GOVERNMENT OF PAKISTAN
AUDITOR-GENERAL OF PAKISTAN
******

No.66(03)/COORD-A.A.G(P)/E-OFFICE/2025 **Islamabad, the 28th August , 2025**

From

Abeerah Waqar
(O/B) Assistant Auditor-General (Personnel)

To

1- Director General (IT), AGP, Islamabad

SUBJECT: APPOINTMENT OF CHIEF INFORMATION SECURITY OFFICERS (CISO) TO STRENGHTHEN NATIONAL CYBERSECURITY

Kindly find attached herewith copy of Director General (nCERT) letter Ref. No. 1-1/2025/DG (NCERT)/401 dated 30th July, 2025

for uploading on the official website for information of the Directorates/F.A.Os of the DAGP.

This issues with the approval of Director General (B&A).

Muhammad Sajjad
AAO (Coord)
01 September, 2025, 12:30:49 PM

Abeerah Waqar
(O/B) Assistant Auditor-General (Personnel)

Copy for information to:-

1- AAO (IT), AGP, Islamabad

Abeerah Waqar
(O/B) Assistant Auditor-General (Personnel)

GOVERNMENT OF PAKISTAN
NCERT
******

No.1-1/2025/DG (NCERT)/401 **Islamabad, the 30th July , 2025**

From

Dr Haider Abbas
DG -(nCERT)

To

1- Chairman HEC, HEC, Islamabad
2- ADG (Immigration), FIA, Islamabad
3- Cabinet Secretary, CAB, Islamabad
4- Chairman, NTCOMM, Islamabad
5- Chief (Water Resources), PC, Islamabad
6- DD-Finance, API, Islamabad
7- DS EXP (Privatization/Overseas/IPC), MOF, Islamabad
8- DS EXP (Religious Affair/NFSR/BOI, MOF, Islamabad
9- Deputy Director Monitoring, FAB, Islamabad
10- Deputy Chief-I (Industries & Commerce), PC, Islamabad
11- Deputy Director Wafaqi Mohtasib, MONHS, Islamabad
12- Director Admin/Housing, NPF, Islamabad
13- Director General, NACTA, Islamabad
14- Director General (Maritime), PC, Islamabad
15- Director General - Admin, NITB, Islamabad
16- Director General FIA, FIA, Islamabad
17- Director Procurement ERRA, NDMA, Islamabad
18- Executive DG (Admin), PEMRA, Islamabad
19- Federal Minister (Communication), MOCM, Islamabad
20- Foreign Secretary, MOFA, Islamabad
21- GM (Human Resource), PPMC, Islamabad
22- Joint Executive Director III (Liquefied Petroleum Gas), OGRA, Islamabad
23- Joint Secretary (Privatization), MOEPWD, Islamabad
24- Parliamentary Secretary, MOC, Islamabad
25- SAPM for Industries & Production Division, MOIP, Islamabad
26- Secretary, NSD, Islamabad
27- Secretary (Revenue Analysis), FBR, Islamabad
28- Secretary Climate Change, MOCC, Islamabad
29- Secretary ECP, ECP, Islamabad
30- Secretary Establishment Division, ESTAB, Islamabad
31- Secretary General(National Assembly), NAS, Islamabad
32- Secretary IT, MoIT, Islamabad
33- Secretary Kashmir Affair,Gilgit Baltistan & SAFRON, kagbsafron, Islamabad
34- Secretary LAW & Justice, MOLJ, Islamabad
35- Secretary NTISB, CAB, Islamabad

36- Secretary Planning, PC, Islamabad
37- Secretary Railway Board, MOR, Islamabad
38- Secretary Revenue Div/Chairman FBR, FBR, Islamabad
39- Secretary Science and Technology, MOST, Islamabad
40- Secretary of Interior, MOINC, Islamabad

SUBJECT: **APPOINTMENT OF CHIEF INFORMATION SECURITY OFFICERS (CISO) TO STRENGTHEN NATIONAL CYBERSECURITY**

Pakistan is undergoing a rapid digital transformation across all sectors. While this evolution presents valuable opportunities for growth, innovation, and operational efficiency, it also introduces significant cybersecurity challenges. Our national infrastructure, institutional operations, and public services are increasingly dependent on digital assets and identities — all of which demand robust and resilient protection mechanisms. Effective cybersecurity, as recognized by global standards, hinges on the triad of People, Process, and Technology (PPT). The "People" component, representing human resources, is paramount. Even with substantial investments in advanced technology, security measures remain ineffective without well-trained and capable human resources to implement, manage and respond to cyber threats.

2. The **National Cybersecurity Policy-2021** and **CERT Rules-2023** set forth requirements for developing existing human resources through capacity building, hiring qualified cybersecurity professionals, and designating a Chief Information Security Officer (CISO) or equivalent based on an organization's particular context and criticality. Qualified human resources will play critical roles in implementing and maintaining a robust cybersecurity posture, shouldering responsibilities including but not limited to the following:-

1. Leading the implementation of cybersecurity frameworks and managing digital risks.
2. Strengthening organizational resilience against evolving cyber threats.
3. Ensuring regulatory compliance.

3. Considering these critical insights, it is highly recommended that organizations, in public and private sector across various industries, to take essential steps tailored to their specific context and also formally appoint a Chief Information Security Officer (CISO) in line with the Cyber Security Policy 2021 who possesses the necessary authority, resources, and expertise. This is a vital move not only for protecting an organization's digital infrastructure but also for contributing to the overarching vision of a Cyber Secure Pakistan.

4. Building a cyber-secure Pakistan is a shared national responsibility demanding unified effort, cooperation, unwavering commitment, and active participation from all stakeholders. Suggested JDs and qualification for CISOs are attached as **Annexure-A** for reference and to tailor to meet specific organizational requirements.

5. All departments are requested to disseminate these with all under command departments/ organizations.

Distribution To:

- PM Office
- All Federal Ministries/ Attached Departments
- All Private Sector Organizations

Dr Haider Abbas
DG -(nCERT)

Annexure- A

Position Title: Chief Information Security Officer (CISO)

Reporting To:

Chief Executive Officer (CEO) / Secretary / Head of Organization / Board / Executive Committee (as applicable)

1. **Qualifications:**

2. **Education:**

   a. 16 years of education from Higher Education Commission (HEC) recognized institution or an internationally reputable university, with major in Cybersecurity, Information Security, Computer Science, or an engineering discipline with emphasis on Information and Communication Technologies.

   b. At least one top professional certification as mandatory requirement including CISSP, CCISO, CEH, PHD or equivalent in IS.

   c. Sector specific certifications such as CCSP, SANS SEC-540, ICS/SCADA 410, PCI-DSS and/or certifications on relevant ISO standards etc. may be added as a preferable requirement.

3. **Experience:**

   a. At least 7 years of relevant post-qualification experience with Masters in information security or relevant field, with 3–5 years in a senior security leadership role.

   b. At least 10 years of relevant post-qualification experience with bachelor in Cybersecurity, Information Security, Computer Science, or relevant engineering discipline with emphasis on Information and Communication Technologies, with 3–5 years in a senior security leadership role.

   c. Proven track record of designing, implementing, and managing cybersecurity programs.

   d. Proven experience in managing at least one of the following programs: Governance, Risk, and Compliance (GRC), Security Operations Center (SOC), Security Testing, or Digital Forensics.

e. Experience with regulatory compliance (e.g. GDPR, NIST, ISO 27001, PCI-DSS, DORA and relevant local cybersecurity frameworks as per organizational needs).

4. **Skills**:

a. In-depth knowledge of information security governance, risk management, compliance, incident response, and emerging cyber threats.

b. Must have sound knowledge of technology solutions in Information Security, such as XDR, SIEM, SOAR, Threat intelligence, NGFW, WAF, EDR, Pen Testing, Source Code Testing etc.

c. Strong understanding of **cloud security landscape**, threats, and best practices to secure cloud infrastructure and services.

d. In-depth knowledge of **generative AI security landscape**, including associated threats, risks, and mitigation strategies.

e. Excellent logical, interpersonal, communication (both oral and written) and analytical skills.

f. Strong leadership and communication skills, with the ability to collaborate across departments and communicate effectively with executive leadership.

g. Familiarity with national and sectoral cybersecurity policies and international standards.

5. **Job Description (May be tailored as per Organizational requirement)**:

The Chief Information Security Officer (CISO) is responsible for establishing and leading the organization's information security strategy, ensuring the confidentiality, integrity, and availability of digital assets. The CISO will work closely with leadership to align cybersecurity initiatives with business goals and regulatory requirements.

Key Responsibilities:

a. **Cybersecurity Governance**:

(1) Develop and enforce an enterprise-wide information security strategy, policies, and procedure.

(2) Ensure alignment with the Pakistan National Cybersecurity Policy 2021 and other relevant national guidelines.

b. **Risk Management**:

(1) Conduct regular cybersecurity risk assessments and business impact analyses.

(2) Identify, evaluate, and mitigate cyber risks across the organization.

c. **Compliance & Audit**:

(1) Ensure compliance with local and international cybersecurity regulations and standards.

(2) Lead internal and external audits of security practices and controls.

d. **Security Architecture & Operations**:

(1) Oversee deployment and management of security tools, technologies, and frameworks.

(2) Implement controls to safeguard networks, systems, applications, and data.

e. **Incident Response**:

(1) Develop and maintain the incident response plan (IRP).

(2) Lead the response to cybersecurity incidents, including containment, recovery, investigation, and reporting.

f. **Awareness & Training:**

(1) Promote cybersecurity awareness across all levels of the organization.

(2) Develop training programs to improve security posture and reduce human error.

g. **Collaboration & Reporting:**

(1) Serve as the primary liaison with National CERT and other regulatory bodies.

(2) Report regularly to executive leadership on cybersecurity posture, risks, and ongoing initiatives.