QUALIFICATION FILE – CONTACT DETAILS OF SUBMITTING BODY

Name and address of submitting body:

- NIELIT Gorakhpur,
  M.M.M.U.T. Campus, Deoria Road Gorakhpur – 273010 (UP)
  Phone No.: 0551-2273371
  Branch Office
- NIELIT Lucknow
  A-1/9, Sumit Complex, Vibhuti Khand, Gomti Nagar, Lucknow- 226010(UP)
  Phone No.: 0522 272 0590

Name and contact details of individual dealing with the submission

Name:	**Pawan Verma**
Position in the organisation	**Technical Officer**
Address if different from above	**NA**
Tel number(s)	**0522 2720590**
E-mail address	**pawanverma@nielit.gov.in**

List of documents submitted in support of the Qualifications File

1. **Detailed Curriculum**
2. **Industry Validation (Attached at Annexure I)**

Since the proposed jobrole has not been identified by SSC, the industry mapping will be as per progression pathways indicated in the QF

QUALIFICATION FILE SUMMARY

Qualification Title	Certificate Course in Cyber Forensic
Qualification Code	
Body/bodies which will assess candidates	**Examination Cell,** National Institute of Electronics and Information Technology, 6-CGO Complex, Electronics Niketan, Lodhi Road, New Delhi. 110003.
Body/bodies, which will award the certificate for the qualification.	**Certification Division,** National Institute of Electronics and Information Technology, 6-CGO Complex, Electronics Niketan, Lodhi Road, New Delhi. 110003.
Body, which will accredit providers to offer the qualification.	**Accreditation Division,** National Institute of Electronics and Information Technology, 6-CGO Complex, Electronics Niketan, Lodhi Road, New Delhi. 110003.
Occupation(s) to which the qualification gives access	• Computer Forensics Technician • Junior Forensics Analyst • Senior Forensics Analyst • Senior Forensics Manager • Computer Forensics Engineer • Computer Forensics Investigator • Computer Forensics Specialist • Computer Forensics Analyst • Computer Forensics Examiner
Proposed level of the qualification in the NSQF.	6
Notional Learning Hours	500 hours.
Entry requirements / recommendations.	Graduate in Science/Engineering Stream pursuing
Progression from the qualification.	**Computer Forensics Technician -Junior Forensics Analyst-Senior Forensics Analyst** Initially, candidate can work as Junior Forensics Analyst who would be capable of recovering information from computers and storage devices. The trained candidate may assist to law enforcement officers with cyber crimes and to retrieve evidence. Computer forensics analysts uncover digital data (such as e-mail correspondence or erased files), preserve it for later use as evidence, and analyze the data in light of the crime in question. For example, they may have to determine how hackers or

	unauthorized personnel gained access to information or computer systems as well as where and how they navigated within the system.
Planned arrangements for RPL.	• Presently only candidates who undergo training shall be assessed. • It will be incorporated once RPL strategy is finalized

Formal structure of the qualification

	Title of unit or other component (include any identification code used)	**Mandatory / Optional**	**Estimated size (learning hours)**	**Level**
CCCFI	CYBER CRIME, INDIAN IT (A) Act 2008 AND COMPUTER FORENSICS	Mandatory	120	6
CCCFII	SEIZURE & IMAGING OF DIGITAL EVIDENCE	Mandatory	120	
CCCFIII	ANALYSIS OF DIGITAL EVIDENCE	Mandatory	120	
CCCFIV	COMPUTER FORENSICS FOR WINDOWS & LINUX SYSTEMS AND ANTI-FORENSICS	Mandatory	120	
CCCFV	ENHANCING COMMUNICATION & SOFT SKILL	Mandatory	20	

Please attach any document giving further detail about the structure of the qualification – e.g. a Curriculum or Qualification Pack.Detailed Curriculum attached at Annexure III.

SECTION 1
ASSESSMENT

Name of assessment body:
Examination Cell
National Institute of Electronics and Information Technology
6-CGO Complex, Electronics Niketan,
Lodhi Road, New Delhi. 110003.

Will the assessment body be responsible for RPL assessment?

Give details of how RPL assessment for the qualification will be carried out and quality assured.

Presently, only candidates undergoing training shall be assessed. Later on, candidates having experience and knowledge shall be assessed. The information will be provided on finalization of such procedure.

Describe the overall assessment strategy and specific arrangements which have been put in place to ensure that assessment is always valid, consistent and fair and show that these are in line with the requirements of the NSQF:

The emphasis is on practical demonstration of skills & knowledge based on the performance criteria. Each OUTCOME is assessed & marked separately. Student is required to pass in all OUTCOMEs individually and marks are allotted. Following assessment methodologies are

used.

A. Written Assessment (Multiple Choice Questions)
B. Practical Assessment
C. Viva Voce Assessment

Supporting evidences for Assessment

The assessment results are backed by following evidences.

1 The assessor collects a copy of the attendance for the training done under the scheme. The attendance sheets are signed and stamped by the In charge / Head of the Training Centre.
2 The assessor verifies the authenticity of the candidate by checking the photo ID card issued by the institute as well as any one Photo ID card issued by the Central/Government. The same is mentioned in the attendance sheet.
3 The assessor assigns roll number.
4 The assessor takes photograph of all the students along with the assessor standing in the middle and with the centre name/banner at the back as evidence.

Please attach any documents giving further information about assessment and/or RPL.

ASSESSMENT EVIDENCE

Complete the following grid for each grouping of NOS, assessment unit or other component as listed in the entry on the structure of the qualification on page 1.

Job Role

- Computer Forensics Technician
- Junior Forensics Analyst
- Senior Forensics Analyst
- Senior Forensics Manager
- Computer Forensics Engineer
- Computer Forensics Investigator
- Computer Forensics Specialist
- Computer Forensics Analyst
- Computer Forensics Examiner

Title of Unit/Component:

(Detailed Curriculum attached)

Assessable Outcomes	Assessment criteria for the outcome	Total Mark	Written	Practical	Vivo-voce
1. **WILL LEARN CYBER CRIME, INDIAN IT (A) ACT 2008 AND COMPUTER FORENSICS**	Categorization of Cyber Crimes, security policy violations, online financial frauds, elaboration of cybercrimes.	200	15	5	4
	Explain Indian IT (Amendment) Act 2008, Objective, Applicability, and Jurisdiction;		15	10	5
	Explain basics of Architecture. Importance of File systems		15	10	4

	Windows file structure				
	Can perform Data Hiding Techniques, Swap Files, Slack space, Unallocated and Allocated space, ADS		15	10	4
	Use and working with optical, magnetic, semiconductor, etc. and their interfaces with a computer system, Hard Disks-IDE, SATA, SCSI; CD/DVD		15	15	4
	Perform Swap Files, Slack space, Unallocated and allocated space, alternative data streams (ADS)		10	10	4
	Need of computer forensic investigation of the cyber crimes, forensic investigation process, identification, seizing, imaging and analysis of digital evidence, report preparation		15	15	4
	Role of a First Responder, First Responder's Toolkit.				
		Total	**100**	**75**	**25**
2. **WILL ACQUIRE KNOWLEDGE AND SKILLS ON SEIZURE & IMAGING DIGITAL EVIDENCE**	Handling of digital evidence at the site of the crime and basic rules of digital evidence; safe & secure packing and transportation of digital evidence	200	25	20	5
	EXplain Volatile data, order of volatility, importance of volatile data etc. Collecting Volatile Data, acquisition of RAM data. Use of tools to capture, steps to image the volatile data (RAM) and other volatile data from a live system		30	35	7
	Use of Disk imaging software tools & hardware equipment, Dead & Live Acquisition of digital evidence, imaging of virtual systems		20	20	7
	Execute wiping of data, integrity verification of digital evidence		25	15	6
		Total	**100**	**75**	**25**
3. **ANALYSIS OF DIGITAL EVIDENCE**	Recovery of Deleted files, recovery of data from the hard disk, damaged FAT, using of file carving tools	200	15	10	4

	Explain Methodology of analysis, preparation & updation of the list of relevant keywords, their search		15	10	3
	Analysis of media files headers, manual of graphics, audio, video files; Steganography in media files, process of hiding of data / data files in media files		15	10	4
	Role of logs in forensic analysis, access logs from various sources, log analysis tools, analysis of logs using log analysis tools and manually.		15	10	3
	Use of Tools for finding/ cracking/ bypassing of passwords, encryption keys for recovery of data from the password protected / encrypted documents		15	10	4
	Use of well-known commercial and freeware toolkits, their features, advantages over other CLI/GUI tools		10	10	3
	Preparation of Computer Forensic Analysis Reports, Executive Summary, Goals/Objective of the Analysis, case questionnaires with relevant findings, referring to annexing of supporting documents, screenshots, photographs; tools used, forensic analysts involved, Report writing Guidelines, organizing the Reports, Documenting Investigative Steps with sections & subsections, Conclusion, Expert witness, testimony by a forensic analyst and role of an expert witness in judicial courts		15	15	4
		Total	**100**	**75**	**25**
4.**TO FAMILARIZED WITH COMPUTER FORENSICS FOR WINDOWS & LINUX SYSTEMS AND ANTI - FORENSICS**	Examination of recycle bin windows shortcut files, swap file pagefile.sys, hibernation file, print spool files, windows registry analysis, registry analysis tools, registry hives, knowing about USB devices used,	200	20	15	5
	Use of built-in command line tools for computer forensic investigation , data recovery tools		20	15	5

	Analysis of websites in favorites, history, cookies, temporary internet files, data in cache, saved passwords, auto-complete feature, internet usage analysis tools		20	15	5
	Can perform following tasks: recovery of deleted e-mails, e-mail headers, viewing & analysing the e-mail headers in popular e-mail software applications, and forensic toolkits in tracing e-mails		**20**	15	**5**
	Handling challenges or bottlenecks in computer forensic investigation for a computer forensic analyst; encrypted, compressed, password protected documents		**20**	15	**5**
		Total	**100**	**75**	**25**
5.ENHANCING COMMUNICATION & SOFT SKILL	Communication with colleagues, Clients, superiors.	**50**	10	N/A	N/A
	Managing career, staff and professional relationships		20	N/A	N/A
	Ready for interview		20	N/A	N/A
		Total	**50**	N/A	N/A
	Grand Total	**850**	**450**	300	100

Means of assessment 1 Proctored online assessments (LAN and Web based), carried out using a variety of question formats applicable for linear / adaptive methodologies; performance criteria being assessed via situation judgement tests, simulations, code writing, psychometrics and multiple choice questions etc.

SECTION 2

What evidence is there that the qualification is needed?

EVIDENCE OF NEED

Information Technology Act, 2000 (IT Act 2000) was a landmark piece of legislation for India as it provided the base for Indian cyber law and matters related to the same. With gradual developments and amendments, issues pertaining to cyber crimes, cyber forensics, electronic evidences, cyber security, etc were also incorporated into the IT Act 2000.
Although the need for a comprehensive and holistic techno legal framework is still haunting Indian government yet there is no escape from the conclusion that Indian cyber law must also be repealed and replaced by a better piece of legislation. At the same time Indian law enforcement agencies must be suitably trained in the matters of cyber law, cyber crimes investigation, cyber forensics, etc.
This career will grow at a rate of at least 22 percent (the projected rate of growth for private investigator jobs) and probably higher than 27 percent (the projected rate of growth of computer-support-related jobs) through 2018.

The proliferation of criminal activity on the Internet, such as identity theft, spamming, e-mail harassment and illegal downloading of copyrighted materials, will increase the demand for private investigators. Opportunities are expected to be excellent for computer forensic investigators.
On the other hand, cyber crimes have significantly increased in India. The trends in this regard are not very promising. For instance, the cyber law (PDF), cyber security (PDF) and cyber forensics (PDF) trends in the year 2013 have showed poor performance of Indian government in these fields. This position has not changed in 2014 as well. For instance, the cyber forensics trends of India 2014 still show inability of India to deal with cyber forensics related issues.
Perry4Law Organisation and Perry4Law's Techno Legal Base (PTLB) believe that cyber crimes investigation requires sound techno legal expertise. Skills development through online training and skills development courses in urgently required for Indian law enforcement agencies. Cyber crimes investigation training in India is one such skills development activity that must be imparted to make law enforcement agencies of India modern and upto date. Other stakeholders must also have basic level cyber law and cyber security awareness so that cyber crimes can be minimised in India.

(Source :Cyber Forensics Research Centre Of India (CFRCI) By PTLB)
URL: http://ptlb.in/cfrci/

NASSCOM SETS-UP CYBER SECURITY TASK FORCE TO BUILD INDIA AS THE CYBER SECURITY HUB

Task force in accordance with the Prime Minister's vision for India to take leadership in this critical and emerging space
Focus on building key recommendations on the four pillars of Industry + Policy + Technology + Skills

National Association of Software and Services Companies (NASSCOM) and Data Security Council of India today announced the launch of the NASSCOM Cyber Security Task Force that aims to build India as a global hub for providing cyber security solutions, developing cyber security R&D plan and develop a skilled workforce of cyber security experts.

The taskforce members include industry leaders across IT, BPM and Internet, leaders from user organizations like banks and telcos as well as representatives from the government and academia. Mr Rajendra Pawar, Chairman, NIIT was requested to chair this taskforce. The taskforce over a 12 week period will identify the key priorities and build the detailed action plan for the sector.

Key Statistics

- IT Security market estimated at USD77 billion in 2015 and growing at over 8 percent

annually

- Demand for security workforce to rise globally to 6 million by 2019, up from 4 million currently, with projected shortfall of 1.5 million.
- Security market in India estimated to be 1% of the overall IT-BPM industry.
- Rapid growth in security software product segment – USD 250 million revenues in FY 2015

Mr. Rajendra Pawar, Chair, NASSCOM Cyber Security Task Force and Chairman, NIIT, said, "Securing the cyberspace has become an important priority for governments, businesses and citizens across the world. In line with the Prime Minister's vision of making India a cyber-security expert nation and his recent exhortation to the industry, we have created the cyber security task force. This taskforce aims to make India a global hub for providing cyber security solutions including cyber security products and services. The taskforce will focus on the four key pillars of Industry development, Policy enablement, Technology development and Skill development."

Mr Mohan Reddy, Chairman, NASSCOM said "Cyber Security is an important priority for NASSCOM."

This Task Force will study the Indian cyber security ecosystem to identify issues and challenges and develop an action plan to address the priority issues. It will also identify possible intervention opportunities for the Indian IT industry in global cyber security space and bring together stakeholders from across the board to develop cutting-edge technologies and address the global market requirements. Learnings from global countries will be undertaken to understand how to catalyse the security product ecosystem in India.

Mr. R. Chandrashekhar, President, NASSCOM, said, "Cybersecurity is a multi-dimensional concept which includes many disciplines and fields. Nations have to take appropriate steps in their respective jurisdictions to create necessary laws, promote the implementation of requisite security practices, incident management, and information sharing mechanisms, and continuously educate both corporate and home users about cybersecurity. It is a global problem that has to be addressed by all stakeholders jointly. This Task Force will work towards enhancing cyber security and enabling India to emerge as a leader in this space."

Mr Gopal Pillai, former Home Secretary and Chairman, DSCI said "Cyber Security has emerged as a key facet of national security. This initiative by NASSCOM and DSCI is an important effort aimed at optimizing the role of industry in this space, both at the national and international levels."

The vision of the Taskforce aims to build the cyber security industry in India from the 1 percent market share to 10 percent by 2025; a trained base of 1 million certified and skilled cyber security professionals and build 100+ successful security product companies from India.

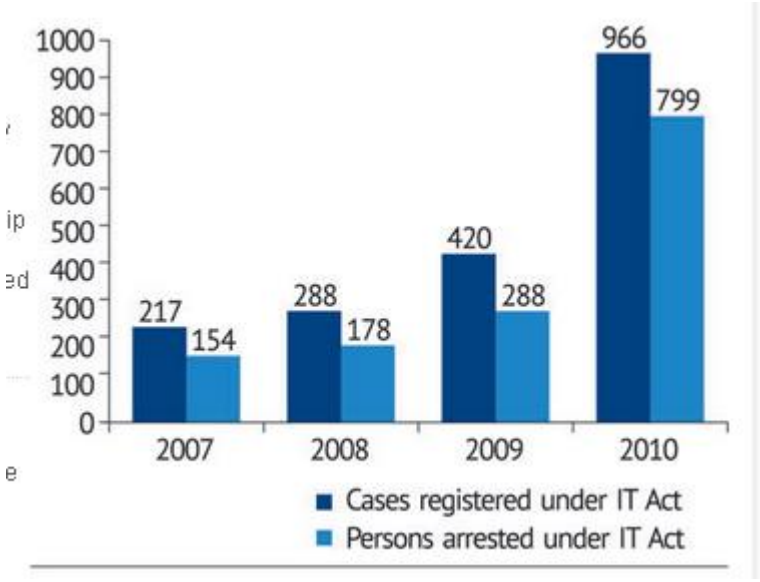
(Source: http://www.nasscom.in/nasscom-setsup-cyber-security-task-force-build-india-cyber-security-hub)

Securing India's Cyber Frontiers

Cyber security continues to be a core area of focus for NASSCOM-DSCI and the IT-BPO industry, and several initiatives have been rolled out to keep India free from cybercrime.

This is also the reason why the issue of cyber security is appearing on the agenda of Indian CEOs and becoming important for national security. Recognising the fact that more and more critical infrastructure is being owned and operated by the private enterprises, the Data Security Council of India (DSCI), an independent organisation set up by NASSCOM constituted the DSCI Cyber Security Policy Forum (CSPF).

Headed by Rajendra Pawar, past Chairman, NASSCOM, it included DSCI as Member Secretary and experts from the public and private sector and law enforcement. The group was entrusted with the task of making recommendations to the government on cyber security. DSCI consolidated the preliminary recommendations provided by the Cyber Security Advisory Group (CSAG) members in a report titled 'Securing Our Cyber Frontiers'. Released by P Chidambaram, the Union Home Minister, in April 2012, the report makes 10 key recommendations outlining the roles of the government and the industry.



According to the recommendations, India should:

- Create a National Structure for Cyber Security, which clearly defines roles and responsibilities for every stakeholder, establishes coordination and information sharing mechanisms, focuses on building public-private partnership models and creates an environment for enhancing trust between the industry and the government. A fully empowered head for Cyber Security should be appointed, positioned at the highest level within the government
- Design and implement a Competency Framework for building a competent and adequate Cyber Security Workforce. The Competency Framework should assess the security skills requirements, identify existing gaps and challenges, define competency areas across different security roles and devise strategies and programmes for building the required

capacity

- Create and maintain an Inventory of Critical Information Infrastructure in the country to provide the required visibility over the critical information infrastructure and help priorities deployment and monitoring of the protection measures
- Establish a Centre of Excellence for Best Practices in Cyber Security to institutionalize the development, sharing, collation, distribution and implementation of best practices in the country
- Establish a National Threat Intelligence Centre, which should integrate all the existing information sources such as sectorial CERTs, intelligence bodies, security alerts issued by security vendors, threats seen by critical sectors and industry to enable cross-domain awareness and a comprehensive view of cyber threats at the national level
- Build Capacity of the Law Enforcement Agencies (LEAs) in Cyber Crime Investigations and Cyber Forensics by establishing training facilities in every state and union territory
- Build Lawful Interception Capabilities for balancing national security and economic growth by establishing a national centre for performing research in encryption and cryptanalysis
- Establish a Centre of Excellence for Cyber Security Research to develop solutions that will protect the country's information infrastructure in the future by defining and executing a research roadmap developed on the country's research needs
- Set up Testing Labs for accreditation of ICT products to mitigate security risks arising from procurement of ICT products especially from foreign vendors and yet take full benefits from the global supply chain that includes access to world-class products, services and expertise at competitive prices
- Establish a Cyber Command within the defense forces to defend the Indian Cyberspace. The Cyber Command should be equipped with defensive and offensive cyber weapons, and manpower trained in cyber warfare

(Source: Reports on Securing India's Cyber Frontiers **http://www.nasscom.in/securing-india%E2%80%99s-cyber-frontiers?fg=143159)**

Please attach any documents giving further information about any of the topics above.
NIL

SECTION 3
SUMMARY EVIDENCE OF LEVEL

Level of qualification:6

Summary of Direct Evidence:
Justify the NSQF level allocated to the QP by building upon the five descriptors of NSQF. Explain the reasons for allocating the level to the QP. Generic NOS is/are linked to the overall authority attached to the job role.

Computer Forensics Analyst/Forensic Expert/Computer Forensics Investigator					
Process required	**Professional knowledge**	**Professional skill**	**Core skill**	**Responsibility**	**Level**
The job roles demands a widerange of specialisedtechnical skill, clarityof knowledge andpractice in broadrange of activityinvolving standard and non-standardpractices Computer forensic analysts use forensic tools and investigative methods to find specific electronic data, including Internet use history, word processing documents, images and other files.. • Candidates must be	The trained candidates would have factual and theoretical knowledge in broad contexts The trained candidate would be able to provide Conduct data breach and security incident investigations, Recover and examine data from computers and electronic storage devices by utilising knowledge gained during the training i.e. • Windows Forensics • Linux Forensic • Anti-Computer Forensics • Recovery of Data • Digital Evidence • Seizing & Imaging of non volatile data	The trained candidates would have a range of cognitive and practical skills required to generate solutions to specific problems in a field of work or study After acquiring professional knowledge on cyber Forensics,tools and Techniques, the candidates will be expertise in hacking and intrusion techniques and prior experience with security testing and computer system diagnostics. • The role of the analyst is to Recover data like documents, photos and e-mails from computer hard drives and other	Reasonable good in mathematical calculation,understanding of social,political and reasonably good in data collecting organising information, and logicalcommunication They are able to make independent decision involved in providing solution. The core skill acquainted by trained candidates are • Technical Audit of Server • Identify additional systems/networks compromised by cyber attacks	Responsibility for own work and learning and full responsibility for other's works and learning They are able to lead team as well as work in team.They will assign some task to their team members.The are also responsible for • Conduct data breach and security incident investigations	6

familiar with standard computer operating systems, networks and hardware as well as security software and document-creation applications. .		data storage devices, such as zip and flash drives, that have been deleted, damaged or otherwise manipulated. • Analysts often work on cases involving offenses committed on the Internet ('cyber crime') and examine computers that may have been involved in other types of crime in order to find evidence of illegal activity. .	• Stay proficient in forensic, response and reverse engineering skills • Identify additional systems/networks compromised by cyber attacks	, Recover and examine data from computers and electronic storage devices • Dismantle and rebuild damaged systems to retrieve lost data • Identify additional systems/networks compromised by cyber attacks • Compile evidence for legal cases	
6	6	6	6	6	

SECTION 4

EVIDENCE OF RECOGNITION OR PROGRESSION

What steps have been taken in the design of this or other qualifications to ensure that there is a clear path to other qualifications in this sector?

This qualification comprises both technical and analytic skills and can be linked to any qualification higher than this one, existing or to come.

This course is already running underInformation Security Education &Awareness (ISEA)Project Sponsored by Department of Electronics & IT(DeitY), Ministry Of Electronics& IT(MeitY), Government of India.

Please attach any documents giving further information about any of the topics above.
Sources**:**
https://isea-pmu.in/
http://meity.gov.in

SECTION 5

EVIDENCE OF INTERNATIONAL COMPARABILITY

List any comparisons, which have been established.