

No. A-12031/1/2023-PERS-BCAS-Part(2) (E-298440)

Government of India
Ministry of Civil Aviation
Bureau of Civil Aviation Security

'A' Block, IInd Floor, Udaan Bhawan,
Safdarjung Airport, New Delhi- 110003.

Dated: 16th October 2026

CIRCULAR

Subject: Inviting applications from individuals, who are citizen of India, for the post of Cyber Security Consultant for an initial period of one year in the Bureau of Civil Aviation Security, Ministry of Civil Aviation on a Contractual basis– reg.

The Bureau of Civil Aviation Security (BCAS), an attached office of the Ministry of Civil Aviation, Government of India, invites applications from individuals, who are citizens of India, for the post of CYBER SECURITY CONSULTANT for an initial period of one year in the Bureau of Civil Aviation Security, Ministry of Civil Aviation on a Contractual basis, *within 30 days of publication of this circular in the Employment newspaper*, as under:

Name of the Post	Number of Vacancy
Cyber Security Consultant	01

2. The details of eligibility requirements, duties/responsibilities, number of vacancies, upper age limit, period of engagement, remuneration, etc. for engagement of consultants are provided below:

Sl. No.	Name of the Post	Cyber Security Consultant
(i)	Total Vacancy	01
(ii)	Eligibility Criteria	<u>MANDATORY (ESSENTIAL) REQUIRMENTS:</u> 1. <u>Educational Qualification:</u> Master's degree in Computer Science/ Information Technology/ Cyber Security, Electronics & Communication or equivalent from a recognised University or Institution 2. <u>Professional Certifications:</u> At least one of the globally recognised cyber-security certifications such as CISSP, CISM, CISA, CCSP, or equivalent. 3. <u>Experience:</u> <ul style="list-style-type: none">• Minimum 10 years of experience in cyber security / information security domain, of which at least 3 years should be in a senior/lead role.• Comprehensive understanding and practical understanding of one or more of the following: security policy formulation, risk assessments, incident response, vulnerability management, security architecture, security audits.• Practical experience of working in large-scale IT/OT/Network environments (for example in Government / PSU / large enterprise).

		<p>4. <u>Knowledge & Skills:</u></p> <ul style="list-style-type: none"> • Strong knowledge of cybersecurity frameworks, standards and controls (e.g.; ISO/IEC 27001, NIST SP 800 series, COBIT, ITIL security, etc). • Good understanding of network protocols, OS platforms (Windows, Linux/Unix), firewalls, IDS/IPS, endpoint security, encryption, identity & access management. • Ability to conduct/lead risk assessments, threat modelling, vulnerability assessments, security architecture reviews, incident investigations. • Good written and verbal communication skills, ability to prepare security policies, SOPs, reports, presentations. <p>5. <u>Compliance & Regulatory Awareness:</u></p> <ul style="list-style-type: none"> • Familiarity with Indian legal and regulatory environment in cyber/information security. • Awareness of Government of India cybersecurity policy, guidelines, best practices (Information Technology Act, 2000, Understanding of Government policies/guidelines regarding cyber-crimes and cyber/IT laws in India.) <p>6. <u>Key Responsibilities:</u></p> <ul style="list-style-type: none"> • Develop, review, and enforce comprehensive cybersecurity policies, standards, and procedures specifically designed for airport infrastructure and operations. • Formulate long-term cybersecurity strategies aligned with national cybersecurity guidelines (CERT-In, NCIIPC). • Lead cybersecurity tabletop exercises, simulations, and training sessions based on documented policies to enhance organizational preparedness. • Conduct risk assessments to identify vulnerabilities and policy gaps. recommend mitigation measures accordingly. • Lead awareness programs and training initiatives to embed cybersecurity best practices across all Airport operational and administrative teams. • Monitor cybersecurity trends, threats, and regulatory changes to update policies and strategy proactively. • Develop incident response policies and governance frameworks to improve resiliency and recovery. • Report regularly to senior management and stakeholders on policy compliance status, risk posture, and strategic progress. • Develop and implement a comprehensive cybersecurity strategy for airport IT and OT (Operational Technology) systems. • Monitor, detect, and respond to cybersecurity incidents across all network layers including SCADA, baggage handling systems, access control, and flight operations systems. • Ensure compliance with Indian cybersecurity frameworks (CERT-In, NCHIPC guidelines, DGCA regulations, and BCAS directives).
--	--	---

		<ul style="list-style-type: none"> • Collaborate with Government Security Agencies and vendors for security audits and system upgrades. • Train airport IT and operations personnel in cyber hygiene and emerging threat awareness. • Develop disaster recovery and business continuity plans focusing on cyber resilience <p>7. <u>Skills Required:</u></p> <ul style="list-style-type: none"> ○ Malware Analysis ○ Threat Intelligence <p><u>DESIRABLE:</u></p> <ul style="list-style-type: none"> ○ International experience of having trained officers of International Bodies on Cyber Security. ○ Having testified before any Government Committee. ○ Having organized and spoken at international conferences on the subject of Cyber Security, Cybercrime and Cyber law. ○ Running/conducting courses on Cyberlaw, Cybercrime, Cybersecurity and Artificial Intelligence. ○ Having authored publications and Books on Cyberlaw and Cybersecurity law, to his/her credit. ○ Work experience in fields related to Information Technology Act, 2000 and its amendments. Understanding of Government policies/guidelines regarding cybercrimes and cyber/IT laws in India.
--	--	---

2.1 Age Criteria: The applicant should not be above the age of 55 years and not below the age of 35 years as on the closing date of this advertisement. Applicant should be in good health for discharging his/her official duties effectively.

2.2 Period of Engagement: The engagement of the Consultants shall be purely on a contractual professional consultancy basis initially for a period of one year or curtailed as per the requirement and satisfactory performance of the Consultant. The term of engagement may be extended on the basis of performance review and mutual agreement by upto one year at a time with the approval of the Competent Authority. However, no extension will be given beyond the age of 65 years. The Consultants will not confer any right for regular appointment in BCAS.

2.3 Remuneration & Allowances:

2.3.1 The Consultant shall be paid a fixed consolidated lump sum monthly remuneration of Rs. 2,00,000/- (Rs. Two Lakhs only).

2.3.2 No Transport allowance, DA, HRA, PF, Pension, Insurance, Gratuity, Medical Attendance Treatment, Seniority, Promotion, etc., or any other benefits will be admissible.

2.3.3 The amount of remuneration so fixed shall remain unchanged for the term of the contract.

2.3.4 The Income Tax or other tax(es) will be deducted at source as per Government instructions.

2.4 Working Conditions: The consultant shall provide professional consultancy services to the office of DG/Jt.DG, BCAS on the various subjects and aspects as detailed above.

2.5 Termination of Agreement: The BCAS may terminate the contract, if: -

2.5.1 The Consultant is unable to address the assigned work.

2.5.2 The quality of the assigned work is not upto the satisfaction of the Controlling Officer/ Competent Authority in the BCAS.

2.5.3 The Consultant is found lacking in honesty and integrity.

2.5.4 The Competent Authority in the BCAS may also terminate the contract by giving 01-month's advance notice and also without assigning any reason. If the Consultant wishes to resign from the post, he/she has to inform BCAS *in writing* at least 01 month before.

2.6 General Terms & Conditions:

2.6.1 The Intellectual Property Rights (IPR) of the data collected as well as deliverables produced for the BCAS shall remain within the office.

2.6.2 No one shall utilize or publish or disclose or part with, to a third party, any part of the data or statistics or proceedings or information collected for the purpose of his assignment or during the course of the assignment and even after termination of the contract without the express written consent of the BCAS.

2.6.3 The Consultant would be required to sign a non-disclosure undertaking before being assigned any work.

2.6.4 The Consultant shall in no case represent or give opinion or advice to others in any matter which is adverse to the interest of BCAS nor will he/she indulge in any activity outside the terms of the contractual assignment. If at any point of time, it appears so, the engagement can be terminated with immediate effect.

2.6.5 The Consultant shall not claim any benefit/compensation/absorption /regularization of service with this Department.

2.6.6 The candidates called for Personal Interview/Interaction will not be entitled to any TA/DA for attending the same. Similarly, the candidate selected as Cyber Security Consultant will not be entitled to any TA/DA for joining the BCAS.

3. The person who fulfills the eligibility criteria as mentioned above and is willing to provide their professional consultancy services as a Consultant against the above post on the terms and conditions mentioned above must submit his/her application in the prescribed format enclosed as **Annexure-I, along with the self-attested copies of documents**, and a Non-Disclosure Undertaking, as per **Annexure-II** to the undersigned **within 30 days of publication of this circular in the Employment newspaper.**

4. **Procedure for Selection:** Candidates meeting the conditions above will be shortlisted based upon criteria formulated by the BCAS and as per the extant provisions of General Financial Rules (GFRs).

4.1. The decision of the Evaluation Committee constituted for the purpose will be final and binding on all candidates. Applications received with incomplete information or received beyond the closing date will not be considered and will be summarily rejected without any further communication.

Okalra
26/10/26

(Veena Kalra)

Joint Director (Admn.-I)

Tele No: 011 - 24655166

Email: diradmn.bcas@gov.in

To:

- i. All Ministries/Departments of Government of India – *through BCAS/MoCA website.*
- ii. The President, ASSOCHAM, 4th Floor, YMCA Cultural Centre and Library Building, 01, Jai Singh Road, New Delhi – 110001 *with the request to give wide publicity to this Circular among the eligible and willing candidates and furnish list of potential Consultants for engagement.*
- iii. NIC to upload this Circular on the website of Ministry of Civil Aviation & BCAS.
- iv. All I/Cs of Regional Offices of BCAS *with the request to give wide publicity to this Circular.*
- v. Notice Board.
- vi. Office Order Folder.

Annexure-I**Application for engagement as Cyber Security Consultant on contractual basis in the BCAS:**

1.	Name of the post applying for		Photo		
2.	Name				
3.	Father/Mother/Husband's Name				
4.	Date of Birth				
5.	Permanent Address				
6.	Address for Correspondence				
7.	Contact Tel No./Mobile No.				
8.	Email ID				
9.	Educational Qualification(s) (self-attested copies of certificates)				
10.	Bank A/c Details (with copy of passbook/cancelled cheque)				
11.	Details of Experience (Add separate sheet if required)				
12.	Designation/Position and Name of Organization	From	To	Nature of Work	Remarks
13.	Any other experience/details				

DECLARATION

I do hereby declare that the particulars above are true and correct to the best of my knowledge. I understand and agree that in the event of any information being false incorrect/incomplete or ineligibility being detected at any time before or after the selection, my candidature is liable to be rejected and I will be bound by the decision of BCAS in this regard. All terms and conditions of engagement as mentioned in the circular are acceptable to me.

Signature

Place:

Date:

Full name of the applicant

NON-DISCLOSURE UNDERTAKING

To

The Joint Director (Admn.-I),
Bureau of Civil Aviation Security,
'A' Block, IInd Floor, Udaan Bhawan,
Safdarjung Airport, New Delhi- 110003.

Sir,

I hereby undertake:

- Not to represent or give opinion or advice to others in any matter which is adverse to the interest of the office nor will I indulge in any activity outside the terms of the contractual assignment. If at any point of time, it appears so, the engagement can be terminated with immediate effect.
 - To treat all the information that comes to my knowledge as part of my duties in this office as confidential information and keep it strictly confidential;
 - Not to sell, trade, publish, or otherwise disclose to anyone in any manner whatsoever including by means of reproduction either in physical, hardcopy, digital or in electronic format;
 - To hold such confidential information in trust and confidence both during and after the term of my engagement;
 - Not to engage in any other employment/occupation/consultancy or any other activity during my engagement with BCAS which would otherwise conflict with my obligations towards BCAS;
 - To abide by data security policy and related guidelines issued by BCAS;
 - Not to resort to any corrupt practices in any aspect and at any stage during the tenure of engagement; and
 - To maintain the highest standards of ethics & integrity during the period of engagement as a Consultant in BCAS.
2. In the event of termination of my engagement for any reason whatsoever, I shall promptly surrender and deliver to the BCAS any records/material/equipment/documents or data which is of confidential nature.
3. I shall keep BCAS informed of any change in my address or contact details during the period of my engagement.
4. I understand that I can be terminated at any point of time for breach of the above conditions and can be proceeded against under the relevant laws for the time being in force.
5. For the purpose of this undertaking, confidential information means any such information received from any source, whether in physical, electronic or in digital format.

Yours sincerely,

Signature

Name:.....

Address & Contact No.....

Dated:.....