MINISTRY OF
ELECTRONICS &
INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA

Digital India
Power To Empower

NeGD
National e-Governance Division

asci
Leadership through Learning

Cybersecurity and Privacy for Government Personnel

A Capacity Building Programme under Digital India

Batch 1: 02-04 APR, 2025

Batch 2 : 11-13 JUN, 2025

Programme Objectives

The objectives outlined below have been carefully chosen to establish a holistic framework around which officers may be trained towards becoming more aware of cybersecurity risks within their organizations:

Understanding Cyber Security and Privacy: This goal seeks to equip trainees with updated awareness about cyber vulnerabilities plus the necessary skills required for implementing robust control measures.

Risk Management: It aims at imparting knowledge on evaluating threats from potential attackers and then responding accordingly based on real-life incidents or events simulated during training.

Promoting Secure Private Digital Environments: Cultivating attitudes among staffers that foster consciousness regarding securing personal information stored electronically within agency boundaries therefore heightening overall compliance levels vis-à-vis regulations designed to safeguard such data.

Strategic Crisis Management: Equipping managers with strategic decision-making abilities needed during times when IT infrastructure suffers breaches due to either external or internal factors leading to quick efficient actions minimizing further damage caused by delays.

Adoption of Emerging Technologies: Instilling culture exploration adoption latest protective mechanisms against unauthorized access ownership alteration dissemination through either digital or physical means.

Building Resilient Organizations: Ensuring continuity of business operations protection against losses arising out of interruption of normal activities occasioned by occurrences related to failure to protect against loss unauthorized disclosure alteration destruction records.

Promoting Enhanced Staff Awareness on Cyber Security Issues: Creating an environment where staff must always keep watch for any emerging trends relating threats faced daily basis while ensuring adherence good practices pertaining the use of information systems.

These objectives are designed to create a focused and impactful training programme that addresses key aspects of cybersecurity and privacy preparedness among the government officials, leveraging the unique environment of Cyber Theme Park (CTmP).

CYBER THEME PARK (CTmP)

Cyber Theme Park is an innovative, first-of-its-kind experience centre developed at ASCI that transforms theoretical knowledge into practical wisdom. It is a dynamic environment where individuals come together to engage in meaningful interactions, exchange ideas, and challenge their existing perspectives. We believe that true learning occurs when theoretical knowledge is applied and tested in real-life scenarios & situations. It aims to bridge the gap between theory and practice by creating an immersive experience with 4 distinct mindsets - Attacker, Protector, Defender, and Overseer that transforms abstract concepts into tangible outcomes. The programme seamlessly blends theory with practical, immersing the participants in the world of attacker and defender techniques. CTmP will be an integral part of the programme.

MINISTRY OF
ELECTRONICS &
INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA

Digital India
Power To Empower

NeGD
National e-Governance Division

asci
Leadership through Learning

Programme Coverage & Structure

Day 01

Time	Topic	Details of Subtopics	Lab/CTmP
9:00 AM - 10:30 AM	Opening Ceremony and Cybersecurity Fundamentals	Cyber Threat Landscape: Understanding key cybersecurity concepts, common cyber threats like malware and phishing, and their impact on privacy.	
11:00 AM - 12:30 PM	Information Security Policies & Governance, Risk, and Compliance	• Importance of Security Policies for organizational security • Key types of policies (Access Control, Incident Response, Data Protection) • Overview of Governance, Risk Management, and Compliance (GRC) frameworks (e.g., NIST, ISO 27001) • Role of auditing and compliance in ensuring security	
2:00 PM - 3:30 PM	Security Architecture, Network Security & Mobile/ Endpoint Security	• Basics of security architecture, secure network design, and the use of firewalls and VPNs. • Key threats to mobile devices, Mobile Device Management (MDM), and securing mobile access • Best practices for securing endpoints, including antivirus, EDR, DLP, and patch management	• Defensive tool Demo • End point Security Solutions Demo
4:00 PM - 5:30 PM	Identity and Access Management (IAM) & Encryption Practices	Principles of IAM, role-based access control, and management of digital identities to protect data.	• Creating and Managing Users and Groups • Assigning Permissions Using Roles and Policies • Implementing Least Privilege Access • Temporary access management • Data encryption techniques

Day 02

Time	Topic	Description	Lab/CTmP
9:00 AM - 10:30 AM	Threat Intelligence and Monitoring	Utilizing threat intelligence, security monitoring systems, and proactive threat mitigation strategies.	• Security Monitoring with SIEM & EDR • Investigating Suspicious Domains with Threat Intelligence
11:00 AM - 12:30 PM	Fundamentals of Privacy	Definitions and importance of privacy, types of personal and sensitive information, and privacy as a human right.	• Secure Data Storage & Encryption • Phishing & Social Engineering Awareness
2:00 PM - 3:30 PM	Data Protection Laws and Regulations	Overview of major privacy laws like GDPR, CCPA, HIPAA, and penalties for non-compliance.	
4:00 PM - 5:30 PM	Principles of Data Protection	Discussing principles like lawfulness, fairness, transparency, and data minimization among others.	

Day 03

Time	Topic	Description	Lab/CTmP
9:00 AM - 10:30 AM	Roles and Responsibilities in Data Protection & Privacy by Design	• Understanding key roles: Data Controller, Data Processor, Data Protection Officer (DPO), and Data Subject. • Legal obligations of each role under regulations like GDPR. • Organizational accountability for data protection, including managing risks and ensuring compliance.	
11:00 AM - 12:30PM	Data Subject Rights & Incident Response	• Overview of the core rights under GDPR and other regulations: Access, Rectification, Erasure (Right to be Forgotten), Portability, and Restriction of Processing.	• Ransomware Attack Response & Recovery • Insider Threat Investigation Using UEBA (User Behavior Analytics)
2:00 PM - 3:30 PM	Third-Party Data Sharing, Privacy Impact Assessments (PIA), and Emerging Technology Risks	• Risks and compliance requirements when sharing personal data with third parties. • Examining privacy and security challenges in technologies.	• Analyzing API Data Sharing Between Applications • Deepfake & Synthetic Media Detection
4:00 PM - 5:30 PM	Group Discussion and Closing Ceremony	• The culmination of the week's events and discussions, providing a platform for participants to reflect on their learnings and share insights imparted throughout the Cyber Security & Privacy program followed by closing ceremony that acknowledges the contributions of speakers and participants, and sets the stage for ongoing collaboration and community building within the field of cybersecurity.	

MINISTRY OF
ELECTRONICS &
INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA

Digital India
Power To Empower

National e-Governance Division

asci
Leadership through Learning

The accommodation & programme details

- There are two Batches for the programme as per the details below.
- Single occupancy AC accommodation will be provided either at the Executive Hostel of ASCI's Bella Vista campus in Hyderabad or at a Hotel nearer to the campus.

Programme Details

BATCH 1: 02-04 April, 2025		BATCH 2: 11-13 June, 2025	
Check-in	01 April, 2025 – afternoon	Check-in	10 June, 2025 – afternoon
Check-out	05 April, 2025 – morning	Check-out	14 June, 2025 – morning
Location	Administrative Staff College of India (ASCI), Bella Vista, Raj Bhavan Road, Hyderabad – 500 082.		

Andragogy

This on-campus programme will be conducted at our state-of-the-art campus in Bella Vista Campus, Hyderabad. Strong emphasis will be given to interactive and participative learning. The programme will comprise of lecture sessions, experiential Cyber Theme Park (CTmP) sessions, group discussions and experience-sharing sessions.

All relevant study materials including PPTs, details of various Acts and Guidelines etc. will be shared with the participants.

The programme will be conducted by experienced faculty, practicing professionals and industry veterans with a unique blend of expertise from industry, government, and regulatory bodies. The programme is expected to go beyond theory and impart real-life and practical skills to equip the participants to handle all possible scenarios and provide good leadership. The programme straddles the frontiers of governance and technology, and takes the participants on a transformative journey, led by seasoned professionals who have shaped the cybersecurity and privacy landscape of governance.

MINISTRY OF
ELECTRONICS &
INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA

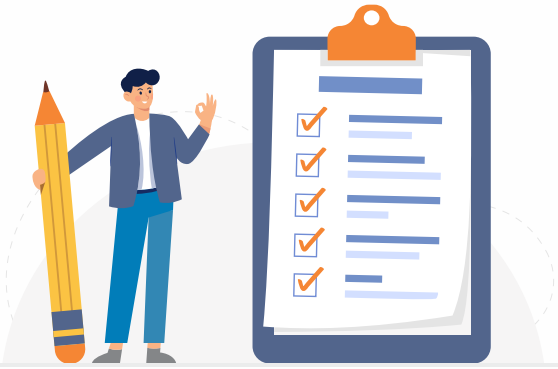
Digital India
Power To Empower

NeGD
National e-Governance Division

asci
Leadership through Learning

Eligibility for the participation

This course is specially designed to create a unique and immersive learning experience for the senior professionals of Ministries and departments of Government of India, State Governments and Other autonomous bodies.



- Policy level: who are responsible to conceptualise a project and take critical decision making in a project.
- Program management level/Mid-level: who are responsible to design, implement & monitor projects.

Nomination Process

- Interested candidates may apply online by visiting https://tmis2.negd.in/
- Only online registration along with nomination letter from competent authority will be accepted
- Nominations will be finalized on eligibility and suitability of candidates.

The confirmation of participation and details of venue/change in date, if any, will only be communicated to the registered email ID and contact number. Please ensure to use your official and active email ID and contact number while registering online.

Last date for submission of nominations-

Batch 1 - 21st Feb, 2025
Batch 2 - 01st May, 2025

For further details on programme, please contact:

E-mail: negdcb@digitalindia.gov.in | Call: 011-24303742

MINISTRY OF
ELECTRONICS &
INFORMATION TECHNOLOGY
GOVERNMENT OF INDIA

Digital India
Power To Empower

National e-Governance Division

asci
Leadership through Learning

CONTACT US

Administrative Staff College of India
BellaVista, Raj Bhavan Road, Khairatabad,
Hyderabad, India – 500082.

E-Mail: poffice@asci.org.in or mpr@asci.org.in

asci
Leadership through Learning

Follow us on:

- https://www.facebook.com/ascihyd
- https://www.linkedin.com/company/administrative-staff-college-of-india-asci/
- https://x.com/ASCIMEDIA?t=waAofpmODEIg1Rr8XevW_Q&s=08
- https://www.instagram.com/ascibv/?igsh=NWg2OGIydWIxcWNi#

National e-Governance Division

Follow us on:

- https://www.facebook.com/NeGDofficial
- https://www.youtube.com/user/MyNeGP/playlists
- https://in.linkedin.com/company/digital-india
- https://twitter.com/NeGD_GoI
- https://www.instagram.com/officialdigitalindia/

National e-Governance Division
4th Floor, Electronics Niketan, Ministry of Electronics & IT,
6, CGO Complex, Lodhi Road, New Delhi: 110003
Phone No. : 011-24301943, 24303764

E-Mail: negdcb@digitalindia.gov.in