiry
12.15 pm-12.55 pm & 13.00 pm-13.40 pm	Simulated Field Exercise on Foot Surveillance
15.00 pm-15.40 pm	Filling up of Feedback Form for Future Training Need Analysis
15.47 pm-16.25 pm	Key Note Speech by an Eminent Speaker Valediction
16.30 pm-17.10 pm	

APPENDIX – 1
(Refer Para 1.4 (a), Chapter 1)

SOURCES

A Source is a Human Being associated with a target, fully motivated and loyal to the Handler. He/She is one of the Main Person responsible for obtaining Authentic Actionable Intel Input.

UTILITY:

- Provides Documents
- Can Forewarn & Forecast
- Can assist Us in Operations
- Can Pinpoint Target's Plans, Modus Operandi, Strength & Weaknesses etc.
- Can Confirm, Contradict & Provide Missing Links of an Information
- Apart from General Information, they are bound to provide specific Information when asked For

TRAITS TO LOOK FOR WHILE SELECTING A PERSON TO ACT AS A SOURCE: The Source to be developed should be:

- ❖ Discreet
- ❖ Faithfull
- ❖ Not Excessively Greedy
- ❖ Manageable (He/She should not be able to control the I.O.)
- ❖ Sound Memory
- ❖ Observant
- ❖ Should have a Cool Temper

MOTIVATION FACTORS WHICH MAKES A PERSON TO ACT AS A SOURCE:

Money, Emotions, Frustration, Ideology, Adventurism, Blackmail etc. are some of the Factors which can be identified by the Handler for Developing Reliable & High Value Sources.

Sources Developed by Exploiting their Emotions or Ideology are generally the Most Reliable Sources. Our Intel Operatives should develop such Sources.

RECRUITMENT PROCESS FLOWCHART:



CULTIVATION OF SOURCES: Handler of the Source has to regularly

Create Situations for frequent Meetings & build Rapport. He should Look after the Material & Emotional Needs of the Source. The Handler should also Elicit Intel about His/Her Financial Needs.

Following Precautions are to be taken by the Handler while Handling their Sources:

- No blind faith on the Source
- Monitoring of Performance, Loyalty, Motive & Accuracy of the Intelligence received Regularly
- No False Promise
- Treat as a Valuable Asset & not as Personal Servant
- Make Payments in time
- Assign task within his Capabilities
- Show sympathetic interest in his Personal Problems
- Review & find out Remedial Measures if Performance Worsens

The RPF Intel Operatives seldom follow these Necessary Tactics – Appropriate Training Interventions are Required.

Payment Criteria: It is decided on Basis Of:

- ❖ No. of Reports
- ❖ Quality & Utility of Report
- ❖ Risk involved
- ❖ Value of the Intelligence.
- ❖ Future Prospects of the Source
- ❖ It is supplemented by Rewards, Gift & reimbursement of other Contingency Expenses - Payment makes a Source Dependent
- ❖ Obtain Receipts – I.O. to keep proper Account
- ❖ No Payment through Cheque or new Currency Notes in running Numbers
- ❖ Evaluate Performance for Raise

Criteria related to Evaluation of Intel Input by the Intel Operative:

5 W's (Who, What, When, Where, Why) regarding Intelligence received from Source are to be checked by the Handler in order to detect missing Links. Accuracy & utility to be evaluated & Graded by the Source Handler

ACTION TO BE TAKEN IN CASES OF DETERIORATION IN INTEL:

Deterioration can be due to:

- Decline in Target's Activities
- Drying up of sub-sources of the Source
- Personal & Family Problems
- Transfer or change in Operational Area of the Source Handler
- Disappearance of Source's Motive
- Source turning Professional & Greedy
- Denial of Raise

Reusing of Source by the New Source Handler: Every Source should be approached by senior officer & registration process should be followed Invariably. Efforts should be made for Establishing Liaison with other Agencies to get their Sources. Intel Operative's work should be judged by number of Sources He/She has in the RPF Intel Setup

.....

APPENDIX – 2

VITAL INSTALLATION

- a)** Vital Installation is an installation in which partial or complete damage would have an immediate and serious impact on the ability and activity of not only that installation, but also other units too which are dependent on this vital installation for their operation like power plant, pump house etc.

- b)** Security of Vital Installation is as important as vital part of any system. It aims at safeguarding the critical installations against unauthorised access as to prevent it against sabotage.

- c)** The security of Vital Installations must be carefully planned, continuously reviewed and aggressively Implemented.

- d)** Security of Vital Installation will depend mainly on two factors i.e., Criticality & Vulnerability. In case, the Installation is both highly critical and highly vulnerable, then apart from the extensive and intensive program of Physical Security & Personnel Security, Security of Information is of Paramount Importance.

- e)** There are a number of installations in this country which are necessary for one's life but all of them cannot be considered essential for the community even though they contribute to the economic life of the country. So, there should be a yard-stick by which the importance of the installations could be

measured, for deciding how far these installations are Essential or Strategic

- f)** There are three basic considerations for judging the importance of installations:
- Is relative importance to the National Economy and Defense Potential.
 - Its Vulnerability, viz, how far the installations is protected and how far the installations is safeguarded against attacks by hostile Powers. This depends upon its Location and other Conditions.
 - Its Replaceability i.e. how far the installations could be replaced if it is damaged, by similar facilities existing in the Country so that alternative arrangements could be made to keep up the Supply.
- g)** Thus, the production capacity of an entire community supporting many industries may be vitally affected by the destruction of an essential facility such as power, water and transportation etc.
- h)** Also, it is necessary that this concept of importance of the installation required continuous analysis. Thus, an installation which is very vital today may be less vital tomorrow, hence, the vital nature of the installation must be determined on the basis of the importance of the facility to the whole scheme of which the installation is a unit. Various installations have been categorized into three categories, namely, category 'A', 'B' & 'C' the definition of which are given below:

CATEGORY 'A'

Units, whose Product or Services are vital to the country's economic and defense potential and whose total loss or service damage will affect many other sectors dependent on them, which are also important from the point of view of economy and defense

CATEGORY 'B'

Units, whose products or service are very important to national economy and defense, and which cannot be replaced in case of total loss or severe damage

CATEGORY 'C'

Units, whose products and services are important to national economy and defense but can be replaced to some extent by the products or services of other units of a similar nature.

Each Divisional SW unit shall furnish information in respect of vital installation so as to reach the Zonal Headquarter where a thorough review may be done and the finalized Report in this regard may be sent to the Intelligence Cell, Security Directorate, Railway Board by 15th June each year. This information is required for keeping the record for meeting emergent exigencies.

The Report may be sent in the following Format:

- i)** Name of the installation
- ii)** Situation and rough sketch of the installation
- iii)** Importance of the installation

iv) Security Arrangements

v) Whether any threat like Fire, Sabotage etc. occurred in the Past? If so, give its full details and state the steps to prevent recurrence of such Incident.

.....

APPENDIX – 3

PROTECTED/PROHIBITED PLACE IN THE DIVISIONAL UNIT

Sub-Section 8 of Section 2 of the Official Secret Act 1923 defines the Prohibited Place as under:

"PROHIBITED PLACE" MEANS:

a) Any work of defense, arsenal, naval, military or Air Force establishment or station, mine, minefield, camp, ship or aircraft belonging to, or occupied by or on behalf of Govt. any military, telegraph or telephone so belonging or occupied, any wireless or signal station or office so belonging or occupied, and any factory, dockyard or other place so belonging or occupied and used for the purpose of buildings, repairing, making or storing any munitions of war or any sketches, plans models or documents relating thereto, or for the purpose of getting any metals, oil or minerals of use in time of war.

b) Any Place not belonging to Govt. where any munitions of war or any sketches, models, plan documents relating thereto are being made, repaired, gotten or stored under contract with, or with any person on behalf of Govt. or otherwise on behalf of Govt.

c) Any Railway, Roadways or Channel, or other means of communication by land or water (including any work or structures being part thereof or connected there with or any place used for gas, water, or electricity works or other works for purpose of a public character, or any place where any munitions of war or any sketches, models, plans or documents

relating thereto, are being made, repaired, or stored otherwise than on behalf of Govt. which is for the time being declared by the Central. Govt. by notification in the official Gazette, to be a prohibited place for the purpose of this Act on the ground that information with respect thereto, or the destruction or obstruction thereof, or interference therewith, would be useful to an enemy and to which a copy of the notification in respect thereof has been affixed in English and in the vernacular of the locality".

SKETCH

Sketch includes any photographs or other models of representing any place of thing.

The Photography in a prohibited place is strictly forbidden.

No Photography of the installation or any part thereof is allowed if it is:

- a)** a "Prohibited Place" under the Official Secrets Act: or
- b)** a "Protected Place" or area under the Defense of India Act & Rules: or
- c)** Has a Special Enactment for itself in which photography has been Prohibited.

The Unit Head shall ensure that the Management gets the concerned undertaking or its part thereof, failing under the provision of Sub-Section 2 of Official Secrets At, 1923. declared as Prohibited Place by the concerned State Govt. and notification thereof both in English and vernacular of the locality is affixed at the gate and prominent place shall be

written in block letters in red having the background of the board painted with white colour.

Report Format: All Zonal/PUs RPF Heads shall submit to Security Directorate, Railway Board, a Report in respect of Protected/Prohibited Place in the Railway Units falling within their jurisdiction as per instructions as under:

- a)** Name of the point, place, building, area etc.
- b)** General situation and a rough sketch of it,
- c)** Importance of the point, place, building etc and its use.
- d)** Reasons for declaring prohibited/protected place.
- e)** Security arrangements.
- f)** Has any threat like sabotage, fire etc. occurred in the Past?. If so, give full details and steps taken to prevent recurrence.
- g)** Any other useful information

.....

APPENDIX – 4

SECURITY CLEARANCE TO FOREIGNERS COMING TO A RAILWAY UNIT

There are various instances of Foreigners coming for meetings in the Railway Unit as Representatives of Foreign Railways/MNCs or for any other Work as the Case May be.

FOREIGNERS VISITING VITAL INSTALLATIONS:

A. CASUAL VISITORS:

In the case of foreigners desiring to visit vital installations for the purpose of sight seeing it has been decided that no prior reference need be made to Home Ministry for security clearance. The visits may be permitted by the security officers of the concerned installations subject to the observance of the following conditions:

- 1.** The visit is confined to nonstrategic areas in the installations which should be clearly demarcated in advance.
- 2.** The visit to non strategic area is so conducted that the visitors do not have any close view of the security areas.
- 3.** The unit's RPF Officer shall accompany the visitor's group.
- 4.** No photography of the installations or any Part thereof is allowed if it is –
 - a.** Protected Place or area under the Defense of India Act and Rules or
 - b.** A Prohibited Place (under the Official Secret Act) or
 - c.** Has a special enactment for itself in which photography has been prohibited.

B. TRAINING/EMPLOYMENT

In the case of foreigners who are coming for training or employment in any vital installation, a prior reference should be made to Home Ministry for security clearance and the training/employment should be allowed only after Home Ministry's clearance is obtained.

C. FOREIGNERS UNDERGOING TRAINING IN ONE INSTALLATION VISITING ANOTHER WHILE UNDER TRAINING

In the case of a foreigner who has been cleared from the security angle for training in an installation under one Ministry, it is not necessary to obtain further clearance to visit any other installation under the same Ministry, when the visit is part of the training course. However, if the installation to be visited is under another Ministry/Department, it should be necessary to get the clearance of that Ministry/department who may in case of doubt, consult this Ministry also.

RESTRICTED AND PROTECTED AREAS

A prior reference is necessary for clearance in respect of visits of all foreigner (including Nationals of commonwealth countries, diplomats etc to the protected and restricted areas). It is essential that while making reference for security clearance information on the following points should invariably be furnished to Home Ministry.

- 1. Full name (expanding the initials)**

- 2.** Nationality
- 3.** Date of birth
- 4.** Parentage
- 5.** Present Address
- 6.** Permanent address
- 7.** Passport number date and place of issue and its validity if available.
- 8.** Occupation and
- 9.** Whether previously in India, if so, date and place of previous visit.

.....