भारत सरकार

वित्त मंत्रालय

वित्तीय सेवाएं विभाग

लोक सभा

अतारांकित प्रश्न संख्या 1038

जिसका उत्तर सोमवार, 2 दिसम्बर, 2024/11 अग्रहायण, 1946 (शक) को दिया गया

बैंकिंग क्षेत्र/सार्वजनिक क्षेत्र के बैंकों में साइबर सुरक्षा ढांचे की स्थिति

1038. श्री बैन्नी बेहनन:
श्री एंटो एन्टोनी:
श्री तनुज पुनिया:
श्री के. सुधाकरन:

क्या वित्त मंत्री यह बताने की कृपा करेंगे किः

(क) सार्वजनिक क्षेत्र के बैंकों (पीएसबी) में कार्यान्वित साइबर सुरक्षा ढांचे की वर्तमान स्थिति क्या है;

(ख) नवीनतम सुरक्षा नयाचारों का अनुपालन करने वाले सरकारी क्षेत्र के बैंकों की सूची क्या है;

(ग) विशेषकर बढ़ते डिजिटल लेन-देन और ऑनलाइन बैंकिंग सेवाओं के संदर्भ में साइबर खतरों से वित्तीय आंकड़ों की सुरक्षा करने में किन-किन विशिष्ट चुनौतियों का सामना करना पड़ा है;

(घ) उक्त चुनौतियों का सामना करने और साइबर हमलों से स्वयं को बचाने में वित्तीय संस्थाओं को सक्षम बनाने के लिए क्या कदम उठाए गए हैं; और

(ड.) सरकार द्वारा इन साइबर सुरक्षा उपायों की प्रभावकारिता की निगरानी और मूल्यांकन करने के लिए क्या उपाय किए गए हैं/किए जा रहे हैं?

उत्तर

वित्त मंत्रालय में राज्य मंत्री (श्री पंकज चौधरी)

(क) और (ख): भारतीय रिजर्व बैंक (आरबीआई) सार्वजनिक क्षेत्र के बैंकों (पीएसबी) सहित सभी बैंकों को साइबर सुरक्षा ढांचे को सुदृढ बनाने के लिए समय-समय पर विविध परिपत्र/दिशानिर्देश जारी करता है। इन परिपत्रों/दिशानिर्देशों को बैंकों द्वारा लागू किया जाना अपेक्षित है। इनमें, अन्य बातों के साथ-साथ, निम्नलिखित शामिल हैं:-

- बैंकों में व्यापक साइबर सुरक्षा ढांचे के संबंध में 2 जून, 2016 का परिपत्र जिसमें बोर्ड द्वारा अनुमोदित साइबर सुरक्षा नीति, सुरक्षा परिचालन केंद्र, साइबर संकट प्रबंधन योजना आदि लागू करने का अधिदेश दिया गया है।
- डिजिटल भुगतान सुरक्षा नियंत्रण के संबंध में 18 फरवरी, 2021 को जारी मास्टर निदेश में बैंकों को इंटरनेट, मोबाइल बैंकिंग, कार्ड भुगतान आदि जैसे विभिन्न भुगतान चैनलों के सुरक्षा नियंत्रण के सामान्य न्यूनतम मानकों को लागू करने का अधिदेश दिया गया है।
- सूचना प्रौद्योगिकी सेवाओं की आउटसोर्सिंग के संबंध में 10 अप्रैल, 2023 के मास्टर निदेश के माध्यम से सूचना प्रौद्योगिकी (आईटी) सेवाओं की आउटसोर्सिंग से संबंधित जोखिमों के प्रबंधन, संकेन्द्रण जोखिम के प्रबंधन, समूह या समूह के भीतर आउटसोर्सिंग तथा क्लाउड कंप्यूटिंग सेवाओं के उपयोग संबंधी विशिष्ट आवश्यकताओं के लिए एक ढांचा प्रदान किया गया है।

- सूचना प्रौद्योगिकी अभिशासन, जोखिम, नियंत्रण और आश्वासन पद्धतियों के संबंध में 7 नवंबर, 2023 के मास्टर निदेश के माध्यम से बैंकों के भीतर आईटी अभिशासन, जोखिम प्रबंधन और आश्वासन पद्धतियों को बेहतर बनाने पर जोर दिया गया है।

(ग) और (घ): डिजिटलीकरण और डिजिटल लेनदेन के दायरे के बढ़ने के कारण, समय के साथ बैंकों के लिए साइबर खतरों का जोखिम भी बढ़ गया है। बैंकों की साइबर सुरक्षा स्थिति को सुदृढ बनाने के लिए, आरबीआई ने संभावित कमियों को दूर करने और धोखाधड़ी, आंकडों की चोरी और अन्य दुर्भावनापूर्ण गतिविधियों को रोकने के लिए विभिन्न दिशानिर्देश/सलाह जारी की हैं। इसके अलावा, भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सीईआरटी-इन) नवीनतम साइबर खतरों के संबंध में चेतावनी और परामर्शिका जारी करता है और डिजिटल प्रौद्योगिकियों के सुरक्षित उपयोग को सुनिश्चित करने के लिए नियमित आधार पर जवाबी उपाय सुझाता है। इसके अलावा, बैंक सीईआरटी-इन के माध्यम से सूचीबद्ध लेखापरीक्षकों द्वारा समय-समय पर आईटी और प्रणाली लेखापरीक्षा भी करते हैं।

(ड.): विनियामकीय ढांचे के अनुसार, बैंकों को सभी असामान्य साइबर घटनाओं की सूचना ऐसी घटनाओं के घटित होने के दो से छह घंटे के भीतर आरबीआई को देना अनिवार्य है। आरबीआई की साइबर सुरक्षा और आईटी जांच (सीएसआईटीई) टीम द्वारा साइबर सुरक्षा संबंधी दिशा-निर्देशों के कार्यान्वयन का मूल्यांकन समय-समय पर स्थल पर (ऑनसाइट) और स्थलेत्तर (ऑफसाइट) निरीक्षणों के माध्यम से किया जाता है। ऐसे निरीक्षणों के दौरान पाई गई कमियों, यदि कोई हों, को दूर करने के लिए बैंकों को अधिदेश दिया गया है। इसके अलावा, आरबीआई द्वारा जारी ऐसे निर्देशों का पालन न करने पर बैंकों के खिलाफ़ प्रवर्तन की कार्रवाई आरम्भ की जाती है।

*****