पेंशन निधि विनियामक और
विकास प्राधिकरण
बी–14/ए, छत्रपति शिवाजी भवन,
कुतुब संस्थागत क्षेत्र,
कटवारिया सराय, नई दिल्ली–110016
दूरभाष : 011–26517501, 26517503, 26133730
फैक्स : 011–26517507
वेबसाईट : www.pfrda.org.in

PENSION FUND REGULATORY
AND DEVELOPMENT AUTHORITY
B-14/A, Chhatrapati Shivaji Bhawan,
Qutub Institutional Area,
Katwaria Sarai, New Delhi-110016
Phone : 011-26517501, 26517503, 26133730
Fax : 011-26517507
Website : www.pfrda.org.in

CIRCULAR

CIR No.: PFRDA/2021/20/ICS-INTERMDRY/1 **Date: June 30, 2021**

To,

All NPS Intermediaries

Subject: Timely Report of Data Breach to CERT In

Digital transformation in the pension sector has brought a lot of unique advantages for the stake holders to provide and avail the benefits of NPS/APY by the intermediaries and the Subscribers respectively. However, the ease offered by the digital enablers is also challenged by cyber security incidents and the breaches which are perpetrated by exploiting the prevailing vulnerabilities in the data system framework of NPS intermediaries.

1. Cyber Security incidents are real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service or disruption, unauthorized use of a computer resource for processing or storage of information or changes to data, information without authorization.

2. Cyber Security breaches are unauthorized acquisition or unauthorized use by a person as well as an entity of data or information that compromises the confidentiality, integrity or availability of information maintained in a computer resource.

3. The Personally Identifiable Information of NPS/APY Subscribers viz Date of Birth, Email Id, Permanent Retirement Account No (PRAN), Aadhaar No, Address, PAN, Associated Bank Acct No, IFSC, Nominee details, Corpus in the Acct, Tier I/II details etc. which if availed by the cyber criminals by breaching into the IT system of intermediaries could be used for further attacks such as identity theft, social engineering etc.

4. Computer Emergency Response Team India (CERT-IN) tracks the cyber threats to provide guidance and assist NPS intermediaries to bolster the security system and manage the implications of such breaches/attacks which requires *the intermediaries to proactively report those incidents*.

5. The policy on cyber security issued by PFRDA vide its circular no *PFRDA/2017/31/CRA/5 dated 04-10-2017* requires that the intermediaries need to adhere to the rules, regulations and guidelines prescribed by CERT-In and National Critical Information Infrastructure Protection Centre (NCIIPC) under the IT act. The intermediaries need to strengthen the cyber audit framework as per the emerging cyber threats and share information about cyber incidents, breaches and vulnerabilities to CERT-In.

6. All the NPS intermediaries are advised to report any such cyber security threats as per the format (Annexure II) and as a best practice, the cyber security breaches shall be reported to CERT-In within *2 to 6 hours*. An indicative list of cyber security threats (Annexure I) provided for ready reference.

7. For any queries/assistance, Mr. C. Vignesh (*vignesh.c@pfrda.org.in*) or the undersigned can be contacted.

This circular is issued under section 14 of PFRDA Act 2013 and is available at PFRDA's website (www.pfrda.org.in) under the Regulatory framework in "Circular" section.

Yours Sincerely,

K Mohan Gandhi

General Manager

(k.mohangandhi@pfrda.org.in)

ANNEXURE I

An indicative list of cyber security threats

1. Targeted scanning/probing of critical networks/systems.
2. Compromise of critical systems/information.
3. Unauthorized access of IT systems/data.
4. Defacement of website or intrusion into a website and unauthorized changes such as inserting malicious code, links to external websites, etc.
5. Malicious code attacks such as spreading of virus/worm/Trojan/botnets/spyware.
6. Attacks on servers such as database, mail, and DNS and network devices such as routers.
7. Identity theft, spoofing and phishing attacks.
8. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks.
9. Attacks on critical infrastructure, SCADA systems and wireless networks.
10. Attacks on applications such as e-governance, e-commerce, etc.

ANNEXURE II

Incident Reporting Form

Form to report Incidents to CERT-In			
For official use only:		Incident Tracking Number : **CERTIn-xxxxxx**	
1. Contact Information for this Incident:			
Name:	Organization:	Title:	
Phone / Fax No:	Mobile:	Email:	
Address:			
2. Sector : (Please tick the appropriate choices)			
Government Financial Power	Transportation Manufacturing Health	Telecommunications Academia Petroleum	InfoTech Other _____
3. Physical Location of Affected Computer/ Network and name of ISP.			
4. Date and Time Incident Occurred:			
Date:	Time:		
5. Is the affected system/network critical to the organization's mission? (Yes / No). Details.			
6. Information of Affected System:			
IP Address:	Computer/ Host Name:	Operating System (incl. Ver./ release No.)	Last Patched/ Updated	Hardware Vendor/ Model
7. Type of Incident:			
Phishing Network scanning /Probing Break-in/Root Compromise Virus/Malicious Code Website Defacement System Misuse	Spam Bot/Botnet Email Spoofing Denial of Service(DoS) Distributed Denial of Service(DDoS) User Account Compromise	Website Intrusion Social Engineering Technical Vulnerability IP Spoofing Other_____	
8. Description of Incident:			

9. Unusual behavior/symptoms (Tick the symptoms)	
System crashes New user accounts/ Accounting discrepancies Failed or successful social engineering attempts Unexplained, poor system performance Unaccounted for changes in the DNS tables, router rules, or firewall rules Unexplained elevation or use of privileges Operation of a program or sniffer device to capture network traffic; An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user A system alarm or similar indication from an intrusion detection tool Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server	Anomalies Suspicious probes Suspicious browsing New files Changes in file lengths or dates Attempts to write to system Data modification or deletion Denial of service Door knob rattling Unusual time of usage Unusual usage patterns Unusual log file entries Presence of new setuid or setgid files Changes in system directories and files Presence of cracking utilities Activity during non-working hours or holidays Other (Please specify)

10. Has this problem been experienced earlier? If yes, details.

12. Agencies notified?			
Law Enforcement	Private Agency	Affected Product Vendor	Other_____

11. When and How was the incident detected:

13. Additional Information: (Include any other details noticed, relevant to the Security Incident.)	
Whether log being submitted	Mode of submission:

OPTIONAL INFORMATION

14. IP Address of Apparent or Suspected Source:	
Source IP address:	Other information available:

15. Security Infrastructure in place:				
	Name	OS	Version/Release	Last Patched/Updated
Name OS Version/Release Last Patched / Updated				
Anti-Virus				
Intrusion Detection/Prevention Systems				
Security Auditing Tools				
Secure Remote Access/Authorization Tools				
Access Control List				
Packet Filtering/Firewall				
Others				

16. How Many Host(s) are Affected		
1 to 10	10 to 100	More than 100
17. Actions taken to mitigate the intrusion/attack:		
No action taken System Binaries checked	Log Files examined System(s) disconnected form network	Restored with a good backup Other_____
Please fill all mandatory fields and try to provide optional details for early resolution of the Security Incident		
Mail/Fax this Form to: CERT-In, Electronics Niketan**,** CGO Complex, New Delhi 110003 Fax:+91-11-24368546 or email at: incident@cert-in.org.in		