

भारत निर्वाचन आयोग

निर्वाचन सदन, अशोका रोड, नई दिल्ली-110001

न. 491/मीडिया-एफ.ए.क्यू./2017

दिनांक: 14 अप्रैल 2017

ईवीएम की सुरक्षा विशेषताओं के बारे में बार बार पूछे जाने वाले प्रश्न

पिछले दिनों भारतीय निर्वाचन आयोग की इलेक्ट्रॉनिक वोटिंग मशीनों को लेकर आमजनों के मस्तिष्क में कुछ सवाल उठे हैं। निर्वाचन आयोग बार-बार कहता रहा है कि ईसीआई-ईवीएम और उनसे संबंधित प्रणालियां सुदृढ़, सुरक्षित और छेड़खानी-मुक्त हैं।

निम्नांकित बार बार पूछे जाने वाले प्रश्नों (एफएक्यूज़) के उत्तरों के जरिए ईवीएम की अद्यतन प्रौद्योगिकी संबंधी विशेषताओं सहित सुरक्षा विशेषताओं की विस्तृत जानकारी दी गई है। इनमें यह भी बताया गया है कि इन मशीनों के विनिर्माण से लेकर भंडारण तक इनके इस्तेमाल के प्रत्येक चरण में कड़े प्रशासनिक उपाय किए जाते हैं।

1. ईवीएम के साथ छेड़खानी करने का क्या अर्थ है ?

टैम्परिंग या छेड़खानी का अर्थ है, कंट्रोल यूनिट (सीयू) की मौजूदा माइक्रो चिप्स पर लिखित साफ्टवेयर प्रोग्राम में बदलाव करना या सीयू में नई माइक्रो चिप्स इंsert करके दुर्भावनापूर्ण साफ्टवेयर प्रोग्राम शुरू करना और बैलेट यूनिट में प्रेस की जाने वाली ऐसी 'कीज़' बनाना, जो कंट्रोल यूनिट में वफादारी के साथ परिणाम दर्ज न करती हो।

2. क्या ईसीआई-ईवीएम को हैक किया जा सकता है?

नहीं।

ईवीएम मशीनों के एम 1 (माडल 1) का विनिर्माण 2006 तक पूरा कर लिया गया था और कुछ कार्यकर्ताओं द्वारा किए जा रहे दावों के विपरीत एम 1 मशीनों की सभी अनिवार्य तकनीकी विशेषताओं को ऐसा बनाया गया था, कि उन्हें हैक न किया जा सके।

2006 में तकनीकी मूल्यांकन समिति की सिफारिशों के आधार पर 2006 के बाद और 2012 तक विनिर्मित ईवीएम के एम 2 माडल में अतिरिक्त सुरक्षा विशेषता के रूप में एन्क्रिप्टेड फार्म यानी कूट रूप में प्रमुख कोड्स की डायनामिक कोडिंग शामिल की गई, जिसके फलस्वरूप बैलेट यूनिट से कंट्रोल यूनिट में की-प्रेस संदेश हस्तांतरित करना संभव हुआ। इसमें प्रत्येक की-प्रेस की रीयल टाइम

सेटिंग भी शामिल है, ताकि तथाकथित दुर्भावनापूर्ण सीक्वेंस की गई की-प्रेस सहित की-प्रेस की सीक्वेंसिंग का पता लगाया जा सके और रैण्ड किया जा सके।

इसके अतिरिक्त ईसीआई-ईवीएम कम्प्यूटर नियंत्रित नहीं है, वे स्टैंड अलोन यानी स्वतंत्र मशीनें हैं और वे इंटरनेट और/या किसी अन्य नेटवर्क के साथ किसी भी समय बिंदु पर कनेक्टिड नहीं हैं। अतः किसी रिमोट डिवाइस के जरिए उन्हें हैक करने की कोई गुंजाइश नहीं है।

ईसीआई-ईवीएम में वायरलेस या किसी बाहरी हार्डवेयर पोर्ट के लिए किसी अन्य गैर-ईवीएम एक्सेसरी के साथ कनेक्शन के जरिए कोई फ्रीक्वेंसी रिसीवर या डेटा के लिए डीकार्डर नहीं है। अतः हार्डवेयर पोर्ट या वायरलेस या वाईफाई या ब्लूटूथ डिवाइस के जरिए किसी प्रकार की टैम्परिंग या छेड़छाड़ संभव नहीं है, क्योंकि कंट्रोल यूनिट (सीयू) बैलेट यूनिट (बीयू) से केवल एन्क्रिप्टिड या डाइनामिकली कोडिड डेटा ही स्वीकार करती है। सीयू द्वारा किसी अन्य प्रकार का डेटा स्वीकार नहीं किया जा सकता।

3. क्या विनिर्माताओं द्वारा ईसीआई-ईवीएम में कोई हेराफेरी (मैनीपुलेशन) की जा सकती है?

संभव नहीं है।

साफ्टवेयर की सुरक्षा के बारे में विनिर्माता के स्तर पर कड़ा सुरक्षा प्रोटोकॉल लागू किया गया है। ये मशीनें 2006 से अलग अलग वर्षों में विनिर्मित की जा रही हैं। विनिर्माण के बाद ईवीएम को राज्य और किसी राज्य के भीतर जिले से जिले में भेजा जाता है। विनिर्माता इस स्थिति में नहीं हो सकते कि वे कई वर्ष पहले यह जान सकें कि कौन सा उम्मीदवार किस निर्वाचन क्षेत्र से चुनाव लड़ेगा और बैलेट यूनिट में उम्मीदवारों की सीक्वेंस क्या होगी। इतना ही नहीं, प्रत्येक ईसीआई-ईवीएम का एक सीरियल नम्बर है और निर्वाचन आयोग ईवीएम-ट्रैकिंग सॉफ्टवेयर का इस्तेमाल करके अपने डेटा बेस से यह पता लगा सकता है कि कौन सी मशीन कहाँ पर है। अतः विनिर्माण के स्तर पर हेराफेरी की कोई गुंजाइश नहीं है।

4. क्या सीयू में चिप के भीतर ट्रोजन होर्स को घुसाया जा सकता है?

ईवीएम में वोटिंग की सीक्वेंस निम्नांकित अनुसार ट्रोजन होर्स के इंजेक्शन की आशंका को समाप्त करती है। निर्वाचन आयोग द्वारा किए गए कड़े सुरक्षा उपाय फील्ड में ट्रोजन होर्स का प्रवेश असंभव बना देते हैं।

जब कंट्रोल यूनिट में कोई बैलेट की प्रेस की जाती है, तो सीयू, बीयू को वोट रजिस्टर करने की अनुमति देती है और बीयू में की-प्रेस होने का इंतजार करती है। इस अवधि के दौरान सीयू में सभी कीज़ उस वोट के कास्ट होने की समूची सीक्वेंस पूरा होने तक निष्क्रिय हो जाती हैं। किसी मतदाता द्वारा कीज़ (उम्मीदवारों के वोट बटन) में से कोई एक की दबाने के बाद बीयू उस की से

संबंधित जानकारी सीयू को ट्रांसफर करती है। सीयू को डेटा प्राप्त होता है और वह तत्क्षण बीयू में एलईडी लैंप की चमक के साथ उसकी प्राप्ति स्वीकार करती है। सीयू में बैलेट कोसक्षम करने के बाद केवल 'प्रथम प्रेस की गई की' को सीयू द्वारा सेंस और स्वीकार किया जाता है। इसके बाद, भले ही कोई मतदाता अन्य बटनों को दबाता रहे, उसका कोई असर नहीं होता, क्योंकि बाद में दबाए गए बटनों के परिणामस्वरूप सीयू और बीयू के बीच कोई कम्युनिकेशन नहीं होता है और न ही बीयू किसी की-प्रेस को रजिस्टर करती है। इसे दूसरे शब्दों में इस प्रकार कहा जा सकता है कि सीयू का इस्तेमाल करके सक्षम किए गए प्रत्येक बैलेट के लिए केवल एक वैध की-प्रेस (प्रथम की-प्रेस) होता है। एक बार वैध की प्रेस होने (वोटिंग प्रक्रिया पूरी होने) पर सीयू और बीयू के बीच कोई गतिविधि तब तक नहीं होती, जब तक कि सीयू द्वारा अन्य बैलेट सक्षम बनाने वाली की प्रेस की व्यवस्था नहीं कर दी जाती। अतः देश में इस्तेमाल की जा रही इलेक्ट्रॉनिक वोटिंग मशीनों में तथाकथित 'सीक्वेंस्ड की प्रेसिज़' यानी 'सिलसिलेवार बटन दबाने' के जरिए दुर्भावनापूर्ण संकेत भेजना संभव नहीं है।

5. क्या ईसीआई-ईवीएम का पुराना मॉडल अभी भीचलन में है?

ईवीएम मशीनों का एम 1 माडल 2006 में बनाया गया था और पिछली बार 2014 के आम चुनावों में इस्तेमाल किया गया था। 2014 में जिन ईवीएम मशीनों ने 15 वर्ष का जीवनकाल पूरा कर लिया था और एम 1 माडल की ऐसी मशीनें, जो वीवीपीएटी (वोटर-वेरिफाइड पेपर आडिट ट्रेल) के अनुकूल नहीं थीं, को देखते हुए निर्वाचन आयोग ने 2006 तक विनिर्मित सभी एम 1 ईवीएम को हटाने का फैसला किया। ईवीएम मशीनों को हटाने के लिए निर्वाचन आयोग ने एक मानक प्रचालन प्रक्रिया (एसओपी) निर्धारित की है। ईवीएम और उसके चिप को नष्ट करने की प्रक्रिया को विनिर्माताओं की फैक्टरी के भीतर राज्य मुख्य निर्वाचन अधिकारी या उसके प्रतिनिधि की मौजूदगी में अंजाम दिया जाता है।

6. क्या ईसीआई-ईवीएम के साथ भौतिक रूप से छेड़छाड़ की जा सकती है या बिना किसी के ध्यान में आए उनके संघटकों को बदला जा सकता है?

ईसीआई-ईवीएम के पुराने मॉडलों एम1 एवं एम2 में विद्यमान सुरक्षा विशेषताओं के अतिरिक्त 2013 के बाद बनाई गई नई एम3 ईवीएम में टेम्पर डिटेक्शन एवं सेल्फ डाइग्नोस्टिक्स जैसी अतिरिक्त विशेषताएं हैं। टेम्पर डिटेक्शन विशेषता के कारण जैसे ही कोई व्यक्ति मशीन खोलने का प्रयास करता है, ईवीएम निष्क्रिय हो जाता है। सेल्फ डाइग्नोस्टिक्स विशेषता के कारण जब भी ईवीएम मशीन को स्विच ऑन किया जाता है, यह पूरी तरह मशीन की जांच करता है। इसके हार्डवेयर या सॉफ्टवेयर में किसी भी परिवर्तन का इससे पता लग जाएगा।

उपरोक्त विशेषताओं के साथ नये मॉडल एम3 का एक प्रोटोटाइप जल्द ही तैयार हो जाएगा। एक तकनीकी विशेषज्ञ समिति इसकी जांच करेगी और फिर निर्माण आरंभ हो जाएगा। उपरोक्त अतिरिक्त विशेषताओं एवं नई प्रौद्योगिकीय उन्नतियों के साथ एम3 ईवीएम की खरीद के लिए सरकार द्वारा लगभग 2000 करोड़ रुपये जारी किए गए हैं।

7. इसीआई-ईवीएम को छेड़खानी मुक्त बनाने के लिए नवीनतम प्रौद्योगिकीय विशेषताएं क्या हैं?

ईसीआई-ईवीएम मशीन को 100 प्रतिशत छेड़खानी मुक्त बनाने के लिए कई अन्य कदमों के अलावा वन टाइम प्रोग्रामेबल (ओटीपी) माइक्रोकंट्रोलर्स, की कोड्स की गतिशील कोडिंग, प्रत्येक की प्रेस की तिथि एवं समय की स्टाम्पिंग, उन्नत इनक्रिप्शन प्रौद्योगिकी एवं ईवीएम लॉजिस्टिक्स के संचालन के लिए ईवीएम ट्रेकिंग सॉफ्टवेयर जैसी सर्वाधिक परिष्कृत प्रौद्योगिकीय विशेषताओं का उपयोग करती है। इसके अतिरिक्त, नये मॉडल एम3 ईवीएम में टेम्पर डिटेक्शन एवं सेल्फ डाइग्नोस्टिक्स जैसी अतिरिक्त विशेषताएं भी हैं। चूंकि, सॉफ्टवेयर ओटीपी पर आधारित है, प्रोग्राम को न तो बदला जा सकता है, न ही इसे रि-राइट या रि-रेड ही किया जा सकता है। इस प्रकार यह ईवीएम को छेड़खानी मुक्त बना देता है। अगर कोई इसकी कोशिश करता भी है तो मशीन निष्क्रिय बन जाएगी।

8. क्या इसीआई-ईवीएम विदेशी प्रौद्योगिकी का उपयोग करते हैं?

इस प्रकार की गलत सूचना एवं जैसा कि कुछ लोग आरोप लगाते हैं, के विपरीत भारत विदेशों में बने किसी ईवीएम का उपयोग नहीं करता। ईवीएम का निर्माण स्वदेशी तरीके से सार्वजनिक क्षेत्र की दो कंपनियों यथा-भारत इलेक्ट्रॉनिक्स लिमिटेड, बेंगलुरु एवं इलेक्ट्रॉनिक्स कारपोरेशन ऑफ इंडिया लिमिटेड, हैदराबाद द्वारा किया जाता है। सॉफ्टवेयर प्रोग्राम कोड इन दोनों कंपनियों द्वारा आंतरिक तरीके से तैयार किया जाता है न कि उन्हें आउटसोर्स किया जाता है। ये सुरक्षा के सर्वोच्च मानकों का अनुपालन करने और उन्हें बनाए रखने के लिए फैक्ट्री स्तर पर सुरक्षा प्रक्रियाओं के विषय होते हैं। प्रोग्राम को **मशीन कोड** में रूपांतरित किया जाता है और उसके बाद ही विदेशों के चिप मैन्युफैक्चर को दिया जाता है, क्योंकि हमारे पास देश के भीतर सेमीकंडक्टर माइक्रोचिप निर्माण करने की क्षमता नहीं है।

प्रत्येक माइक्रोचिप के पास मेमोरी में सन्निहित एक पहचान संख्या होती है और उन पर निर्माताओं के डिजिटल हस्ताक्षर होते हैं। इसलिए, उनके विस्थापन का कोई प्रश्न ही नहीं उठता क्योंकि माइक्रोचिप्स सॉफ्टवेयर से संबंधित क्रियात्मक परीक्षणों के विषय होते हैं। माइक्रोचिप को विस्थापित करने की किसी भी कोशिश का पता लगाया जा सकता है और ईवीएम को निष्क्रिय

बनाया जा सकता है। इस प्रकार, वर्तमान प्रोग्राम को परिवर्तित करने एवं नया प्रोग्राम लागू करने, दोनों का ही पता लगाया जा सकता है जिसके बाद ईवीएम को निष्क्रिय बनाया जा सकता है।

9. भंडारणके स्थान पर हेरफेर किए जाने की कितनी आशंका हैं?

जिला मुख्यालय में ईवीएम को उपयुक्त सुरक्षा के तहत एक दोहरे ताले वाली प्रणाली में रखा जाता है। उनकी सुरक्षा की समय-समय पर जांच की जाती है। अधिकारी स्ट्रॉंग रूम को नहीं खोलते हैं, लेकिन वे इसकी जांच करते हैं कि ये पूरी तरह सुरक्षित है या नहीं और क्या ताला समुचित अवस्था में है या नहीं। किसी भी अनधिकृत व्यक्ति को किसी भी स्थिति में ईवीएम के पास जाने की अनुमति नहीं होती। जब चुनाव का समय नहीं होता है, इस अवधि के दौरान, सभी ईवीएम का वार्षिक भौतिक सत्यापन डीईओ द्वारा किया जाता है और ईसीआई को रिपोर्ट भेजी जाती है। निरीक्षण एवं जांच का कार्य अभी हाल ही में संपन्न किया गया है।

10. स्थानीय निकाय चुनावों में ईवीएम के साथ छेड़छाड़ करने के आरोप किस हद तक सही हैं?

न्यायाधिकार क्षेत्र के बारे में जानकारी के अभाव के कारण इस संबंध में गलतफहमी है। नगरपालिका निकायों या पंचायत चुनावों जैसे ग्रामीण निकायों के चुनावों के मामले में उपयोग में लाए गए ईवीएम भारत के चुनाव आयोग के नहीं होते। स्थानीय निकाय चुनावों से ऊपर के चुनाव राज्य चुनाव आयोग (एसईसी) के अधिकार क्षेत्र के तहत आते हैं, जो अपनी खुद की मशीनें खरीदते हैं और उनकी अपनी संचालन प्रणाली होती है। भारत का चुनाव आयोग उपरोक्त चुनावों में एसईसी द्वारा उपयोग में लाए गए ईवीएम के कामकाज के लिए जिम्मेदार नहीं है।

11. ईसीआई-ईवीएम के साथ छेड़छाड़ न हो सके, यह सुनिश्चित करने के लिए सतत जांच एवं निगरानी के विभिन्न स्तर कौन से हैं?

- **प्रथम स्तर जांच ईसीआईएल के इंजीनियर प्रत्येक ईवीएम की तकनीकी एवं भौतिक /बीईएल :** जांच के बाद संघटकों की मौलिकता को प्रमाणित करते हैं, जो कि राजनीतिक दलों के प्रतिनिधियों के समक्ष किया जाता है। त्रुटिपूर्ण ईवीएम को वापस फैक्ट्री में भेज दिया जाता है। एफएलसी हॉल को साफसुथरा बनाया जाता है-, प्रवेश को प्रबंधित किया जाता है एवं अंदर किसी भी कैमरा, मोबाइल फोन या स्पाई पेन लाने की अनुमति नहीं दी जाती है। राजनीतिक दलों के प्रतिनिधियों के द्वारा औचक रूप से चुने गए 1000 प्रतिशत ईवीएम पर न्यूनतम 5 मतों का एक कृत्रिम मतदान किया जाता है और उनके सामने इसका परिणाम प्रदर्शित किया जाता है। पूरी प्रक्रिया की वीडियोग्राफी की जाती है।
- **यादछिक्कीकरण (रैंडोमाइजेशन) :** किसी विधानसभा और बाद में किसी मतदान केंद्र को आवंटित किए जाने के समय ईवीएम की दो बार बेतरतीब तरीके से (यादछिक्क) जांच की जाती

है जिससे किसी निर्धारित आवंटन की संभावना खत्म हो जाए। मतदान प्रारंभ होने से पहले, चुनाव वाले दिन उम्मीदवारों के मतदान एजेंटों के समक्ष मतदान केंद्रों पर कृत्रिम मतदान का संचालन किया जाता है। मतदान के बाद ईवीएम को सील किया जाता है और मतदान एजेंट सील पर अपने हस्ताक्षर करते हैं। मतदान एजेंट परिवहन के दौरान स्ट्रॉग रूम तक जा सकते हैं।

- **स्ट्रॉग रूम :** उम्मीदवार या उनके प्रतिनिधि स्ट्रॉग रूम पर अपने खुद के सील लगा सकते हैं, जहां मतदान के बाद मतदान किए हुए ईवीएम का भंडारण किया जाता है और वे स्ट्रॉग रूम के सामने शिविर भी लगा सकते हैं। इन स्ट्रॉग रूम की सुरक्षा 24 घंटे बहुस्तरीय तरीके से की जाती है।
- **मतगणना केंद्र :** मतदान किए हुए ईवीएम को मतगणना केंद्रों पर लाया जाता है और मतगणना आरंभ होने से पहले उम्मीदवारों के प्रतिनिधियों के समक्ष सीलों और सीयू की विशिष्ट पहचान प्रदर्शित की जाती है।

12. क्या हेरफेर किए गए किसी ईवीएम को बिना किसी की जानकारी के मतदान प्रक्रिया में पुनः शामिल किया जा सकता है?

इसका प्रश्न ही नहीं उठता।

ईसीआई द्वारा ईवीएम को छेड़छाड़ मुक्त बनाने के लिए उठाए गए सतत जांच एवं निगरानी के ठोस कदमों की उपरोक्त श्रृंखला को देखते हुए, यह स्पष्ट है कि न तो मशीनों के साथ छेड़छाड़ की जा सकती है और न ही त्रुटिपूर्ण मशीनों को किसी भी समय मतदान प्रक्रिया में फिर से शामिल ही किया जा सकता है क्योंकि गैर ईसीआई-ईवीएम का उपरोक्त प्रक्रिया और बीयू एवं सीयू से बेमेल होने के कारण उनका पता लगा लिया जाएगा। कड़ी जांचों एवं परीक्षणों के विभिन्न स्तरों के कारण न तो ईसीआई-ईवीएम ईसीआई प्रणाली को छोड़ सकता है और न ही कोई बाहरी मशीन (गैर-ईसीआई-ईवीएम) को इस प्रणाली में शामिल किया जा सकता है।

13. अमेरिका एवं यूरोपीय संघ जैसे विकसित देशों ने ईवीएम को क्यों नहीं अपनाया है और कुछ देशों ने यह प्रणाली क्यों त्याग दी है?

कुछ देशों ने अतीत में इलेक्ट्रॉनिक मतदान के साथ प्रयोग किया है। इन देशों में मशीनों के साथ समस्या यह थी कि वे कंप्यूटर द्वारा नियंत्रित थे एवं नेटवर्क से जुड़े थे, जिसके कारण उनमें हैकिंग किए जाने की आशंका थी जिससे इसका उद्देश्य पूरा नहीं हो पाता था। इसके अतिरिक्त, उनकी सुरक्षा, हिफाजत एवं संरक्षण से संबंधित कानूनों एवं विनियमनों में पर्याप्त सुरक्षा के उपायों की कमी थी। कुछ देशों में अदालतों ने केवल इन्हीं कानूनी आधारों की वजह से ईवीएम के उपयोग को स्थगित कर दिया।

भारतीय ईवीएम एक स्वतंत्र प्रणाली है जबकि अमेरिका, नीदरलैंड, आयरलैंड एवं जर्मनी के पास प्रत्यक्ष रिकार्डिंग मशीने थीं। भारत ने हालांकि आंशिक रूप से ही सही, कागज लेखा परीक्षा निशान (पेपर ऑडिट ट्रेल) लागू किया है। दूसरे देशों के पास लेखा परीक्षण निशान नहीं थे। उपरोक्त सभी देशों में मतदान के दौरान सोर्स कोड को बंद कर दिया जाता है। भारत के पास भी मेमोरी से जुड़े क्लोज्ड सोर्स और ओटीपी है।

दूसरी तरफ, ईसीआई-ईवीएम स्वतंत्र उपकरण है, जो किसी भी नेटवर्क से नहीं जुड़े हैं और इसलिए भारत में व्यक्तिगत रूप से किसी के लिए भी 1.4 मिलियन मशीनों के साथ छेड़छाड़ करना असंभव है। मतदान के दौरान देश में पहले होने वाली चुनावी हिंसा एवं फर्जी मतदान, बूथ कैप्चरिंग आदि जैसी अन्य चुनाव संबंधी गलत प्रचलनों को देखते हुए ईवीएम भारत के लिए सर्वाधिक अनुकूल हैं।

उल्लेखनीय है कि जर्मनी, आयरलैंड एवं नीदरलैंड जैसे देशों के विपरीत भारतीय कानूनों एवं ईसीआई विनियमनों में ईवीएम की सुरक्षा एवं हिफाजत के लिए पर्याप्त अंतर्निहित सुरक्षोपाय हैं। इसके अतिरिक्त, सुरक्षित प्रौद्योगिकीय विशेषताओं के कारण भारतीय ईवीएम बहुत उत्कृष्ट श्रेणी के हैं। भारतीय ईवीएम इस वजह से भी विशिष्ट हैं क्योंकि मतदाताओं के लिए पूरी प्रक्रिया को पारदर्शी बनाने के लिए चरणबद्ध तरीके से ईवीएम में वीवीपीएटी का भी उपयोग होने जा रहा है।

नीदरलैंड के मामले में, मशीनों के भंडारण, परिवहन एवं सुरक्षा को लेकर नियमों का अभाव था। नीदरलैंड में बनी मशीनों का उपयोग आयरलैंड एवं जर्मनी में भी किया जाता था। 2005 के एक फैसले में जर्मनी के न्यायालय ने चुनाव की सार्वजनिक प्रकृति एवं मूलभूत कानून के विशेषाधिकार के उल्लंघन के आधार पर मतदान उपकरण अध्यादेश को असंवैधानिक पाया। इसलिए इन देशों ने नीदरलैंड में बनी मशीनों के उपयोग को बंद कर दिया। आज भी अमेरिका समेत कई देश मतदान के लिए मशीनों का उपयोग कर रहे हैं।

ईसीआई-ईवीएम बुनियादी रूप से मतदान मशीनों एवं विदेशों में अपनाई गई प्रक्रियाओं से अलग है। किसी अन्य देश की कंप्यूटर नियंत्रित, ऑपरेटिंग सिस्टम आधारित मशीनों के साथ कोई भी तुलना गलत होगी और उसकी समानता ईसीआई-ईवीएम के साथ नहीं की जा सकती।

14. वीवीपीएटी सक्षम मशीनों की क्या स्थिति है?

ईसीआई ने मतदाता सत्यापित कागज लेखा परीक्षा निशान (वीवीपीएटी) का उपयोग करते हुए 107 विधानसभा क्षेत्रों एवं 9 लोकसभा चुनाव क्षेत्रों में चुनावों का संचालन किया है। वीवीपीएटी के साथ-

साथ एम2 एवं नई पीढ़ी एम3 ईवीएम का उपयोग मतदाताओं के भरोसे एवं पारदर्शिता को बढ़ाने की दिशा में एक सकारात्मक योजना है।

ELECTION COMMISSION OF INDIA

Nirvachan Sadan, Ashoka Road, New Delhi-110001

No. 491/Media-FAQ/2017

Dated: 14th April, 2017

FAQs ON SECURITY FEATURES OF THE ECI-EVMs

In the recent past, there have been some queries in the minds of common people about the security features of Electronic Voting Machines (EVMs) of Election Commission of India (ECI). The Election Commission has, *time and again*, stated that ECI-EVMs and its systems are robust, secure and tamper-proof.

The following FAQs give a detailed view of security features including latest technological features of EVMs and stringent administrative measures taken at every step of its usage from manufacturing to storage.

1. What is meant by Tampering of EVM?

Tampering means alteration in the software program written either on existing microchips of Control Unit (CU) or introducing malicious software program by inserting new microchips in CU and also making keys - pressed in Ballot Unit (BU) not record faithfully in the Control Unit.

2. Are the ECI- EVMs hackable?

No.

M1 (model one) of EVM machines were manufactured till 2006 and had all necessary technical features making M1 non-hackable contrary to claims made by some activists.

On the recommendations of the Technical Evaluation Committee in 2006, M2 model of EVMs produced after 2006 and upto 2012 incorporated dynamic coding of key codes thereby enabling transfer of the key - press message from Ballot Unit (BUs) to Control Unit (CUs), in an encrypted form as an additional security feature. It also contains Real time setting of each key press so that

sequencing of key presses including so called malicious sequenced key presses can be detected and wrapped.

Further, the **ECI- EVMs are not computer controlled, are stand alone machines and not connected to the internet and /or** any other network at any point of time. Hence, there is no chance of hacking by remote devices.

The ECI-EVMs do not have any frequency receiver or decoder for data for wireless or any external hardware port for connection to any other **non-EVM** accessory or device. Hence no tampering is possible either through hardware port or through **Wireless, Wi-Fi or Bluetooth device** because CU accepts only encrypted and dynamically coded data from BU. No other kind of data can be accepted by CU.

3. Can ECI-EVMs be manipulated by Manufacturers?

Not Possible.

There is very stringent security protocol at manufacturer level regarding security of software. The Machines have been manufactured in different years starting from 2006. After manufacturing, EVMs are sent to State and district to district within a State. ***The manufacturers are in no position to know several years ahead which candidate will be contesting from a particular constituency and what will be the sequence of the candidates on the BU.*** Also, each ECI-EVM has a serial number and the Election Commission by use of EVM –tracking software can find out from its database which machine is located where. So, any manipulation at manufacturing stage is ruled out.

4. Can Trojan Horse be incorporated into the chip in CU?

Sequence of voting in EVM eliminates the possibility of injection of Trojan Horse as mentioned below. The stringent security measures by ECI make it impossible to introduce Trojan Horse in the field.

Once a ballot key is pressed in CU, the CU enables BU for registering the vote and waits for the key pressing in the BU. During this period, all keys in the CU become Inactive till the entire sequence of casting of that vote is complete. Once any of the keys (candidates vote button) is pressed by a voter in BU, the BU transmits the key information to CU. The CU gets the data and acknowledges it by glowing the corresponding LED lamps in BU. After the enabling of ballot in CU, only the 'first key press' is sensed and accepted by CU. After this, even if a voter keeps on pressing the other buttons that is of no use as there will not be any communication between CU and BU as the result of those subsequent key presses, nor will BU register any key press. To put it in other words, there can be only one valid key press (the first key press) for every ballot enabled using CU. Once a valid key press (voting process)

is complete, until another ballot enabling key press is made there will not be any activity between the CU and the BU. Hence, sending of any malicious signal, by way of so called 'sequenced key presses', is impossible in the Electronic Voting Machines being used in the country.

5. Are Old model ECI- EVMs still in use?

M1 model of EVM machines were produced up to 2006 and were last used in 2014 General Elections. In 2014, EVM machines which completed 15 years of economic life and also because M1 were not compatible with VVPAT (voter-verified paper audit trail) , ECI decided to discontinue use of all M1 EVMs manufactured upto 2006. There is a Standard Operating Procedure laid down by ECI to discard EVMs. The process of destruction of EVM & its chip is carried out in the presence of Chief Electoral Officer of the state or his representatives inside the factory of manufacturers.

6. Can ECI-EVMs be Physically Tampered with/ their components be changed without anyone noticing?

In addition to the existing security features in earlier models M1 & M2 of ECI-EVMs, the new **M3** EVM produced after 2013 have additional features like **Tamper Detection** and **Self Diagnostics**. The tamper detection feature makes an EVM inoperative the moment anyone tries to open the machine. The **Self diagnostic** feature checks the EVM fully every time it is switched on. Any change in its hardware or software will be detected.

A prototype of a new model M3 with above features is going to be ready shortly. A Technical Experts Committee will examine it and then production will commence. About Rs. 2,000 crores have been released by the Government to procure M3 EVMs with above additional features and new technological advancements.

7. What are the latest technological features to make ECI-EVMs tamper proof?

The ECI-EVMs use some of the most sophisticated technological features like **one time programmable (OTP) microcontrollers, dynamic coding of key codes, date and time stamping of each and every key press, advanced encryption technology and EVM-tracking software to handle EVM logistics, among others to make the machine 100% tamper proof**. In addition to these, new model M3 EVMs also have tamper detection and self-diagnostics as added features. Since, software is based on OTP the program cannot be altered, re-written or Re-read. Thus, making EVM tamper proof. If anyone make, attempt, the machine will become in operative.

8. Do the ECI-EVMs use foreign technology?

Contrary to misinformation and as alleged by some, India do not use any EVMs produced abroad. EVMs are produced indigenously by 2 PSUs viz. Bharat Electronics Ltd., Bengaluru and Electronics Corporation of India Ltd., Hyderabad. The Software Programme Code is written in-house, by these two companies, not outsourced, and subjected to security procedures at factory level to maintain the highest levels of integrity. The programme is converted into **machine code** and only then given to the chip manufacturer abroad because we don't have the capability of producing semi-conductor microchips within the country.

Every microchip has an identification number embedded into memory and the producers have their digital signatures on them. So, the question of their replacement does not arise at all because microchips are subjected to functional tests with regard to the software. Any attempt to replace microchip is detectable and can make EVM in-operative. Thus, both changing existing programme or introducing new one are detectable making EVM in-operative.

9. What are the possibilities of manipulation at the place of storage?

At the district headquarters, EVMs are kept in a **double-lock system under appropriate security. Their safety is periodically checked.** The officers do not open the strong room, but they check whether it's fully protected and whether the lock is in proper condition or not. **No Unauthorized person can get access to the EVMs at any point of time.** During non election period, Annual Physical Verification of all EVMs is done by DEOs and report sent to ECI. Inspection & checking have recently been completed.

10. To what extent are allegations of EVM tampering in local body polls true?

There is a misunderstanding in this regard due to lack of knowledge about jurisdiction. In case of elections to Municipal bodies or Rural bodies like Panchayat Elections, the EVMs used do not belong to the Election Commission of India. Above local bodies elections come under the jurisdiction of State Election Commission/s (SECs), which procure their own machines and have their own handling system. **ECI is not responsible for functioning of EVMs used by SECs in above elections.**

11. What are the different levels of checks and balances ensuring tamper proofing of ECI-EVMs?

- **First Level Checking:** BEL/ECIL engineers certify originality of components after technical and physical examination of each EVM, undertaken in front of representatives of political parties. Defective EVMs are sent back to factory.

The FLC Hall is sanitized, entry is restricted and no camera, mobile phone or spy pen is allowed inside. Mock poll of at least 1000 votes is conducted on 5% EVMs selected randomly by reps of political parties and the result shown to them. The entire process is video graphed.

- **Randomization:** EVMs are randomized twice while being allocated to an Assembly and then to a polling booth ruling out any fixed allocation. Mock Poll at polling station is conducted in front of polling agents of candidates on the poll day, before polls begin.

After Poll, EVMs are sealed and polling agents put their signature on the seal. Polling agents can travel upto strong room during transportations.

- **Strong Rooms:** Candidates or their representatives can put their own seals on the strong rooms where polled EVMs are stored after the poll and also camp in front of strong room. These strong rooms are guarded 24x7 in multilayers.
- **Counting Centres:** The polled EVMs are brought to the Counting Centres and Unique IDs of the seals and CU are shown to reps of candidates before start of counting.

12. Can a manipulated ECI- EVM be re-inducted in the polling process without anyone coming to know?

Question does not arise.

Looking at the above series of fool-proof checks and balances that are undertaken by the ECI to make EVMs tamper proof, it is evident that neither the machines can be tampered-with nor defective machines can get re-inducted into the polling process at any point of time because Non ECI -EVMs will get detected by the above process and mismatch of BU & CU. Due to different level of stringent checks and balances neither ECI-EVMs can leave the ECI system nor any outside machine (Non-ECI -EVM) can be inducted into the system.

13. Why have Developed Nations like the US and European Union not adopted EVMs and some have discontinued?

Some countries have experimented with electronic voting in the past. The problem faced with the machines in these countries was that they were computer controlled and **connected to the network, which in turn, made them prone to hacking** and hence totally defeating the purpose. Moreover, there were not adequate security measures and safeguards in their corresponding laws regulations for security, safety and protection. In some countries, Courts struck down the use of EVMs on these legal grounds only.

Indian EVM is stand-alone *whereas*, USA, The Netherlands, Ireland & Germany had direct recording machines. India has introduced paper audit trail, though partly. Others did not have audit trail. Source code is closed during polling in all of the above countries. India also has closed source burnt into memory and is OTP.

ECI-EVMs, on the other hand, are stand-alone devices not connected to any network, thus making it impossible for anyone to tamper with over 1.4 million machines in India individually. EVMs are most suited for India, looking at the country's past poll violence and other electoral malpractices like rigging, booth capturing etc. during the polls.

It is worth mentioning that in contrast with countries like Germany, Ireland and the Netherlands. Indian Laws & ECI regulations have in-built adequate safeguards for security & safety of EVMs. Besides, Indian EVMs are far superior on account of secured technological features. Indian EVMs also stand apart because VVPATs going to be used with EVMs in phases to make entire process transparent for voters.

In case of The Netherlands, rules regarding storage, transport and security of machine were lacking. Machines produced in The Netherlands were also used in Ireland & Germany. In a judgment in 2005, German Court found voting device ordinance unconstitutional on the ground of violation of the privilege of the public nature of election & the basic law. So, these countries discontinued the use of machines produced in The Netherlands. Even, today many countries including USA are using machines for voting.

ECI -EVMs are fundamentally different from the voting machines and processes adopted in foreign countries. Any comparison based on computer controlled, operating system based machines elsewhere will be erroneous and ECI -EVM cannot be compared with.

14. What is the status of VVPAT enabled machines?

The ECI has conducted elections in 255 assembly constituencies and nine Lok Sabha constituencies using Voters Verified Paper Audit Trail (VVPAT). The use of M2 and new-generation M3 EVMs along with VVPAT is the way forward for further confidence and transparency of the voters.