Direct Number: (213) 243-2582
ddmcmillan@jonesday.com

JP398519:tlg:20942697.1

February 16, 2004

Marc Carrel, Vice Chair
Voting Systems and Procedures Panel
300 South Spring Street
Los Angeles, CA 90013

Re: DESI PRODUCTS TO BE USED BY COUNTY

Dear Mr. Carrel:

Product	Counties
AccuVote OS ("Optical Scan") Voting System plus GEMS software	Twelve Counties: Fresno, Humbuldt, Lassen, Marin, Menducino, Modoc, Placer, San Luis Obispo, Santa Barbara, Siskiyou, Trinity, and Tulare. (Cmplt. ¶ 34)
AccuVote TS ("Touch Screen") Voting system, AccuVote OS to scan absentee ballots, plus GEMS software.	Two Counties: Alameda County and Tulare County. (Cmplt. ¶ 35)
AccuVote TS x voting system, AccuVote OS to scan absentee ballots, plus GEMS software.	Four Counties: San Diego, San Joaquin, Solano and Kern. (Cmplt. ¶ 36.)
AccuVote TS for early voting (16 terminals) plus GEMS software to tally voters from LA County's proprietary "InKaVote" devices.	One County: LA County. (Cmplt. ¶ 37)

Regards,

Daniel D. McMillan

Encls.

LAI-2094721v1

JP002381:pr
01/29/2004

To: Daniel D. McMillan

DIEBOLD ELECTION SYSTEMS, INC.

Re: VSPP Request for Documents

I. ORGANIZATIONAL STRUCTURE

DESI's organizational structure has recently changed. The current organizational chart is attached to this memorandum. DESI's old organizational structure was comprised of the following nine departments: sales; support; research and development; marketing; administration; finance; legal; human resources; and a catch-all department.

A. Research and Development

The research and development department included product development. The director of product development is Pat Green. DESI has the following four facilities under the product development department: (1) Canton, Ohio; (2) Vancouver, Canada; (3) Sacramento, California (DIMS office); and (4) Washington State (Printed Products). The Canton facility is responsible for electrical engineering and low-level software operating systems and control code (pic chip). The Canton facility reports to Pat Green. The facility in Vancouver, Canada also reports to Pat Green. The Vancouver facility is responsible for the development of software, firmware, applications/programming, thermal wear programming, and is in control of product development. The printed products and DIMS office do not report to Pat Green. The printed products facility is no longer under the research and development department. The printed products facility reports to the president of DESI. The DIMS office in Sacramento is responsible

for voter registration applications and also does not report to Pat Green. The DIMS office is a separate and wholly owned subsidiary of Diebold, and is a sister company to DESI.

B. Services and Support

The services and support department consists of the field and depo areas responsible for hardware service; the service bureau; certification; a repair depo of Diebold that helps prepare hardware (Seville facility handles the maintenance); information security; and project management. The services and support department also has a project management office (PMO office), with both west and east coast management implementation of client software from start to finish. Barney Lucas handles all calls that come in for hardware repair and then he decides where the hardware is to be repaired. He gives return material authorization (RMA). DESI has a documented process of ISO certification. DESI has an internal web site called "livelink" with different levels of access. Livelink is a web-based interactive internal web site.

C. Sales

The sales department has no formal office. The director of the sales department is Barry Herron. The regional manager for the west coast is Frank Kaplan. The sales representatives work primarily out of their homes and correspond with customers directly. The sales people maintain files with original documents. *We will need to look into this issue in more detail.*

D. Marketing

Mark Radsey in Canton, Ohio heads the marketing department. The marketing department has more of a public relations role, but it overlaps with the sales department on demonstrating equipment.

II. SOURCES OF DOCUMENTS

A. West Coast Sources

California employees may have original documents. *We need to have an inventory of documents. We also need to take an image of the California employees' hard drives. The people in California that may have documents are Kaplan, Sylar, Steve, Rob Chinn, Debra, and Irene Shaw.* Additionally, the west coast has direct a communication with the Vancouver facility that the rest of the company does not know about. DESI also maintains a private e-mail distribution list for internal communications. You must be a member to use the list. There is a support list regarding setting up elections, etc. The e-mail distribution lists contain active and non-active lists and within each there are archived and non-archived e-mails. Certain lists are archived and some are not. DESI monitors the e-mails and archives certain e-mails that are significant. The hardware list, Seville, water cooler, and development, are non-archived. In addition, DESI has regular company e-mail. DESI does not have a regular practice of maintaining company e-mails. The e-mails move off the exchange server after 90 days.

DESI gives its California employees computers; some even have two or more computers. *We need to find out what documents are on these computers.* We can go to any computer and access the e-mail distribution lists, but not personal e-mails; only approved machines.

- *Some people may also have compact diskettes with responsive documents.*
- *Some people may have palm pilots or black berries, but nobody in sales or support have any.*
- *Some sales people use personal e-mail accounts even though it is not allowed.*

III. BREACHES OF DESI'S WEB SITES

A. Staff Site Breach

The staff site is an internal web site that is password protected. In March 2003, the site was hacked by someone using an employee's password. Bev Harris, of Blackbox Voting, has

obtained some of the documents from this site. The staff site contains internal e-mail lists such as a support list, announce list, SW announce list, product documentation/product certification list, customer list, sales talk, RCR (request for change report), and the bugtrack list within the Bugszilla system. The staff cite also contains a new list called "certification" but it was not breached. The staff site consists of 1.6 gigabytes of information. The staff site is all active and archived. Additions to the lists have been made since the breach.

B. FTP Site Breach

The FTP site contains portions of source and object code and customer databases, including the San Luis Obispo County database. The FTP site does not contain an e-mail exchange like the staff site, but there may be databases for certifications and some were not password protected.

IV. VSPP DOCUMENT REQUEST

A. Preliminary Issues

- *The first issue we need to determine is whether the Secretary of State has documents from the FTP site.*
- *Next, we have to identify what documents are subject to each request from the VSPP.*
- *We need to try to narrow the scope of the document request.*
- The DMCA litigation is ongoing, but Wally O'Dell decided to stop sending cease-and-desist letters because of the bad press that Diebold received in response to the letters.

B. VSPP Requests

1. First Request

The first request concentrates on providing Steve Freeman with categories and classifications for his spreadsheet to determine whether the effect on California was critical, normal, or minor. Steve Freeman has already prepared a spreadsheet regarding the changes to GEMS and has numbered and bulleted the bugs. The VSPP is now requesting DESI to identify

the bug fixes related directly and indirectly to California and classify those as critical or non-critical. A direct change is one that was made to comply with California law. An indirect change is one made to comply with another state's law but that affects the software used in California.

2. Second Request

Documents regarding software modifications to GEMS and the DRE systems in each county will involve an inventory of accounts, and changes in release levels. The release notes are originally in electronic format and they detail differences with prior versions. The release notes show each new version. By using Bugszilla, one can see a full history of all changes reflecting all versions and the differences between them. *We can show the VSPP a full history, but we probably only need to show some of the history. (Steve Freeman will probably show the full history in response to the first request).* The release notes show summary lines for bugs that were fixed and categorized. The volume of a full history is probably less than a box. *All of the Bugszilla system's documents are classified as trade secrets.* The document types in response to this request are release notes, Bugszilla, e-mails on support (not formal documentation), and documents on the development list. *We need to determine the status of internal e-mails and whether they are responsive.*

We have given the Secretary of State release notes and Bugszilla for GEMS, but we are not sure about the DRE systems. A summarized version of the bugs list was given to auditors, and a full detailed list was given to Steve Freeman. Bugszilla covers release notes and a full report; that is, it includes the release notes within the full report of the system. *One issue is whether Steve Freeman has lists only from the security breach to the present time. We should determine if he has pre-breach information so that we can identify that information as confidential. Another issue is to discuss a non-disclosure agreement with Steve Freeman for*

information that is not already in the public domain. We also need to find out what DESI gave to the Audit Committee. A final issue is whether the Secretary of State and the VSPP wants extraneous communications about changes.

3. Third Request

This request regarding federal and state certification documents may be an issue. DESI has certification documents, but not for each version. *One issue is whether the request is limited to existing versions or whether it asks for all versions.* As for the existing versions, certain versions of GEMS did not have federal and state certification. The federal certification report that DESI receives is confidential and DESI gives its customers only a cover letter to show that the version is certified. *One issue is to collect all cover letters that show federal certification. We can notify the VSPP that this report is proprietary, confidential and privileged, and simply provide the VSPP with the cover letter.*

The State of California issues a certificate but the certificate is very sloppy and does not even specify a version number. It is hard to tell from the state certificate what has been certified.

A technical data package (TDP) is a responsive document that goes to the independent testing authority (ITA), but because this information is confidential and proprietary, we have an argument not to disclose this information.

The election management software (EMS), the hardware, which is a Dell server, is non-certified, and the firm ware, which is the software which goes into the hardware such as the ballot station or touch screen are possibly responsive.

One issue is that there is a chart regarding the Accu-Vote.

Another is that we need NASED numbers for hardware and firmware.

We may need central and precinct count firmware, but the central count firmware did not require certification so there is no ITA or state certification. We need to get the document from

Steve Kennick indicating that no state certification is required for central count firmware. The Touch Screen firmware versions may be an issue. We need to narrow the scope to include only the current version.

4. Fourth Request

The document of material control procedures and security controls is manageable. *We need to talk to Barry Lucas to get this information which deals with ISO certification.*

5. Fifth Request

The fifth request is the "smoking gun" request. This request is extremely broad. Apparently, DESI created new versions when old ones had bugs, obtained federal qualification, and used the new versions in counties as an experiment without state certification. *We may need to obtain e-mails, if possible, regarding state certification of uncertified software. We need to devise a plan to locate responsive documents to this request.* This request will be problematic.

6. Sixth Request

Documents regarding DESI's internal software development security procedures should not be too difficult. The current information can be provided without much trouble. Past information may not be written down. The document request specifies documents from product development through client maintenance – *i.e.*, from inception to launch. The request seeks security documents regarding security procedures. *We need to determine whether it is historical or current information that is being sought.* We can most likely designate the current information as proprietary and argue to withhold this information. *We will need to speak with Rob McDonald regarding this request.*

7. Seventh Request

The seventh request is straightforward.

8. Eighth Request

The eighth request is based on Jim March's recommendations. Mr. March thinks that DESI modified the Windows CE programs. The CE program is the core program and it is not modified. The Windows CE drivers are modified, and the drivers are used to enable the CE program to communicate with the other components. The CE program is like a brain without a body. The CE program is embedded in the system. The system is not an off-the-shelf system. The drivers and the core CE program are merged together in one file. *We need to talk to Pat Green in response to this request.*

9. Ninth Request

The ninth request regarding modifications to the Smart Card hardware may pose problems. The Smart Card hardware is essentially the Smart Card readers that are mounted on a TS unit. The reader is the hardware and we can provide technical specifications for the Smart Card readers. The Smart Card hardware is not modified and the firmware within the hardware will already be covered in response to the second request regarding the ballot station software. There may have been modifications to the Smart Card itself but the request is not asking this. The request is simply directed to Smart Card hardware or software; the hardware is not modified, and the software modifications are dealt with in response to the second request.

- *One issue may be the pic chip disclosure. We need to inquire about this. The pic chip is firmware in the TSx, which performs a low-level function. DESI has source code that is proprietary. DESI had made modifications to the pic chip.*
- *The firmware on the optical scan, called the boot load, has undergone minor modifications and should arguably be disclosed because it is arguably software. The boot load is the firmware that operates when you boot the system up. DESI contracts for the boot load with a third-party vendor who does not allow its source code to be disclosed. This may be an issue.*
- *Another issue may be the ballot station software.*

- *The reader for the Smart Card reader firmware is developed by a third-party vendor and it is third-party proprietary information. The third-party vendor does not want DESI or anyone else to know about its source code. Any changes to the Smart Card reader were minor.*

- *The optical scan scanning device has firmware that may be an issue, but it is proprietary.*

- *We need to talk to Pat Green in response to this request.*

Scott P. Shaw
(213) 243-2386
32386

January 29, 2004