

## Learn From Diebold's California Decertification

Richard Hunter, Ray Wagner

California's decision to decertify Diebold Election Systems' (DES's) touch-screen voting technologies offers lessons for other governments and vendors.

## NEWS ANALYSIS

---

### Event

On 29 April 2003, the California secretary of state decertified DES's touch-screen voting technology for use in four counties in the state. This decision — which affects 14,000 DES touch-screen terminals, and as many as 2 million eligible voters — reflects the state's concern that DES allegedly deployed systems in four California counties without required federal testing or state certification. The state further alleges that DES lied about the systems' certification status to the state. The secretary of state has asked the state attorney general to investigate the possibility of criminal and civil fraud charges against DES.

### Analysis

If DES knowingly deployed voting systems in the field without required testing and certification, then the state's decision to decertify DES's voting systems is absolutely justified. Whether DES later lied about the matter is irrelevant, except that it could be grounds for criminal prosecution. Field deployment of uncertified software is completely intolerable in an application in which public trust is a mission-critical requirement.

The software industry has historically favored the rapid introduction of new products, which inevitably leads to high levels of flaws. The release-and-patch approach to software quality and security is no longer acceptable even for consumer-level operating systems, let alone mission-critical applications with major public consequences. The public — which now includes 1 billion Internet users worldwide, all of whom are only too familiar with cybercrime — is simply too sensitive to quality and security concerns. In DES's case, a history of serious security breaches — such as the discovery and worldwide distribution of source code found unprotected on an Internet-connected DES server — and highly critical independent reports alleging security flaws in DES's products serve to underline the importance of strict attention to testing and certification requirements. California's refusal to accept any ambiguity regarding the security of DES's machines is appropriate.

### Recommendations:

#### Governments and other agencies evaluating voting and other critical technologies:

- Use government agencies' enormous purchasing power to promote higher software quality, by making provable quality a nonnegotiable condition of all software purchases.
- Legislate multiple independent certification processes for electronic voting systems and software.

#### Software vendors:

- Recognize that industry dynamics are changing fast, with software quality becoming a matter of public interest and concern, and allocate development resources accordingly.

**Analytical Sources:** Richard Hunter and Ray Wagner, Gartner Research

#### Recommended Reading and Related Research

- "Making Government Security Spending Count" — Government bodies can take proactive steps to deliver near-term security benefits. **By Gregg Kreizman and John Pescatore**

- "Online Voting Can't Be Trusted on Standard PCs" — Until trustable computing platforms are standard, secure hardware must be added to PCs used in online voting systems. **By John Pescatore and Christopher Baum**

(You may need to sign in or be a Gartner client to access all of this content.)

## REGIONAL HEADQUARTERS

---

Corporate Headquarters  
56 Top Gallant Road  
Stamford, CT 06902-7700  
U.S.A.  
+1 203 964 0096

European Headquarters  
Tamesis  
The Glanty  
Egham  
Surrey, TW20 9AW  
UNITED KINGDOM  
+44 1784 431611

Asia/Pacific Headquarters  
Level 7, 40 Miller Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

Latin America Headquarters  
Av. das Nações Unidas 12.551  
9 andar—WTC  
04578-903 São Paulo SP  
BRAZIL  
+55 11 3443 1509