भारत सरकार
Government of India
प्रणाली एवं आंकडा प्रबंधन महानिदेशालय
Directorate General of Systems & Data Management
अप्रत्यक्ष कर एवं सीमा शुल्क
Indirect Taxes and Customs
1st फ़्लोर, एनबीसीसी प्लाजा, पुष्प विहार,नई दिल्ली -110017
1st Floor, NBCC Plaza, Pushp Vihar, New Delhi-110017
Dccs.dgsys@icegate.gov.in 011-29561543

F.No:**DGSYS/APP/DCCS/MISC/24/2023-O/O ADG-DCCS-DGS-DELHI**
Date:09-09-2025

ADVISORY No. 04/2025

Sub: Advisory on Urgent Cybersecurity Measures for All Customs & CGST Zones / Directorates under CBIC who are running their own applications, websites and Utilities OR have IT infrastructure outside the CBIC Data Centre-reg.

In wake of **recent and serious cyber security incidents** targeting critical financial organizations in the country, all Customs & CGST Zones, Directorate Generals, and Directorates under CBIC are hereby directed to immediately strengthen their **cybersecurity posture** across all CBIC IT Infrastructure, Applications, Websites, and Utilities.

1. Threat Intelligence Alert

NIC-CERT and CERT-In have issued alerts regarding a **possible intrusion in CBIC networks** by a sophisticated threat group, likely *Scattered Spider*. This intrusion attempt poses an **imminent risk of large-scale compromise,** including **data exfiltration, ransomware attacks, and persistent backdoors.**

All entities are **mandated to:**

- Conduct immediate investigation to determine any foothold of adversaries in CBIC networks.
- Verify and eliminate any backdoors or unauthorized tools deployed by attackers.
- Reset all potentially exposed credentials.
- Review and harden configurations of all IT systems.
- Carry out a comprehensive sanitization exercise across CBIC's IT infrastructure.

2. Mandatory Monitoring & Security Assurance

All organizations must actively **audit, monitor, and harden** their IT-enabled applications, websites, and utilities — both under development and already in operation. These checks are **non-negotiable** and should be executed without delay.

3. Precautionary Measures (to be implemented immediately):

a. **Deploy phishing-resistant Multi-Factor Authentication (MFA)** at all critical decision points within applications and administrative systems.
b. **Strengthen IT help desk protocols** — enforce rigorous identity verification for password resets, MFA changes, and access requests.
c. **Adopt a Zero-Trust Security Model** to prevent lateral movement and limit unauthorized access within networks.
d. **Conduct mandatory security awareness training** for all officials and staff, with emphasis on identifying and reporting social engineering, phishing, and insider threats.
e. **Create a no-reprisal reporting mechanism** — all staff must feel empowered to escalate suspicious activities without hesitation.

4. Sanitization & Remediation Activities (immediate and continuous):

a. Conduct thorough **backdoor hunting exercises** in applications and servers to detect and remove hidden access points planted by attackers.
b. Scan for **deployment of webshells and remote monitoring/management tools** (AnyDesk, Atera, GoTo Resolve, ScreenConnect, Splashtop, TeamViewer, Zoho Assist, etc.) that may have been stealthily installed.
c. Ensure **timely application of security patches** and urgent remediation of known vulnerabilities across all systems.
d. Frame and enforce a **strict password management policy**, ensuring least-privilege access.
e. **Report without delay** any suspicious or confirmed malicious activity to CERT-In for coordinated response and assistance.
f. Proactively monitor servers for **unfamiliar processes, unknown temp files, suspicious user IDs,** and sanitize them immediately.
g. Institute **mandatory periodic password changes** across all critical systems.
h. Enforce **regular vendor ID sanitization** to eliminate dormant or unauthorized vendor accounts.
i. You may also refer to below mentioned ANTARANG link for various advisories issued in this regard.

https://antarang.icegate.gov.in/communities/service/html/communityview?communityUuid=698b9a54-0931-4632-8e8d-d308a33dfd2a

This is a critical directive, not a routine advisory. Any negligence may directly compromise national revenue systems.

This issues with the approval of Principal Additional Director General, DCCS/CISO, DG Systems & Data Management, New Delhi.

Digitally signed by
Jitendra Bansal
Date: 09-09-2025
17:49:42

(Jitendra Bansal)
Assistant Director/Dy. CISO,
DG Systems & Data Management, New Delhi.