No. 1-6/2025/NCA.TS

भारत सरकार / Government of India

संचार मंत्रालय/ Ministry of Communications

दूरसंचार विभाग/ Department of Telecommunications

राष्ट्रीय संचार अकादमी-प्रौद्योगिकी/National Communications Academy-Technology

Dated: 09 March, 2026

Subject: **Inviting nominations for the Batch-II of Competency Development Program (CDP) in 'Network and Mobile Security' being organized by NCA-T Ghaziabad**

R/Ma'am/Sir(s),

I am directed to inform that in order to create network and cyber security domain experts in Department of Telecommunications (DoT), the Department has approved conduction of Batch-II of Competency Development Programme in 'Network and Mobile Security' by National Communications Academy-Technology, Ghaziabad,

2. The curriculum of CDP Batch-II has been re-designed after incorporating the feedbacks received from participants of CDP Batch -I. The program will cover various aspects of network security like Network Security and Components (Firewalls, IDPS etc.), OS Hardening and Virtualization, Network Traffic Analysis, Cryptography, Log analysis, Vulnerability Analysis & Penetration Testing basics, Software Security and Threat intelligence, OSINT, Network and Digital forensics, Mobile and Social Media Forensics, Protocol Header Analysis, IPDR Analysis etc. including various international certifications in cyber security. The tentative schedule of CDP Batch II is attached in Annexure-I.

3. The CDP Batch -II shall comprise of officers from ITS Group 'A', JTO Group 'B', IP&TAFS Group 'A' and WPC Group 'A' of Department of Telecommunications. Preference will be given to officers of DoT working at Director / ADG / ADET / JTO level in the order of seniority. The proposed batch size for the program is 20 to 25. The maximum nominations from IP&TAFS Group-A and WPC Group-A shall be 5 (IP&TAF Group 'A' – 3 nominations and WPC Group 'A' – 2 nominations). However, NCA-T reserves the right to increase or decrease the number of seats among ITS Group 'A'/ JTO Group 'B'/ IP&TAF Group 'A' and WPC Group 'A', in case lesser number of nominations are received from IP&TAFS Group 'A' and WPC Group 'A'.

4. The entire cost of the training for the DoT officers will be borne by NCA-T except for TA/DA. The participating officers will have to take care of their lodging and boarding as per their official entitlements, as per rules.

5. Further, keeping in view the relevance of capacity building in telecom security for DoT PSU's (BSNL / MTNL / TCIL / ITI) and C-DoT, maximum of 5 nominations are also invited from the officers of DoT PSU's (BSNL / MTNL- 2 Nominations; TCIL- 1 Nomination; ITI – 1 Nomination) and C-DoT – one nomination, **purely on a cost basis**, without any training fee waiver. However, NCA-T reserves the right to increase or decrease the number of seats among ITS Group 'A'/ JTO Group 'B'/PSU(s), in case lesser number of nominations are received from respective PSUs & CDoT.

Any additional information / details related to these training, if required by the PSUs and CDoT can be sought by sending request on email id: dir.ts-ncat-dot@gov.in. It is to mention that the expenditure towards boarding / lodging and TA/DA is also to be borne by the respective organizations.

6. The selection criteria of candidates will broadly be based on the following parameters:

- Educational Qualifications
- Additional acquired knowledge needed to be the Domain Expert
- Demonstration of stand-apart knowhow in the domain
- Proven research and development track record in the domain
- Additional working experience in the domain
- ACR track of last 5 years mentioning special attributes and innovative technology solutions in the domain.

7. The participating officers in CDP Batch-II shall be mandatorily required to undergo all the three phases of training, including passing of all the exams and certifications to be undergone during training. In case, an officer opts to leave the course in between, NCA-T Ghaziabad reserves the right to recover the cost of the training including any cost borne by the government/agency concerned on training. *Further, officers of DoT applying for the CDP Batch II shall note that they may be required to serve in the department in Telecom Security domain for a period of five years.*

8. The participating organizations/agencies will be providing computers/desktops during official training at their campus. However, officers will be advised to carry their own laptops with them for ease in learning and self-study.

9. In view of the above, nominations are hereby invited in the duly filled form (Annexure-II) from officers of DoT and officers of DoT PSUs to take part in the Batch-II of the Competency Development Programme on 'Network and Mobile Security'. Interested officers are requested to forward the duly signed/approved nomination form by the respective Head of the controlling units/competent authority to the email id mentioned as: jtots-ncat@gov.in

10. The last date to send the duly filled nominations (Annexure-II) is **27th March 2026.**

VISHAL DHEER
Digitally signed by VISHAL DHEER
Date: 2026.03.09 17:08:06 +05'30'

(Vishal Dheer I.T.S.)
Director (TS), NCA-T
Email: dir.ts-ncat-dot@gov.in

Enclosures:

1. Annexure-I: Tentative Schedule of Batch-II the CDP.
2. Annexure-II: Application form for nomination in CDP B-II.
3. Annexure-III: Handbook for CDP Batch-II.

To:

1. DG(Telecom)/ All the Heads of LSAs/ DG(NCA-F)/ DG(NCA-W)/ Sr. DDG(TEC)/ Sr. DDG(NCCS)/ CGCA
2. CMD (BSNL)/ CMD(MTNL)/ CMD(TCIL)/ CMD(ITI) and CEO (C-DoT)
3. All DDGs DoT HQ/ DDG(NOCC)/ Administrator (DBN)/ Wireless Advisor, DoT

Copy to:

1. Member (Services)/ Member (Technology)/ Member (Finance), Digital Communications Commission, Sanchar Bhawan, New Delhi
2. Sr. PPS to Wireless Advisor, Sanchar Bhawan, New Delhi
3. PPS to DG (NCA-T), Ghaziabad
4. Sr. DDG(Pers), DoT HQ
5. DDG(Trg), CBT Division, DoT HQ
6. DDG(TM)/ DDG(Admn.), NCA-T Ghaziabad

Annexure-I

Tentative Scheme and Schedule of the Batch-II of Competency Development Programme (CDP) in "Network and Mobile Security":

Phase	**Duration**	**Course Conducting Institute**	**Level**
Phase I	2 weeks	**CDAC, Noida**	Fundamental
Phase II	6 weeks	**Part1**: 1 week at **NCA-T**	Advanced
		Part2: 3 weeks at **CDAC, Noida** and	
		Part3: 2 weeks at **NFSU, Gandhinagar**	
Phase III	To be decided	To be decided ***(3-4 Months)***	Certification Level

* The program is likely to commence in Quarter-1, FY-2026-27. This will not be a continuous program and the training in the three phases will be organized depending upon the availability of slots in the participating institutes.

Annexure-II

APPLICATION FORM FOR CDP B-II – NETWORK AND MOBILE SECURITY

01	Name of the officer in BLOCK letters				
02	Service				
03	Department / Organization				
04	Present post and date since held				
05	Staff number (as per blue book)				
06	Office Address				
07	Mobile Number				
08	Email Address (GOV/NIC)				
09	Date of Birth				
10	Age as on 1st Jan 2026				
11	Date of Retirement				
12	Date of entry into service				
13	Educational Qualifications (Graduation & onward)				
	Qualification	Subject/Stream	Institute	Year of pass-out	
14	Particulars of post held during during past ten years				
	Post & Place	From	To	Nature of Duties	
15	Details of training program attended in past ten years				
	Name of course/ training	Year	Institute of training	Duration	
16	APAR rating for past five years				
	2024-25	2023-24	2022-23	2021-22	2020-21

17	Technical Knowledge and Domain Experience related with Network Security (Describe in max. 250 words)	
18	Additional information related with your suitability for the Competency Development program on Network Security (Describe in max. 250 words)	
19	Any vigilance or disciplinary case against you in past or pending currently	
	If YES, status and penal details	

Declaration:

1. I certify that the information given in this application form is correct and true to the best of my knowledge.
2. I shall mandatorily undergo all the three phases of training, including passing of all the exams and certifications to be undergone during training.

3. I agree to abide by the decision of the authorities concerned regarding my selection to the program.
4. In case, I opt to leave the course in between then NCA-T, Ghaziabad reserves the right to recover the cost of the training including any cost borne by the government/agency concerned on training.

Place:

Signature of the applicant

Name:.....

Designation:.....

Date:.....

Approval of Head of Unit

1. Certified that the service particulars given by the applicant have been verified from his/her service records and found to be correct.
2. Also the officer will be relieved for all the spells/phases of the training of this program, as and when required.

Place:

Signature with seal of the Competent Authority

Name.....

Designation .....

Date.....

Annexure-III

National Communications Academy – Technology, Ghaziabad

Handbook

for

Competency Development Program (Batch II)

on

"Network and Mobile Security"

Course Conducting Division: TS&PR, NCA-T Ghaziabad

1. INTRODUCTION

The telecommunications sector forms the backbone of India's digital ecosystem, enabling seamless connectivity, communication, and data exchange that power critical services across governance, finance, healthcare, transportation, and other key sectors. Its infrastructure underpins not only routine digital interactions but also the functioning of national security systems and essential public utilities. Recognizing its indispensable role and the cascading impact that any disruption could have on the nation's economy and security, the **National Critical Information Infrastructure Protection Centre (NCIIPC)** has declared the **telecommunications sector** as a **Critical Information Infrastructure (CII)**. This designation underscores the sector's strategic importance and the imperative for robust security frameworks, operational resilience, and sustained investment to safeguard it against emerging and evolving threats.

This national priority is further reinforced through the **Telecommunications Act, 2023**, the **Telecommunications (Telecom Cyber Security) Rules, 2024**, and the **Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024**, which mandate all telecommunications entities to adhere to prescribed norms for maintaining a strong cyber security posture. These regulatory frameworks place clear responsibility on Telecom Service Providers (TSPs) and Internet Service Providers (ISPs) to secure and safeguard communication networks, ensure cyber safety, and institutionalize regular security audits and certifications as part of their license obligations.

India's telecom ecosystem, with approximately 1.2 billion mobile connections and massive volumes of call data records (CDRs), location data, and digital financial transactions, is uniquely vulnerable to cyber threats. Any compromise—whether accidental or deliberate—in the handling of such sensitive data can have far-reaching implications for national security, law enforcement operations, economic stability, and citizen privacy. At the same time, the limited availability of specialized in-house cyber security expertise across the sector constrains the ability to proactively monitor, detect, and respond to advanced persistent threats (APTs), zero-day exploits, and state-sponsored cyber espionage campaigns, resulting in a largely reactive security posture and increased systemic vulnerabilities.

Globally, it has been observed that a growing number of cyber threats and incidents are being reported to CERTs, making security in networks and distributed systems a major and persistent challenge. The rapid expansion of wireless networks, ad-hoc networks, IoT ecosystems, and sensor-based infrastructures has introduced new dimensions of risk. Additionally, the increasing demand for high-speed communication, when contrasted with the complexity and time-intensive nature of cryptographic and security mechanisms, creates structural vulnerabilities that adversaries continue to exploit.

Communication networks today form the backbone of multiple critical sectors including civil aviation, shipping, railways, power, nuclear, oil and gas, finance, banking, IT, law enforcement, intelligence agencies, space, defence, and government services. These networks face a wide spectrum of threats such as data theft, fraud, denial-of-service attacks, hacking, cyber warfare, terrorist activities, and anti-national operations, executed through vectors including malware, trojans, phishing, network scanning, probing, and social engineering. Emerging threats from social

networks and digital platforms, where vast volumes of personal data are voluntarily shared, further amplify the attack surface.

In this context, strengthening telecom security architectures is not merely a technological requirement but a human and institutional capacity imperative. The effectiveness of frameworks for Cyber Safety, Security, and Assurance at the network level ultimately depends on the competence, preparedness, and strategic insight of regulatory and oversight institutions. **Routine security audits, compliance certifications, and continuous monitoring mechanisms can only deliver meaningful outcomes when driven by well-trained, informed, and empowered officers.** Therefore, focused capacity building of DoT officers assumes critical importance in enabling a shift from a reactive regulatory posture to a proactive, resilient, and intelligence-driven cyber security governance framework, capable of anticipating threats, shaping policy responses, and safeguarding national telecommunications infrastructure.

To address this need, officers of the Department of Telecommunications must be systematically equipped with specialized expertise in the following domains:

- Secure configuration of hardware and software systems
- Continuo vulnerability assessment and risk analysis
- Monitoring and analysis of network and system audit logs
- Detection, analysis, and mitigation of diverse forms of malware
- Secure configuration and management of network devices, including firewalls, routers, and switches
- Network security architecture and boundary defence mechanisms
- Data protection and information assurance
- Incident response, digital forensics, and cyber crisis management
- Penetration testing methodologies and cyber range–based simulation exercises

Under the overarching framework of the Competency Development Programme (CDP), a dedicated Domain Expert vertical on Network and Mobile Security has been formulated. This programme derives its structural and implementation architecture from the CDP framework and is designed for delivery through a three-tier progression model comprising Fundamental, Advanced, and Certification phases.

The programme is intended for officers who demonstrate a strong aptitude for learning and operating in highly technological, computation-intensive, and programming-driven environments. Each phase of the training programme is followed by a rigorous and structured evaluation process, which candidates must successfully clear to become eligible for progression to the subsequent level. This ensures not only skill acquisition but also validated competency development, enabling the creation of a cadre of technically proficient officers capable of addressing complex and evolving cyber security challenges within the telecom ecosystem.

2. PROGRAM LAYOUT

The CDP Batch-II curriculum shall be scheduled in **three phases** with course content to be covered starting from **Fundamental (Phase I)**, **Advanced (Phase II)** followed by **Certification Level (Phase-III**), as tabulated below:

Phase	Duration	Course Conducting Institute	Level
Phase I	2 weeks	**CDAC, Noida**	Fundamental
Phase II	6 weeks	**Part 1**: 1 week at **NCA-T**	Advanced
		Part 2: 3 weeks at **CDAC, Noida** and	
		Part 3: 2 weeks at **NFSU, Gandhinagar**	
Phase III	3-4 Months	This will be informed in due course.	Certification Level

2.1 PHASE-I

Phase-I ***Fundamental level***

To acquaint the selected officers about the preliminary concepts about the domain expert area, the program will start with a two-week "**Level – I course on Cyber Security**" delivered at CDAC, Noida in classroom training, which shall cover the following topics:

- Network fundamentals
- Network Security and Components (Firewalls, IDPS etc.)
- OS Hardening and Virtualization
- Network Traffic Analysis
- Advanced Network security & cryptography
- Introduction to OSINT tool analysis
- Basics of Cyber forensics

Delivery: Duration : Two weeks

a) "Level – I course on Cyber Security" At CDAC-Noida.
b) Focus on theoretical foundation

2.2 PHASE-II

PHASE – II ***Advanced Level***

The officers will be trained in advanced concepts of Communication Network Systems and associated technologies, Network Security and Network Defense, cyber-attack scenarios to web technologies, network security holes in standard networking architecture & protocols and Security in Mobile Platforms. The program shall cover the following topics:

Part 1:

1-week course at NCA-T in Phase-II of CDP B-II will cover overall ecosystem of cyber security in India, recent developments, security ecosystem of India, various initiatives and role of DoT in telecom cyber security including the "Critical Telecom Infrastructure Rules, 2024" & "Telecom Cyber Security Rules, 2024" etc.

Part 2:

a. 3 Week "Level II (Advanced) Level Course on Cyber Security" at CDAC, Noida

- Introduction to Malware Analysis
- Wireless Security
- Configuration, Analysis, and Security controls
- Threat and vulnerability management
- Vulnerability Analysis & Penetration Testing
- Software Security and Threat Intelligence
- Advanced Technologies in Security
- Mobile and Social Media Forensics

Part 3:

a. 1 Week course on "Certified Network Forensics Analyst" at NFSU, Gandhinagar

- Introduction to Network Forensics
- Network architectural challenges and opportunities
- Tools & Technologies of Network Forensics
- Emerging Trends & Technologies in Cyber Crime
- Network evidence types and sources
- Log collection, aggregation, and analysis
- Handling Network Forensics Events & SOP
- Network Pattern analysis of overwhelming threats

- Network Protocol Header Analysis
- IPDR Analysis
- Analysis of Web Application Based Malicious Network traffic
- Network Forensics - Incident Response & Deep Packet Investigation
- Case Studies

b. 1 Week course on "Vulnerability Analysis and Penetration Testing"

- Introduction to Pentesting
- Procedure for Pentesting
- Vulnerability Scanning
- Password Attacks
- FTP Pentesting
- Banner Grabbing/Banner Hiding
- Brute Forcing/Secure
- Pentesting Frameworks
- Deep Packet Inspection
- Web Application Pentest
- OWASP top 10
- Burp Suite
- MAC Address Snooping
- MAC/ARP Spoofing
- Case Studies

Delivery: Duration: 6 weeks

a) 3 weeks "Level II (Advanced) Level Course on Cyber Security for DoT officials": At CDAC, Noida
b) 1 week course on "Certified Network Forensics Analyst": At NFSU, Gandhinagar
c) 1 week course on "Vulnerability Analysis and Penetration Testing": At NFSU, Gandhinagar
d) 1 week course cyber security ecosystem in India at NCA-T

2.3 PHASE-III

PHASE – III ***Certification Level***

The Phase-III of CDP shall be of certification level and the tentative duration shall be 3-4 months. The institute for Phase-III shall be declared in due course.

Delivery: Duration: 3-4 months

a) Institute will be decided in due course
b) Phase -III to focus on certifications

3. STRUCTURE AND NOMINATIONS

The CDP B-II shall comprise of officers from ITS Group 'A', JTO Group 'B', IP&TAFS Group 'A' and WPC Group 'A' of Department of Telecommunications, with preference will be given to officers of DoT working at Director / ADG / ADET / JTO level in the order of seniority. The total batch size comprising of officers of DoT shall be 20-25. In case a greater number of nominations are received, the selection criteria will broadly be based on in the order given below:

- Educational Qualifications
- Additional acquired knowledge needed to be the Domain Expert
- Demonstration of stand-apart knowhow in the domain
- Proven research and development track record in the domain
- Additional working experience in the domain
- ACR track of last 5 years mentioning special attributes and innovative technology solutions in the domain

The maximum nominations from IP&TAFS Group-A and WPC Group-A shall be 5 (IP&TAF Group 'A' – 3 nominations and WPC Group 'A' – 2 nominations). However, NCA-T reserves the right to increase or decrease the number of seats among ITS Group 'A'/ JTO Group 'B'/ IP&TAF Group 'A' and WPC Group 'A', in case lesser number of nominations are received from IP&TAFS Group 'A' and WPC Group 'A'.

The entire cost of the training for the DoT officers will be borne by NCA-T except for TA/DA. The participating officers will have to take care of their lodging and boarding as per their official entitlements, as per rules.

Further, keeping in view the relevance of capacity building in telecom security for DoT PSU's (BSNL / MTNL / TCIL / ITI) and C-DoT, maximum of 5 nominations are also invited from the officers of DoT PSU's (BSNL / MTNL- 2 Nominations; TCIL- 1 Nomination; ITI – 1 Nomination) and C-DoT – one nomination, **purely on a cost basis**, without any training fee waiver. However, NCA-T reserves the right to increase or decrease the number of seats among ITS Group 'A'/ JTO Group 'B'/PSU(s), in case lesser number of nominations are received from respective PSUs & CDoT.

The officers nominated for the CDP B-II shall be mandatorily required to undergo and complete all the three phases. In case, the participant opts to leave the course in between then NCA-T, Ghaziabad reserves the right to recover the cost of the training including any cost borne by the government/agency concerned on training.

The participating organizations/agencies will be providing computers/desktops during official training at their campus. However, officers will be advised to carry their own laptops with them for ease in learning and self-study.