नाबार्ड

EC No. 332 / DoS 55 /2020

NB.DOS.HO.CSITE.NO/3187/ CS-01 /2020-21

21 December 2020

The Chairman/MD/CEO
All Regional Rural Banks
All State Co-operative Banks
All District Central Co-operative Banks

Dear Sir

Cyber Security Framework in Banks- Reporting of Near Misses

In order to enhance the resilience of cooperative banks and RRBs in improving their defence against cyber risks, NABARD had issued a comprehensive circular on cyber security framework dated 16 March 2018. NABARD had further issued circular dated 6 February 2020 for classifying banks from Level I to Level IV depending upon their digital depth and interconnectedness and putting in place necessary controls in tune with their level and exposure to cyber risks.

2. So far, banks have been reporting cyber incidents, which are actual breaches in the system through various cyber threats like ransomware, phishing attacks, hacking, exploitation of existing vulnerability etc. Banks have been reporting these incidents in the prescribed format (Annexure 3) as envisaged in our circular dated 16 March 2018.

3. However, a need has been felt to capture information relating to cyber incidents which are Near Misses. "Near Miss" may be defined as failed attempt of fraudulent transactions which were prevented, suspicious activity that was detected or calculation errors which were discovered. Although Near Misses have not resulted in any loss/ damage, they are important to prevent future incidents.

नाबार्ड

4. Capturing data on Near Misses/failed attempts provide insights into emerging threat patterns, vulnerabilities and lacunae within legal frameworks. From a supervisor's point of view, this will provide system wide benefits as receiving reports of near misses facilitates adoption of safeguards and development of counter-measures to emerging threat vectors.

5. In order to enable reporting of near misses, the existing reporting format has been revised to cover reporting for both actual breaches and failed attempts/Near Misses. As this is an incident based reporting, in case of occurrence of breaches /Near Misses in your bank, you may submit the return by mail till submission module in ENSURE portal is enabled. A copy of revised Annexure 3, as indicated above, is enclosed.

6. A copy of this circular may be placed before the Board of Directors of the Bank in its ensuing meeting

Please acknowledge receipt to our Regional Office.

Yours faithfully

(K. S. Raghupathi)
Chief General Manager

Encl: As above

Annexure 3

Template for reporting Cyber Incidents

1. Security Incident Reporting (SIR) to NABARD (within 6 hours):

2. Subsequent update(s) NABARD (updates to be provided if the earlier reporting was incomplete i.e. investigation underway or new information pertaining to the incident has been discovered or as per request of NABARD):

Basic Information	
1. Particulars of Reporting:	
•Name of the bank	
• Date and Time of Reporting to RBI,NABARD,CERT-In, other agencies (please mention separately time of reporting to each)	
• Name of Person Reporting	
• Designation/Department	
• Contact details (e.g. official email-id, telephone no, mobile no)	
2.Category of Incident : (a. Successful Attempt or b. Unsuccessful Attempt/ Near Miss)	
3. Details of Incident:	
• Date and time of incident detection	
•Type of incidents and systems affected (i) **Outage of Critical IT system(s)** (e.g. CBS, Treasury Systems, Trade finance systems, Internet banking systems, ATMs, payment systems such as SWIFT, RTGS, NEFT, NACH, IMPS, etc.) (ii) **Cyber Security Incident** (e.g. DDOS, Ransom ware/crypto ware,	

data breach, data destruction, web defacement, etc.)? [Please complete Annex] (iii) **Theft or Loss of Information** (e.g. sensitive customer or business information stolen or missing or destroyed or corrupted)? (iv) **Outage of Infrastructure** (e.g. which premises-DC/Central Processing Units, branch, etc., power/utilities supply, telecommunications supply,)? (v) **Financial** (e.g. liquidity, bank run)? (vi) **Unavailability of Staff** (e.g. number and percentage on loss of staff /absence of staff from work (vii) **Others** (e.g. outsourced service providers, business partners, breach of IT Act/any other law and RBI/NABARD/SEBI regulations. Etc.)?	
• What actions or responses have been taken by the bank at the time of first reporting/till the time of subsequent reporting?	
4. Impact Assessment(examples are given but not exhaustive):	
• Business impact including availability of services – Banking Services, Internet banking, Cash Management, Trade Finance, Branches, ATMs, Clearing and Settlement activities, etc.	
• Impact on stakeholders– affected retail/corporate customers, affected participants including operator(s), settlement institution(s), business partners, and service providers, etc	
Financial and market impact – Trading activities, transaction volumes and	

values, monetary losses, liquidity impact, bank run, withdrawal of funds, etc.	
• Regulatory and Legal impact	
5. Chronological order of events:	
• Date of incident, start time and duration.	
• Escalations done including approvals sought on interim measures to mitigate the event, and reasons for taking such measures	
• Stakeholders informed or involved	
• Channels of communications used (e.g. email, internet, sms, press release, website notice, etc.)	
• Rationale on the decision/activation of BCP and/or DR	
6. Root Cause Analysis(RCA):	
• Factors that caused the problem/ Reasons for occurrence, Cause and effects of incident	
• Interim measures to mitigate/resolve the issue, and reasons for taking such measures, and	
• Steps identified or to be taken to address the problem in the longer term. List the remedial measures/corrections affected (one time measure) and/or corrective actions taken to prevent future occurrences of similar types of incident	
7. Date/target date of resolution_____ (DD/MM/YYYY).	

Note: All fields are REQUIRED to be filled unless otherwise stated

General Information	Report No:

1. Contact Information: (Please provide if different from what is reported in Basic Information above)

Name of bank:

Name of the person reporting and Designation:

Department Official Email :

Telephone/Mobile :

2. Is this a ☐New incident ☐Update to reported incident?

• For the first update, please indicate "1. If this is an update to a reported incident please provide the update number for this update. (X.1, X.2, X.3, X.4, etc. where X is the Report No.

Update No:

3.Category of Incident :

(a. Successful Attempt
or
b. Unsuccessful Attempt/ Near Miss)

4. If any change in the category of Incident which stands different from previous reporting

5.What severity is this incident being classified as?

Severity 1 ☐ Affected critical system(s)/ customer facing applications/systems, crippled Internal network or a combination of the above	Severity 2 ☐ Incident occurred on system or network that could put the bank's network / critical system(s) or a combination of them at risk	

Information about the Incident

6. Please indicate the date and time the incident was reported to the RBI. If it is also reported to Other Agencies (CERT-In/NCIIP), Law enforcement agencies, separately indicate the date and time of such reporting.

If known, any TCP or UDP ports involved in the incident.

If known, provide the affected system's IP address If known, provide the attacker's

IP address

Where relevant, please indicate the Operating System of the affected critical system(s):

11. What is the impact of the attack? (Tick 'one' checkbox for each column)

Customer Service Delivery)	**(Loss of Sensitive Information**	**Public Confidence and Reputation**
☐No Impact	☐No loss	☐No Impact
☐Minor Impact	☐Minor Loss	☐Minor Impact
☐Major Impact	☐Major Loss	☐Major Impact
☐Serious Impact	☐Serious Loss	☐Serious Impact
☐Severe Impact	☐Severe Loss	☐Severe impact

12. Does the affected critical system(s)/ network(s) have potential impact to another critical system/critical asset(s) of the bank?

• If "Yes", please provide more details.

Incident Status

13. What is/are the type(s) of follow up action(s) that has/have been taken at this time?

14. What is the current status or resolution of this incident?

If it is not resolved, what is the next course of actions?

15. What is the earliest known date of attack or compromise? (Tick 'checkbox' if unknown)

(Please specify in Indian Local Time +5.30 GMT)

Date: . Unknown: ☐

16. What is the source/cause of the incident? ('NIL' OR 'NA' if unknown)

17. Has the incident been reported to CERT-In/NCIIP/ any law enforcement agency/ IB-CART?.

- If "Yes", specify the agency that is being reported to.

18. Is chain of custody maintained?

19. Has the bank filled chain of custody form?

20. What tools were used for collecting the evidence for the incident?

Attack Vectors

E1. Did the bank locate/identify IP addresses, **domain names, related to the incident**

Whether the Indicators of Compromise, list of IP addresses identified from the incident, involvement of the IP addresses in the incident (ex. Victim, Malware Command & Control Servers, etc.), domain names resolved, involvement of the domain names in the incident. (ex. Drive-by-download Servers, Malware Control & Command Servers, defaced website), email addresses identified and their involvement, malicious files/attachments (file name, size, MD5/SHA1 hash, etc.) etc. have been reported in IB-CART/CERT-IN/NCIIP/NABARD/ Law enforcement agencies.
