NTIPRIT

National Telecommunications Institute For Policy Research, Innovation & Training

Handbook on Competency Development Program for Network & Mobile Security

NATIONAL TELECOMMUNCITIONS INSTITUTE FOR
POLICY RESEARCH, INNOVATION & TRAINING
Govt. of India Enclave, Admin Building,
ALTTC Campus, Rajnagar, Ghaziabad – 201002

TABLE OF CONTENTS

SECTION – 1

Competency Development Program Framework

01. INTRODUCTION

The telecommunications industry world-wide has experienced sweeping transformation since the advent of Mobile Technologies, especially in last two decades. In addition, emerging new areas like Fourth industrial revolution, Manet/Adhoc networks, 5G networks, IoT, M2M communication, big data analytics, artificial intelligence etc., need to be taken cognizance for improving the safety and security. The responsibility of DoT would be immense as it is uniquely positioned to handle the new emerging landscape effectively, both in terms of technological capabilities and capacities, apart from the works currently undertaken.

To meet the nation's communication needs, and to empower the country towards Digital India, various telecom policies have been adopted from time to time for the growth of telecommunications in India. Out of the three key vision areas – Digital Infrastructure as a utility to every citizen and Digital empowerment of citizens are the areas under which DoT has to work to achieve the desired goals. Towards this, DoT had come out with NDCP 2018, to re-orient itself at every level to cope up with the changing environment.

In past five years Government has been leveraging high on technology and has made sweeping change in way the technology is harnessed by individuals. The Digital India programme has made the technology available to masses. And at the core of this Digital Change Revolution are sitting the most disruptive technologies of today like Artificial Intelligence, Cloud Computing, Big Data Analytics, Blockchain, Secure Network and related technologies. All these new technologies adoption by the Government will call for new skills to be acquired by its officers, which will pave the way for the Government to better understand, manage and support the underlying eco-system. It becomes imperative to build capacities within the Government by involving cross-sectorial teams for improving expertise and promote a sustainable Digital Growth.

Department of Telecommunications (DoT) has largest number of highly qualified and experienced technocrats, than any other organised service cadre. Apart from the Telecom domain, the capable and techno-strategically placed workforce of DoT has unexplored potential to venture into all the aspects of Digital Initiatives of the Government both at Centre and State level. With "Data" being the sole mover & shaker for all the emerging technologies and almost vanishing line between Telecom and Information Technology, role of DoT and its officers is immensely of great importance to fulfil the technology driven vision of the Government.

In last two decades there is paradigm shift in DoT functioning from 'Service Provider' to 'Service Enabler' due to opening up of Telecom Sector for private participation. With corporatisation of service provisioning function of DoT into BSNL, the entire gamut of DoT's working underwent sea-change. Where Telecom officers once needed a solid background in

operations with an added dose of planning, in modern days telecom executives are required not only to keep them abreast of latest technological developments in Telecom but also have to equip themselves with strong technical knowledge of the advance ICT technologies to address the formidable challenges that lie ahead.

There is also a need for continuous in-house capacity building, with focussed and coordinated efforts in order to address the challenges of new technologies and services against regulatory and security concerns, along with driving the sector towards effective participation in the implementation of various Government schemes.

Due to above mentioned importance of competency enhancement this Competency Development program (CDP) concept is conceived. This is not merely pertaining to technical skill set, but about combining it with efficacy of strategic decision making for all round development in art of policy making. CDP is drafted to incorporate the necessary inputs to make DoT future ready.

02. OBJECTIVE

The Competency Development Program seeks to unlock the transformative power of young officers for leveraging digital communications technologies - to achieve the goals of NDCP; this program can also be perceived as a enabler which facilitates practical field exposure coupled with free flow of innovative ideas to bring out policy level/ prototype solutions by leveraging DCTs.

03. FRAMEWORK

3.1 CDP APPROACH

The CDP (Competency Development Program) is implemented through a modular approach with well identified Expert Domains in alignment to fulfilling Government's Digital Initiative. Each module shall be delivered through a containerised Domain Targeted Capacity Development Program. The identified Domains for developing expertise are:

- Network & Mobile Security
- 5G Networks and Use Cases
- Internet of Things
- Artificial Intelligence
- Spectrum Management
- Machine Learning
- Block Chain and Distributed Ledger Technology
- Data Science & Big Data Analytics
- Cloud & Edge Computing

- Quantum Computing

While there is a Broader Common Framework for CDP, each of the identified Expert Domains are guided by a unique Domain Targeted Capacity Development Program detailing the fine-prints of area of capacity building and identifying the available learning platforms and avenue.

3.2 PROGRAM LAYOUT

Under the CDP each target Domain training is envisaged to be imparted at three levels:

- Foundation Level (Maximum Two Weeks) – Phase I
- Intermediate Level (Maximum Four Weeks) – Phase II
- Advance Level (Maximum Six Months) – Phase III

These classroom / online courses are specially designed for the DOT officers with emphasis on hands on experiments / projects. Institutions identified for training may arrange a qualifying examination at the end of the course, to assess the learning and understanding of individual officers, undertaken the course. Depending upon the need felt, NTIPRIT may organise a preparatory training of one week duration for some of the domain.

3.3 SELECTION & IDENTIFICATION

The group of officers to be made Domain-Target Expert will be identified based on their quest to harness technology and showcase their already acquired domain knowledge by way of alternate learning behaviour and their ability to build innovative technical solutions in past based on that learning. While the emphasis will be to train limited, deserving and capable young officers, the selection criteria will broadly be based on:

- 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

For each of the above identified technology area, 2 to 4 SAG level officers, 6 to 8 JAG level officers and 10 STS & 10 JTS level officers will be selected. A batch of 30 officers will be trained in each Technology Domain.

Applications will be called for from the officers about their area of interest, expertise, educational qualification, experience and demonstrative capability in their domain. After preliminary screening of all applications at NTIPRIT, the final selection will be done by a Selection Committee.

3.4 DEPLOYMENT AND RETENTION

After successful completion of Domain Expert program, the specially trained officers will be equipped with in depth knowledge of their domain and will be able to contribute in all related spheres of government activity. For all future requirements related to the specific Technology area, the certified Expert officers will be referred for catering departmental needs as well as the requirements of other- departments/ ministries/ state governments/ PSUs. For next three years, these officers will be posted only on such posts which deal in their relevant Technology area.

Also after successful completion of Domain Expert program, such officers will be allowed to proceed on deputation in the Ministry/Organisation which can utilize their expert skills.

These officers will also be preferably utilized for nomination as members of different international organization and study groups (such as ITU, APTU, IEEE etc.). Their domain expertise will lead to the significant contribution from Indian side at different international platforms which will eventually strengthen the policy opinion of India at different International Forums.

To ensure availability of these expert officers, preferably those below the age of 52, at the time of call of applications, will be eligible for the training subject to fulfilling other eligibility criteria. The trained expert officers will also be required to sign a Security Bond to serve the department for at least three years or pay back equivalent of expenditure incurred on them in this program plus the salary given while on classroom environment training.

The requisite bond will be signed by the selected officer at the time of commencement of “Advance Level” phase.

3.5 EXPECTED OUTCOMES

The CDP (Competency Development Program) is envisaged to raise an army of highly qualified officers who are not only technologically at par with their private counterparts but also more competitive and learned to directly get involved in technology development & implementation as well as empowered to frame policy woven around these technologies.

These officers will serve as immediate experts to evolve innovative solutions to problems in proliferation of Digital India. Apart from Telecom domain, these specially trained officers will have the capability to shape the future course of policy & regulation both at Centre and State level, across all Digital Communication technology areas.

The CDP (Competency Development Program) is envisaged keeping the NDCP strategies and goals in sync with CDP objectives:

A. Propel India Strategies:
    a) Ensuring a holistic and harmonised approach for harnessing Emerging Technologies.
    b) Leveraging AI, Big Data in a synchronized and effective manner to enhance the overall quality of service, spectrum management, network security and reliability.
B. Accelerating Industry 4.0:
    a) Create roadmap for transition to Industry 4.0 by 2020, by closely working with sector specific industry councils.
C. Secure India Strategies:
    a) Develop and deploy robust digital communication network security frameworks.
    b) Developing a comprehensive plan for network preparedness, disaster response relief restoration and reconstruction.

SECTION – 2

Domain Expert Area

Network & Mobile Security

(under CDP Framework)

04. ABOUT THE DOMAIN EXPERT AREA

It has been universally observed that there is large number of recent threats and incidents reported to CERT therefore security in networks and distributed systems has gradually become a global challenge. To deal with such debilitating issue, it is critical to design and develop security solutions from different viewpoints including that of end-to-end. Other than these threats, the growing need of wireless, ad-hoc and sensor networks also create hazards of a new dimension. Another significant technical feature that create risk is the communication speed in networks versus complex and time consuming cryptography/security mechanisms and protocols.

Various communication networks are the mainstay of much of the critical infrastructure in many sectors today such as civil aviation, shipping, railways, power, nuclear, oil and gas, finance, banking, IT, law enforcement, intelligence agencies, space, defence, and government networks. In the Communication Networks, there may be serious security attacks such as data theft, fraud, and denial of service attacks, hacking, and cyber warfare, terrorist and antinational activities.

A cyber-attack which can control the infrastructure may harm the system and disrupt the communication network. The attacks can be through viruses, malware, Trojans, hacking, network scanning, probing, and phishing. Furthermore, the Social network attacks can be one of the major sources of attacks in future because it is used by huge number of users and they post their personal information on sites through these networks.

Developing proper telecom security structures that will ensure Cyber Safety, Security & Assurance at network level is the need of the hour. Also, the networks of the service providers have to be routinely security audited and certified. As per the license agreement, TSPs and ISPs are bound to secure and safeguard communication networks from attacks and are required to have their networks audited every year.

To cater to the need, officers of the department should be equipped with the expertise in

- Secure Configurations for Hardware and Software
- Continuous Vulnerability Assessment
- Monitoring, and Analysis of Network Audit Logs
- All types of Malware Detection & Mitigation
- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Network & Boundary Defence
- Data Protection
- Incident Response and Management

- Penetration Tests and Red Team Exercises

Under the master framework of Competency Development Program, the Domain Expert area of Network & Mobile Security is formulated. This program derives the implementation skeleton from CDP framework and is planned for delivery in three levels or phases of Foundation, Intermediate and Advanced.

Applicant officers must have appetite to learn and perform in highly technological environment involving high-end computing and programing. Each phase of training program is followed by intensive evaluation schedule which the candidate has to pass through for becoming eligible for next phase of training.

05. PROGRM LAYOUT

5.1 PREPARATORY

To acquaint the selected officers about the preliminary concepts about the domain expert area the program will start with a one week Preparatory Program delivered at NTIPRIT in classroom training.

PREPARATORY ***Preparatory at NTIPRIT***

Delivery :

a) At NTIPRIT, from in-house faculty and guest speakers. ***Duration : One week***
b) Focus on theoretical foundation

5.2 PHASE – I, FOUNDATION

The officers will be trained in fundamental 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 is aimed to give the officers an overview of Network Security Space and related terminologies.

Indian Institute of Technology, Kanpur, has been selected on nomination basis for delivery of this phase. This is an online delivery module for one week.

PHASE – I ***Foundation***

Delivery:

a) Online with IIT Kanpur. ***Duration : One week***
b) Focus on theoretical foundation

5.3 PHASE – II, INTERMEDIATE

The officers will be introduced to more practical learning environment which can be put in practice in real communication environment. Learning will be weaved around Communication Network Architecture with detailed protocol level knowledge, Network Foot-printing and Reconnaissance, Scanning Networks, Vulnerability Analysis, Ethical System Hacking Techniques and Ethic Code of Conduct in various network security domains, Malware Detection & Analysis, Social Engineering Techniques, Distributed Attack Scenario, IDS/IPS and Firewalls, Mobile Security, IoT Security Audit & Incident Reporting.

C-DAC Pune has been selected on nomination basis as partner institute for delivery on this phase. This will be fully classroom and hands-on practical training of four weeks duration.

PHASE – II ***Intermediate***

Delivery:

a) Residential program at C-DAC Pune. ***Duration : Four weeks***
b) Significant component of Hands-on mode

5.4 PHASE – III, ADVANCED

In this program the officers will be made domain expert on Network Security getting professional level expert training from premier domestic or international institution. While the course of learning will be same as of associate level but it will be advance in terms of employability and applicability in communication domain. The officers will be exposed to more technological advanced techniques of Network Threat Identification, Auditing and Mitigation procedures with exposure to international best practices. The ultimate aim shall be to produce highly qualified experts in Network Security with cutting edge technical tools and know-how. After the completion of this phase, the officers will also have to undergo at least one internationally acclaimed certification in the area of Cyber & Network Security, like CISSP, CISA, CEH Masters etc. One attempt for such certification will be on offer as part of Phase-III program.

PHASE – III ***Advanced***

Delivery:

a) Residential cum Online program at selected institute. ***Duration : Six Months***
b) Major component in hands-on mode

Note: As of now, NTIPRIT is having approvals for conduction of training upto Phase-II. As per approvals granted for CDP framework and Domain Expert program of Network & Mobile Security, the Phase-III part of the composite program shall be arrived at after evaluating the outcome till Phase-II.