UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

DIVISION OF
CORPORATION FINANCE

April 25, 2006

Harvey Goldman
Holland & Knight LLP
701 Brickell Avenue, Suite 3000
Miami, FL 33131-2847

Act: 1934
Section:
Rule: 14A-8
Public
Availability: 4/25/2006

Re: Applied Digital Solutions, Inc.
Incoming letter dated March 10, 2006

Dear Mr. Goldman:

This is in response of your letter dated March 10, 2006 concerning the shareholder proposal submitted to Applied Digital Solutions by Harrington Investments, Inc. We also have received a letter from the proponent dated March 31, 2006. Our response is attached to the enclosed photocopy of your correspondence. By doing this, we avoid having to recite and summarize the facts set forth in the correspondence. Copies of all of the correspondence also will be provided to the proponent.

In connection with this matter, your attention is directed to the enclosure, which sets forth a brief discussion of the Division's informal procedures regarding shareholder proposals.

Sincerely,

Eric Finseth
Attorney-Adviser

Enclosures

cc: John C. Harrington
President
Harrington Investments, Inc.
1001 2nd Street, Suite 325
Napa, California 94559

Holland+Knight

Tel 305 374 8500
Fax 305 789 7799

Holland & Knight LLP
701 Brickell Avenue, Suite 3000
Miami, FL 33131-2847
www.hklaw.com

HARVEY GOLDMAN
305-789-7506
harvey.goldman@hklaw.com

March 10, 2006

Office Of The Chief Counsel
Division Of Corporation Finance
Securities And Exchange Commission
Judiciary Plaza
450 Fifth Street, N.W.
Washington, DC 20549

Re: Applied Digital Solutions, Inc. -- Shareholder Proposal of John Harrington

Ladies and Gentlemen:

Applied Digital Solutions, Inc, a Missouri corporation (the "Company"), has received a shareholder proposal, dated December 22, 2005 (the "Proposal"), from a shareholder of the Company, Mr. John Harrington (the "Proponent"), for inclusion in the Company's proxy statement for its 2006 annual meeting of shareholders (the "2006 Annual Meeting"). The Company believes it may properly omit the Proposal from its proxy materials for the 2006 Annual Meeting for the reasons discussed below. The Company respectfully requests confirmation that the staff (the "Staff") of the Securities and Exchange Commission (the "Commission") will not recommend enforcement action if the Company excludes the Proposal from its proxy materials in reliance upon Rule 14a-8(i)(3), Rule 14a-8(i)(7) or Rule 14a-8(i)(10) promulgated under the Securities Exchange Act of 1934, as amended (the "Exchange Act").

Pursuant to Rule 14a-8(j) under the Exchange Act, enclosed on the Company's behalf are six (6) copies of each of (i) the Proposal, (ii) this letter, which sets forth the grounds on which the Company proposes to omit the Proposal from its proxy materials, and (iii) the correspondence related to the Proposal attached hereto as Exhibits A through C. Also enclosed is an additional copy of this letter, which we request to have file stamped and returned in the enclosed postage-prepaid envelope. As required by Rule 14a-8(j), a copy of this letter also is being sent to the Proponent as notice of the Company's intention to omit the Proposal from the Company's definitive proxy materials. Pursuant to Rule 14a-8(j), this letter is being submitted not less than eighty (80) days before the Company files its definitive 2006 proxy materials with the Commission.

The text of the Proposal is set forth below.

The Proposal

RFID Risks to Public

WHEREAS, even though radio frequency identification (RFID) chips are passive, not containing their own power source, any information encoded on the chip, whether it is information such as a person's name or a unique identifier number, can be read from a distance by anyone with a reader without the knowledge of the chip holder.

WHEREAS, there have already been several costly breaches of RFID chip technology: the security on chips used in German phone cards was cracked in 1998, resulting in losses of $34 million; the encryption key to the chips used in French bank cards was cracked in 2000; and the RFID chips used in Exxon Mobil gasoline passes and automobile anti-theft devices were cracked in 2005.

WHEREAS, the read range of RFID chips has been shown to be far greater than the range intended: the U.S. State Department showed that a chip quoted as being readable from 4 inches away could be read from 2-3 feet away; in 2004, the National Institute of Technology reported that these chips could be read from as much as 20 feet away; in 2005, Los Angeles based Flexilis was able to read an RFID chip from 69 feet away. Advances in reader technology will only make them more powerful and increase read ranges.

WHEREAS, RFID readers as small as a handheld digital organizer are available for purchase on the Internet for several hundred dollars.

WHEREAS, a chip containing solely a unique identifier number still presents significant privacy and security concerns since this number can be used much like a social security number, providing access to personal information, such as an individual's location or medical and financial records. This identification number could also be used to allow unauthorized people to enter restricted facilities.

WHEREAS, presently there is California legislation pending which creates privacy and security safeguards for the use of RFIDs in government-issued identity documents. The bill is being sponsored by the American Civil Liberties Union (ACLU), Privacy Rights Clearinghouse, and Electronic Frontier Foundation and supported by a broad coalition of organizations.

RESOLVED, shareholders request that the independent directors of the Board of Applied Digital Solutions prepare a report, at reasonable cost and omitting proprietary information, on the harm the continued sale and use of RFID chips could have to the public's privacy, personal safety, and financial security. The report should be available to investors by the 2007 annual meeting.

Supporting Statement

We applaud our company for the privacy guidelines released at the 2004 World ID conference for its VeriChip. We welcome this interest in privacy protection, and we believe, in addition to recognizing the issue, there is a need to study and disclose the adverse impact that RFID technology could have. This would allow shareholders to assess the risk, including legal and financial, created by the company's activity in these areas as well as the company's strategy for managing these risks.

Background

The Company's subsidiary, VeriChip Corporation ("VeriChip"), develops, markets and sells radio frequency identification ("RFID") systems used to identify, locate and protect people and assets, with a focus on providing RFID systems for people in the healthcare industry ("VeriChip System").[1] VeriChip has recently begun to market one application of its VeriChip System as an identification system which is used to rapidly and accurately identify people who arrive in an emergency room and are unable to communicate ("VeriMed"). The Company's VeriMed patient identification system uses the first human-implantable passive RFID microchip, cleared for medical use in October 2004 by the United States Food and Drug Administration ("FDA"). The implantable VeriChip System is a passive RFID microchip, approximately the size of a grain of rice, that is inserted under the skin in a patient's triceps area between the elbow and the shoulder of the right arm by the patient's physician or other authorized healthcare professional. Once inserted, the microchip is not visible to the naked eye. The implantable VeriChip contains a unique identification number. The Company believes that its VeriMed patient identification system, is compelling for emergency room physicians as well as for patients who have cognitive impairment, chronic diseases or implanted medical devices. Using the Company's scanners, an emergency room physician can obtain the patient's name, primary care physician, emergency contact and other pertinent pre-approved data (such as personal health records) by accessing an anonymous identification number not used for any other purpose. The physician is then able to send the identification number to a secure information database that contains the individual's personal contact information, emergency contact information, primary care physician contact information and other pertinent pre-approved patient data. The database is contained outside the microchip and therefore has protection against the risk that an individual in possession of a VeriMed compatible scanner may access the patient's personal information. Additionally, medical personnel and facilities are prescreened and approved prior to their receiving the hand-held reader, and the Company restricts or terminates medical personnel or facility access to patient information if VeriChip agreement violations occur. Finally, medical

[1] VeriChip licenses the rights to the VeriChip System from Digital Angel Corporation, a majority-owned subsidiary of the Company under the terms of a Supply, License and Development Agreement. Digital Angel owns the intellectual property rights underlying the VeriChip System and licenses that intellectual property to VeriChip. Additionally, Digital Angel markets implantable RFID microchips, primarily for identification, tracking and location of pets, livestock and other animals.

personnel and facility passwords are location created and required to be changed every ninety (90) days. The Company expects that this rapid and accurate identification process will reduce the risk of a patient being misdiagnosed or other possible medical errors. The Company currently markets the VeriMed patient identification system to both hospitals and physicians. The Company is educating hospitals as to the benefits in adopting the VeriMed patient identification system.

In addition to the Company's VeriMed patient identification system, the Company markets and sells other RFID systems for other applications in the healthcare industry as well as for security and industrial applications. These RFID systems, which have been installed in over 4,000 healthcare locations throughout North America, include:

- infant protection systems used to prevent mother-baby mismatching and infant abduction;
- wander prevention systems used for protection and location of residents in long-term care facilities;
- asset location and identification systems used to locate and identify medical equipment;
- asset management systems that also incorporate bar code technology used to track mobile assets, equipment and inventory; and
- other systems incorporating the VeriChip technology used for security purposes such as access control, payment verification and military applications.

Bases for Exclusion

The Company hereby respectfully requests that the Staff concur in its view that the Proposal may be excluded in its entirety from the Company's 2006 proxy materials on the bases set forth below:

(I) Rule 14a-8(i)(7). The Proposal relates to the conduct of the ordinary business operations of the Company.

(II) Rule 14a-8(i)(3). The Proposal contains vague, false and materially misleading statements in violation of Rule 14a-9 under the Exchange Act.

(III) Rule 14a-8(i)(10). The Proposal has already been substantially implemented.

I. Rule 14a-8(i)(7). The Proposal May Be Excluded Because It Deals With Matters Relating To The Company's Ordinary Business Operations.

Under Rule 14a-8(i)(7) of the Exchange Act, a shareholder proposal may be omitted from a company's proxy statement if such proposal "deals with matters relating to the company's ordinary business operations." The Commission has stated that the policy underlying the ordinary business exclusion is "to confine the solution of ordinary business problems to the board of directors and place such problems beyond the competence and direction of the shareholders. The basic reason for this policy is that it is manifestly impracticable in most cases for shareholders to decide management problems at corporate meetings." *Release No. 34-19135*, n. 47 (October 14, 1982) (quoting from Hearing on SEC Enforcement Problems before the Subcommittee of the Senate Committee on Banking and Currency, 85th Congress, 1st Session part 1, at 119 (1957)). In its release adopting revisions to Rule 14a-8, the Commission reaffirmed this position by stating that "[t]he general underlying policy of this exclusion is consistent with the policy of most state corporate laws: to confine the resolution of ordinary business problems to management and the board of directors, since it is impracticable for shareholders to decide how to solve such problems at an annual shareholders meeting." *Release No. 34-40018* (May 21, 1998).

The Commission has noted that the policy underlying the ordinary business exclusion rests on two central policy considerations. The first is that "certain tasks are so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight." *Id.* The second "relates to the degree to which the proposal seeks to "micro-manage" the company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment." *Id.* The Staff has established that where the subject matter of a proposed report involves a matter of ordinary business, the proposal will be excludable. *Release No. 34-20091* (August 16, 1983).

A. The Proposal Is Excludable Because It Directly Relates To The Company's Compliance With Laws and Regulations.

The Proposal requests the Company's Board of Director (the "Board") to prepare what could be an extremely detailed and technical report "on the harm that continued sale and use of RFID chips could have to the public's privacy, personal safety, and financial security."

In numerous instances, the Staff has concluded that proposals related to compliance with government statutes and regulations involve ordinary business and therefore are excludable pursuant to Rule 14a-8(i)(7). In *Willamette Industries, Inc.* (March 20, 2001), for example, the Staff concurred that a proposal requiring the board of directors to create an independent committee to prepare a report of the company's environmental problems and efforts to resolve them, including an estimate of worst case financial exposure due to environmental issues for ten years as well as other matters specified in the proposal, could be omitted from the company's proxy materials in accordance with Rule 14a-8(i)(7) because such "evaluation of risk" related to the company's ordinary business operations. In addition, the Staff concurred with Duke Power

Company's conclusion that the company could exclude a similar shareholder proposal because compliance with government regulations relating to the environmental impact of power plant emissions was considered part of the company's ordinary business operations. *Duke Power Company* (March 7, 1988). *See also Allstate Corporation* (February 16, 1999).

The VeriMed patient identification system is a medical device subject to extensive regulation by the FDA, as well as other federal and state regulatory bodies in the United States and comparable authorities in other countries. The Company currently has FDA clearance to market its products in the United States for patient identification and health information. FDA regulations govern the following activities that the Company performs, or that are performed on its behalf, to ensure that medical products distributed domestically or exported internationally are safe and effective for their intended uses:

- product design, development and manufacture;
- product safety, testing, labeling and storage;
- premarketing clearance or approval;
- recordkeeping procedures;
- product marketing, sales and distribution; and
- post-marketing surveillance, reporting of deaths or serious injuries and medical device reporting.

The VeriMed patient identification system is subject to special controls, including, but not limited to, controls on biocompatibility, information security procedures, software validation, performance testing, electromagnetic compatibility and sterility testing. The Company has registered with the FDA as a medical device manufacturer. The FDA has broad post-market and regulatory enforcement powers. The Company is subject to unannounced inspections by the FDA to determine the Company's compliance with the Quality System Regulation and other regulations. Such inspections may include the manufacturing facilities of the Company's suppliers.

Failure to comply with applicable regulatory requirements can result in enforcement action by the FDA, which may include any of the following sanctions:

- warning letters, fines, injunctions, consent decrees and civil penalties;
- repair, replacement, refunds, recall or seizure of the Company's products;
- operating restrictions, partial suspension or total shutdown of production;

- refusing the Company's requests for 510(k) clearance or premarket approval of new products, new intended uses or modifications to existing products;

- withdrawing 510(k) clearance or premarket approvals that have already been granted; or

- criminal prosecution.

Additionally, the Company's activities related to RFID technology are currently regulated by a growing body of laws designed to protect the privacy of personally identifiable information, as well as to protect against its misuse. In the United States, these laws include the Health Insurance Portability and Accountability Act ("HIPAA"), the Federal Trade Commission ("FTC") Act, the Electronic Communications Privacy Act, the Fair Credit Reporting Act, the Gramm-Leach Bliley Act, as well as various state laws and related regulations. Although the Company is not a covered entity under HIPAA, the Company has entered into agreements with certain covered entities in which the Company is considered to be a "Business Associate" under HIPAA. As a Business Associate, the Company is required to implement policies, procedures and reasonable and appropriate security measures to protect individually identifiable health information it may receive from covered entities.

In addition, certain governmental agencies, like the United States Department of Health and Human Services and the FTC, have the authority to protect against the misuse of consumer information by targeting companies that collect, disseminate or maintain personal information in an unfair or deceptive manner. The Company is also subject to the laws of those foreign jurisdictions in which it operates, some of which currently have more protective privacy laws than those of the United States. The Company is also required to obtain certain regulatory approvals from the governments of the countries in which the Company's foreign distributors sell its systems. Compliance with those laws and regulations is a part of the day-to-day business of the Company as it endeavors to produce safe, secure and healthy products.

The discretionary authority to develop products that comply with the FDA and other regulations should reside with the Company's management rather than its shareholders. Regulatory compliance issues, including product safety, have been found by the Staff to be within the ordinary business operations of a company. *Johnson & Johnson* (Feb. 24, 2006) (excluding a proposal requesting the board of directors to appoint a scientific integrity committee to study research integrity, notwithstanding that the company's products were subject to extensive product safety regulation by regulatory agencies, in particular the FDA, as dealing with the day-to-day business operations of the operating companies of the Company regarding legal and regulatory compliance); *General Electric Co.* (Jan. 4, 2005) (excluding a proposal requesting a report detailing the company's broadcast television stations' activities to meet public interest obligations as relating to the company's ordinary business operations (i.e., the general conduct of a legal compliance program), namely its compliance with FCC regulations regarding public interest obligations). In making those determinations, the Staff has implicitly recognized that

the regulation of medical products and devices is a function assigned to the FDA and that those companies engaging in the manufacturing of medical products and devices, like the Company, merely provide access to products approved by the FDA to a broad spectrum of the American population. The Company strives to design and produce safe and secure products and is keenly motivated to protect health information received from customers and has staff devoted to compliance with these various privacy and consumer protection regulations. The Company addresses the issues raised by the Proposal in its ordinary day to day business.

In particular, the FDA's clearance for the VeriChip System limits its use in medical applications by allowing the microchip to only include an identification number. Any additional information, including patient information, must reside in a database contained outside the microchip. Any modification to an FDA-cleared device, such as the VeriChip System, that would significantly affect its safety or effectiveness or that would constitute a major change in its intended use would require new FDA clearance or approval.

Research and development of innovative products used in the healthcare industry is fundamental to the ordinary business operations of certain of the operating companies of the Company. Among other laws and regulations addressing consumer privacy and safety, FDA regulations specifically govern these research and development activities for the VeriChip System, including the assurance of research integrity. Therefore, the Proposal may be excluded as ordinary business under Rule 14a-8(i)(7) because it relates to the Company's compliance with applicable law, particularly with federal regulations issued by the FDA.

B. The Proposal Is Excludable Because It Involves the Shareholders' Assessment Of The Legal and Financial Risks Related To The Company's RFID-Related Activities As Well As The Company's Strategy For Managing These Risks.

The Proposal requests a study be conducted by the Company in order to "allow shareholders to assess the risk, including legal and financial, created by the company's activit[ies] [in RFID related-products] as well as the company's strategy for managing these risks." In essence, the Proposal seeks a report from the Company which includes an evaluation of the risks of potential legal and financial liabilities associated with the Company's RFID-related products. Monitoring financial risks, including those associated with the Company's impact on consumer privacy and safety, is an ongoing component of the overall management of the Company. Financial risks, including those associated with the Company's impact on the consumer public, are among the factors regularly considered by the Board and management when making their business decisions. The Staff has concurred in the exclusion of proposals under Rule 14a-8(i)(7) in analogous situations. In a No-Action Letter issued to E.I. du Pont de Nemours and Co., the Staff indicated that a proposal which involved the phase out of certain chemicals was excludable under rule 14a-8(c)(7)(the predecessor of Rule 14a-8(i)(7)) because it was "directed at those questions concerning the timing, research and marketing decisions that involve matters relating to the conduct of the Company's ordinary business operations." *E.I. du Pont de Nemours and Co.* (March 8, 1991). In Pacific Telesis Group, the Staff indicated that a

proposal seeking to reduce the company's "potential negative environmental impact" (including the reduction of toxic wastes and the minimization of the use of chlorofluorocarbons) was excludable because the proposal appeared to be aimed at matters which involved the conduct of ordinary business operations, and noted that the proposal concerned "the board taking certain specified actions that involve discrete operational matters." *Pacific Telesis Group* (February 21, 1990). Clearly, from a subject matter perspective, evaluating and reporting on the financial risks and management's strategy to manage such risks of the Company is best addressed by the management of the Company. Furthermore, the preparation, parameters, guidelines, timing and purpose of such reports are clearly within the purview of the Board. The Proposal clearly seeks to micro-manage the Company, as explained by the Staff in No-Action Letter precedents, in violation of Rule 14a-8(i)(7), and the Company therefore believes it can exclude the Proposal.

The Company is aware of the social policy issue exception to the ordinary business operations rule, and that proposals focusing on sufficiently significant social policy issues are generally not excludable. The Company also notes, however, that in numerous No-Action Letters, the Staff has not objected to excluding shareholder proposals when such proposals relate to the nature of a company's day-to-day business. *See College Retirement Equities Fund* (Sept. 7, 2000) (proposal requesting that the College Retirement Equities Fund take steps to divest its holdings of a particular entity omitted as it relates to the ordinary business operations of an investment company); *American International Group, Inc.* (Mar. 17, 1998) (proposal requesting that the board of directors review and report on the company's anticipated property loss and/or health care loss liabilities potentially caused by global warming and on the company's public policy stance on global warming as it relates to its loss prevention activities omitted as relating to the company's ordinary business operations); *The Walt Disney Company* (Nov. 10, 1997) (proposal mandating that the board of directors review and report on the way tobacco use is portrayed in its films and programs for television, any potential influence on youth smoking, and whether tobacco companies are paying for product placement and that the board of directors recommend any appropriate responsive policies omitted because the nature, presentation and content of programming and film production relates to the company's ordinary business operations); *Xerox Corporation* (Feb. 29, 1996) (proposal requesting that the company's board of directors appoint a committee to review and report on the company's adherence to human rights and environmental standards with respect to its overseas business omitted as relating to the company's ordinary business activity with respect to employment related matters); *Carolina Power & Light Co.* (Mar. 8, 1990) (proposal requesting a company report, to be made available to shareholders upon request, regarding specific aspects of the company's nuclear operations relating to, inter alia, safety, regulatory compliance, emissions problems, hazardous waste disposal and related cost information omitted as relating to the company's ordinary business of operating a nuclear power plant); *Duke Power Company* (Mar. 7, 1988) (proposal requesting that the board of directors prepare a report providing the best factual and scientific information available detailing the company's environmental protection and pollution control activities omitted as relating to the company's ordinary business of complying with government regulations). In each of these No-Action Letters, the Staff did not object to excluding the shareholder's proposal because the proposal in question related to the day-to-day activities of the

company, regardless of the fact that such day-to-day activities could be tied to larger social issues.

The Proposal does not raise significant social policy concerns. Insofar as we understand the intent of the Proposal, if adopted, it seems to be no more than having the Board prepare a report on issues related to the financial and legal risks to the Company in the RFID industry, notwithstanding that it is couched in language purporting a concern for "the public's privacy, personal safety, and financial security." The underlying intent of the Proposal is evidenced in the Supporting Statement which provides that ". . . . there is a need to study and disclose the adverse impact that RFID technology could have . . . to allow shareholders to assess the risk, including legal and financial, created by the company's activity in these areas as well as the company's strategy for managing these risks . . . ."

Furthermore, in the *College Retirement Equities Fund* No-Action Letter, the Staff did not object to the position that for a shareholder proposal to rise to the level of a significant social policy it must "involve a request to institute a broad or fundamental corporate policy." *College Retirement Equities Fund* (Sept. 7, 2000). The Proposal does not make such a request. The Proposal does not ask the Board to modify, adopt, or retain any corporate policy of the Company. In fact, the Proposal seeks a study on potential adverse impact of the continued sale and use of RFID chips could have to the public's privacy and personal safety, notwithstanding that the Proponent cites no supporting documentation in connection with the purported RFID financial security breaches referenced in the Proposal. Rather, the Proposal states that the study "would allow shareholders to assess the risk, including legal and financial, created by the company's activity in these areas as well as the company's strategy for managing these risks." Elevating the vague Proposal to the status of "a request to institute a broad or fundamental corporate policy" would open the door for any conceivable shareholder proposal to be considered a matter of significant social policy merely by referencing, citing or using the namesake of a well-known social movement. Merely because a shareholder proposal deals with a subject that may touch on a social policy issue does not mean that it may not be excluded if it encroaches on a company's ordinary business operations. Despite the privacy theme and cursory references to the "public's privacy, personal safety, and financial security," the Proposal does not seek to address significant social policy concerns, but rather seeks an evaluation of the Company's financial and legal risks. Consequently, the matters addressed by the Proposal are not matters that should be subject to direct shareholder control. Therefore, the Company believes the Proposal is excludable under Rule 14a-8(i)(7).

II. The Proposal Is Vague And Contains Misleading and False Statements In Violation Of Rule 14a-9 Under The Exchange Act.

Rule 14a-8(i)(3) under the Exchange Act permits a company to omit from its proxy materials a shareholder proposal and any supporting statement if the proposal or supporting statement is contrary to any of the Commission's proxy rules, including Rule14a-9, which prohibits materially false or misleading statements in proxy soliciting materials. Rule 14a-9(a)

under the Exchange Act provides, in pertinent part, that "[n]o solicitation subject to this regulation shall be made by means of any proxy statement, form of proxy, notice of meeting or other communication, written or oral, containing any statement which, at the time and in the light of the circumstances under which it is made, is false or misleading with respect to a material fact, or which omits to state any material fact necessary in order to make the statements therein not false or misleading . . . . " In addition, the Staff has stated that a proposal is sufficiently vague and indefinite to justify its exclusion where "neither the shareholders voting on the proposal, nor the Company in implementing the proposal (if adopted), would be able to determine with any reasonable certainty exactly what actions or measures the proposal requires." *Philadelphia Electric Company* (July 30, 1992). *See also Bristol-Myers Squibb Company* (Feb. 1, 1999). The Staff has found that a company could properly omit entire shareholder proposals and supporting statements when such proposals and supporting statements were vague, indefinite, false or misleading. *See, e.g., Wal-Mart Stores, Inc.* (April 2, 2001); *McDonald's Corporation* (March 13, 2001); *Comshare, Incorporated* (August 23, 2000); *Tri-Continental Corporation* (March 14, 2000). The Staff has also, on many occasions, found that a company could properly omit certain portions of shareholder proposals and supporting statements that contain false and misleading statements or omit material facts necessary to make statements therein not false or misleading. *See e.g., Sysco Corporation* (September 4, 2002); *American Standard Companies, Inc.* (March 18, 2002); *Emerson Electric Co.* (October 27, 2000); *National Fuel Gas Company* (November 18, 1999); *Baldwin Corporation* (February 20, 1998). Moreover, the Staff has recognized that "[i]n drafting a proposal and supporting statement, shareholders should avoid making unsupported assertions of fact." To this end, shareholders "should provide factual support for statements in the proposal and supporting statement" or phrase statements as their opinion where appropriate." *Staff Legal Bulletin No. 14* (July 13, 2001).

A. The Assertion That The Company's RFID Microchip User's Personal Identifier Information May Be Accessed By Any Person With A Hand-Held Reader Is Materially False And Misleading.

The Proposal states, without support, that "any information encoded on the chip, whether it is information such as a person's name or a unique identifier number, can be read from a distance by anyone with a reader without the knowledge of the chip holder." The microtransponder contained in the implantable microchip, in fact, does not contain a user's personal identifying information such as a user's name, social security number, address, telephone numbers, driver's license information or other unique identifying information used for multiple purposes. Instead, the only information assessable from the Company's RFID microtransponder is an anonymous identification number that cannot be used for any other purpose. This contrasts with unique identifier numbers, such as Social Security numbers or Driver's License numbers, which are used for multiple purposes. Furthermore, the VeriChip System, with respect to its medical and building access applications, utilizes the reading of a microchip as only one step in a multi-tiered pathway to information access and actions. As noted above, a VeriMed patient's personal identifying information resides in a database contained outside the microchip, thus alleviating concerns that the use of a hand-held reader provides one-

step access to personal identification information. Therefore, notwithstanding the Proponent's assertions that RFID readers are available for purchase on the Internet, it does not follow that an individual with access to a reader is easily able to procure a VeriChip user's identification. Additionally, an individual with a VeriChip implant specifically consents to information access prior to undergoing the insertion procedure and has control of both the information viewable and the persons who have access to the information. The individual, furthermore, has the option to have the implant removed which would sever the link between the microchip reading and the information database, or use of the personal identification number to identify the individual. Therefore, the Proponent is incorrect in his assertions that the Company's VeriChip System user's personal identifying information may be accessed by any person with a hand-held reader.

B. The Assertions That Private Information "Can Be Read From A Distance By Anyone With A Reader Without The Knowledge Of The Chip Holder" And "The Read Range Of RFID Chips Has Been Shown To Be Far Greater Than The Range Intended" is Unsubstantiated and Materially Misleading.

The Proposal's assertion that the VeriChip hand-held reader may be read from a distance is factually incorrect because the maximum read range of the hand-held reader under the most optimum conditions is 4 inches and the microchip is most reliably read when the microchip is 2.5 inches or less from the hand-held reader. The VeriChip System hand-held reader has an effective read range of no more than 2.5 inches with maximum accuracy as stated in the VeriMed Reader Operator's manual.

C. The Examples Of Recent Security Breaches Of RFID Technology Are Unrelated To The Format Of The Technology Found In The Company's Products And The Reference To These Security Breaches As Well As Hypothetical Security Breaches Are Unsubstantiated And Materially Misleading.

The Proposal states, without support, that "there have already been several costly breaches of RFID chip technology: the security on chips used in German phone cards was cracked in 1998, resulting in losses of $34 million; the encryption key to the chips used in French bank cards was cracked in 2000; and the RFID chips used in Exxon Mobil gasoline passes and automobile anti-theft devices were cracked in 2005." There are many formats of RFID technology. The Company believes that none of the examples of RFID technology cited in the Proposal are comparable and, therefore relevant, to the technology utilized by the Company's VeriChip System. Furthermore, the Proponent has not provided any documentation to support the assertion that the Company's products pose any threat to public privacy or security other than the general association with other unnamed RFID technology products. Therefore, the Proposal should be excluded because the examples of RFID security breaches are unsubstantiated and materially misleading.

The Proposal further states ". . . [the VeriChip System] identification number could also be used to allow unauthorized people to enter restricted facilities." This assertion is materially

misleading as it is merely a hypothetical example of a security breach with no basis in fact. The Company believes that any security system is strengthened by having several layers of protection. The Company has never publicized or made any statement to the effect that the Company's VeriChip System technology should be utilized as a stand-alone security access solution but rather that it should be used to complement other security measures. Based upon these statements, the inclusion of the Proposal in the 2006 proxy materials would constitute a violation of Rule14a-9, which prohibits materially false or misleading statements in proxy soliciting materials.

III. Rule 14a8(i)(10). The Company Has Already Substantially Implemented The Proposal And Therefore The Proposal May Be Excluded.

Rule 14a-8(i)(10) under the Exchange Act authorizes a company to exclude a shareholder proposal from the company's proxy soliciting materials if the company has "substantially implemented" the action requested. The Staff has consistently taken the position that shareholder proposals have been substantially implemented within the meaning of Rule 14a-8(i)(10) when the company already has policies, practices and procedures in place relating to the subject matter of the proposal, or has implemented the essential objective of the proposal. *See, e.g., Telular Corp.* (December 5, 2003) (proposal requesting board to take the necessary steps to change the bylaws for the annual election of directors excludable where the company bylaws already provide for the annual election of directors). When a company can demonstrate that it has already adopted policies or taken actions to address the elements of a shareholder proposal, the Staff has concurred that the proposal has been "substantially implemented" and may be excluded as moot. *See, e.g., Nordstrom Inc.* (February 8, 1995) (proposal that company commit to a code of conduct to ensure its policies and discusses the Company's current and future compliance efforts and plans that was substantially covered by existing company guidelines was excludable as moot). As discussed below, the Company has substantially implemented the Proposal, thereby rendering the Proposal moot.

The Company is deeply committed to the privacy and safety of its VeriChip System users and has previously identified risks factors associated with RFID related technology. In an effort to develop safe and socially responsible products, the Company has undertaken several key initiatives that respond to the protection of private information of RFID users. These initiatives include:

- Implementation of a continuing program of product development to further enhance the effectiveness of the Company's products and as part of the Company's normal business operations strengthening of the security and privacy measures in order to maintain leadership in these areas within the RFID industry;
- Release of the Privacy Guidelines at the 2004 World ID Conference;
- Receipt of approvals for the Company's VeriChip System products from the FDA;
- Implementation of a corporate privacy policy;

RFID Risks to Public

WHEREAS, even though radio frequency identification (RFID) chips are passive, not containing their own power source, any information encoded on the chip, whether it is information such as a person's name or a unique identifier number, can be read from a distance by anyone with a reader without the knowledge of the chip holder.

WHEREAS, there have already been several costly breaches of RFID chip technology: the security on chips used in German phone cards was cracked in 1998, resulting in losses of $34 million; the encryption key to the chips used in French bank cards was cracked in 2000; and the RFID chips used in Exxon Mobil gasoline passes and automobile anti-theft devices were cracked in 2005.

WHEREAS, the read range of RFID chips has been shown to be far greater than the range intended: the U.S. State Department showed that a chip quoted as being readable from 4 inches away could be read from 2-3 feet away; in 2004, the National Institute of Technology reported that these chips could be read from as much as 20 feet away; in 2005, Los Angeles based Flexilis was able to read an RFID chip from 69 feet away. Advances in reader technology will only make them more powerful and increase read ranges.

WHEREAS, RFID readers as small as a handheld digital organizer are available for purchase on the Internet for several hundred dollars.

WHEREAS, a chip containing solely a unique identifier number still presents significant privacy and security concerns since this number can be used much like a social security number, providing access to personal information, such as an individual's location or medical and financial records. This identification number could also be used to allow unauthorized people to enter restricted facilities.

WHEREAS, presently there is California legislation pending which creates privacy and security safeguards for the use of RFIDs in government-issued identity documents. The bill is being sponsored by the American Civil Liberties Union (ACLU), Privacy Rights Clearinghouse, and Electronic Frontier Foundation and supported by a broad coalition of organizations.

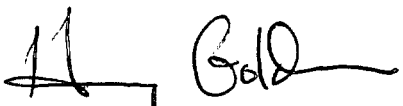
RESOLVED, shareholders request that the independent directors of the Board of Applied Digital Solutions prepare a report, at reasonable cost and omitting proprietary information, on the harm the continued sale and use of RFID chips could have to the public's privacy, personal safety, and financial security. The report should be available to investors by the 2007 annual meeting.

- Compliance with health regulations addressing privacy of information including, without limitation, HIPAA;
- Compliance with medical protocols requiring individual consent for the VeriChip System implantation procedure; and
- Development of information system access and storage with multi-tiered privacy protections.

The Company believes it has substantially implemented the Proposal and requests that the Staff concur with its conclusion that the Proposal may be omitted under Rule 14a-8(i)(10).

For all of the reasons given above, the Company believes it is entitled to omit the Proposal from its 2006 proxy materials. If the Staff disagrees with the Company's conclusion to omit the proposal, we request the opportunity to confer with the Staff prior to the final determination of the Staff's position. Notification and a copy of this letter is simultaneously being forwarded to the Proponent. If the Staff has any questions or comments regarding this filing, please contact the undersigned, at 305-789-7506.

Very truly yours,



Harvey Goldman
Holland & Knight LLP

cc: Scott Silverman, Chief Executive Officer
Michael Krawitz, General Counsel
John Harrington

Exhibit A

December 22, 2005

Scott R. Silverman
Chairman and Chief Executive Officer
Applied Digital Solutions, Inc.
1690 South Congress Avenue, Suite 200
Delray Beach, Florida 33445

Dear Mr. Silverman:

Re: Shareholder Resolution

Harrington Investments, Inc., is a socially responsible investment firm managing assets for individuals and institutions concerned with a social and environmental as well as financial return. I believe that our company needs to ensure our products do not pose a threat to consumers, and I am deeply concerned about the possible adverse effects RFID chips may have on the public's privacy and safety.

Therefore, I am submitting the enclosed shareholder proposal on my own behalf for inclusion in the 2006 proxy statement, in accordance with Rule 14a-8 of the General Rules and Regulations of the Securities Exchange Act of 1934.1 am the beneficial owner, as defined in Rule 13d-3 of the Securities Exchange Act of 1934, of 2,000 shares of Applied Digital Solutions, Inc. I have held my shares continuously for more than one year and will be providing verification of my ownership. I will continue to hold all the shares through the next shareholders' meeting. My representative or I will attend the shareholders' meeting to move the resolution as required by the SEC rules. Thank you.

Sincerely,

John C. Harrington
President

Encl.

Exhibit B

December 28, 2005

Scott R. Silverman
Chairman and Chief Executive Officer
Applied Digital Solutions, Inc.
1690 South Congress Avenue, Suite 200
Delray Beach, Florida 33445

Dear Mr. Silverman:

Re: Proof of Ownership

Please find the enclosed letter from Charles Schwab & Co., verifying stock ownership of Applied Digital Solutions (ADSX) for John C. Harrington. This letter satisfies the SEC rule 14-a(8)(b).

This letter accompanies my previously submitted shareholder proposal regarding RFIDs. Please do not hesitate to contact me if you should care to discuss this letter. Thank you. Sincerely,

John C. Harrington

President

Exhibit C

December 23, 2005

Scott R. Silverman
Chairman and Chief Executive Officer
Applied Digital Solutions, Inc.
1690 South Congress Avenue, Suite 200
Delray Beach, Florida 33445

Dear Mr. Silverman:

RE: John C. Harrington
Charles Schwab Account # 1101-4608
Applied Digital Solutions, Inc. (ADSX)

This letter is to verify that John C. Harrington has continuously held at least $2000 in market value of Applied Digital Solutions stock for at least one year prior to December 22, 2005 (December 22, 2004 to present).

If you need additional information to satisfy your requirements, please feel free to contact me at (877) 806-4101.

Sincerely,

Jennifer D. Lowry
Charles Schwab & Co., Inc.
Institutional Service Group

Supporting Statement

We applaud our company for the privacy guidelines released at the 2004 World ID conference for its VeriChip. We welcome this interest in privacy protection, and we believe, in addition to recognizing the issue, there is a need to study and disclose the adverse impact that RFID technology could have. This would allow shareholders to assess the risk, including legal and financial, created by the company's activity in these areas as well as the company's strategy for managing these risks.

HARRINGTON
INVESTMENTS, INC.

March 31, 2006

Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F Street, NE
Washington, D.C. 20549

Re: Appeal of No Action Request from Applied Digital Solutions, Inc. for a Shareholder Proposal Submitted by John C. Harrington

Ladies and Gentlemen:

This letter is in response to a letter dated March 10, 2006 from Harvey Goldman sent on behalf of Applied Digital Solutions, Inc. (the "Company"), stating the Company's intention to exclude a shareholder proposal and supporting statement filed by John Harrington (the "Proposal") from its proxy materials for the Company's 2006 Annual Meeting of shareholders. This Proposal was filed in order to allow shareholders the right to vote on whether or not the Company should report on the potential adverse impacts of RFID technology.

The Company seeks to exclude the shareholder resolution from their proxy material based on:

1. **Rule 14a-8(i)(3),** which states that the Proposal may be omitted if it contains false or misleading statements; and

2. **Rule 14a-8(i)(7),** which states that the Proposal may be omitted if it deals with a matter relating to the company's ordinary business operations; and

3. **Rule 14a-8(i)(10),** which states that the Proposal may be omitted if the company has already substantially implemented the Proposal.

I respectfully request that the Commission *not* allow the Company to exclude the resolution from its proxy materials for the following reasons:

1. **Rule 14a-8(i)(3)** The Company claims that the assertions made in the proposal are false, misleading, and unsubstantiated. This is not the case. The Proposal's assertions are carefully researched and sources are provided where appropriate. Furthermore, the three points made by the Company contain false and misleading information and are a deliberate misinterpretation of the Proposal's text and intent.

1001 2ND STREET, SUITE 325 NAPA, CALIFORNIA 94559 707-252-6166 800-788-0154 FAX 707-257-7923
HARRINV@NAPANET.NET WWW.HARRINGTONINVESTMENTS.COM

(a) the assertion that the Company's RFID Microchip User's Personal Identifier information may be accessed by any person with a reader is completely accurate.

In the Company's no-action request it states, "The implantable VeriChip contains a unique identification number." This appears to corroborate the Proposal's use of the term "unique identifier number." It is made clear that this number is not a social security number when the Proposal explains that "this number can be used much like a social security number, providing access to personal information." One again, the Company's no-action request validates this statement when it states, "Using the Company's scanners, and emergency room physician can obtain the patient's name, primary care physician, emergency contact and other pertinent pre-approved data (such as personal health records) by accessing an anonymous identification number not used for any other purpose."

The Company argues that since the personal information is stored in a database contained outside the microchip this means it is not at risk of being read by an unauthorized person with scanner. This is simply not true. A report by the United States Government Accountability Office entitled, "Information Security: Radio Frequency Identification Technology in the Federal Government," states, "Without effective security controls, data on the tag can be read by any compliant reader; data transmitted through the air can be intercepted and read by unauthorized devices; and data stored in the databases can be accessed by unauthorized users." Even though personal information is not contained in the microchip, being able to read the unique identifier number gives unauthorized users the ability to access personal information if they have a way to access the database, which can be done.

Journalist Annalee Newitz had a VeriChip implanted under her skin as research for an article. As a test, security researcher Jonathan Westhues used a hand-held reader to read and copy her chip. Once the chip was cloned, he could then use it for whatever Ms. Newitz would use it for, whether it was making purchases are entering buildings (Http://www.internetnews.com/security/print.php/3582971: "The New Chip-erati"; Susan Kuchinskas; February 6, 2006). Certainly, other security measures could be put in place to make this difficult. However, this demonstration shows that a unique identifier number could be easily obtained by an unauthorized user with a hand-held reader.

In its no-action request, the Company also states that, "The individual, furthermore, has the option to have the implant removed which would sever the link between the microchip reading and the information database, or use of the personal identification number to identify the individual." Not only does this statement substantiate the Proposal's assertion that obtaining the personal identification number can enable an unauthorized user to gain someone's identity, the claim that chips can be removed is misleading. A communication from Ms. Newitz explains, "The chips are technically removable. However, the doctor who implanted mine -- Allan Pantuck of UCLA -- explained to me that it would be a rather painful and elaborate procedure because the chip is so small and there would have to be some "hunting around" for it. In other words,

they'd have to slice me open in the spot where the chip was, and then sort of dig around for it. Not very pleasant, and not very quick." It is hard to imagine that this would be a viable option for most of our Company's customers.

(b) the assertions that private information "can be read from a distance by anyone with a reader without the knowledge of the chip holder" and "the read range of RFID chips has been shown to be far greater than the range intended" are supported and accurate.

The sources are given for each of the read distances cited in the Proposal. Though the information cited does not refer specifically to VeriChip microchips, it does illustrate the fact that read distances can vary a great deal, often depending on the equipment used and the circumstances under which it is used. In its no-action request, the Company argues that even under the most optimum conditions, the VeriChip System hand-held reader is able to read a microchip at no more than four inches. That may indeed be true; however, the Proposal's intent is to show that read distances are not cast in stone and have the potential of increasing. Furthermore, it would be ridiculous to assume that any attempt by an unauthorized user to access information on the Company's products would be limited to using an unaltered VeriChip System hand-held reader.

(c) the examples of recent security breaches of RFID technology are related to the format of the technology found in the Company's products and the references to them and a hypothetical security breach are accurate and do not need further support.

The three examples given in the Proposal are all events that would be considered public knowledge, and, therefore, would not require further support (see Exhibits A, B, and C). Although they were not examples of security breaches involving VeriChips, they were used to illustrate that this type of technology has experienced security breaches. The Proposal makes it clear that it is referring to "RFID chip technology" in general. Shareholders should be allowed to vote on whether to be informed about possible adverse impacts before its use becomes more widespread.

As a matter of fact, the examples cited are all cases in which the manufacturer of the chip used cryptographic methods in an attempt to make it more secure and resist cloning, but it turned out to be possible to defeat that cryptographic security. The VeriChip does not use cryptographic security, so it actually is easier to clone than the examples.

The Proposal's statement that the unique "identification number could also be used to allow unauthorized people to enter restricted facilities" is completely accurate. Access to this number gives unauthorized users the opportunity to attack any other levels of security for a facility and if successful gain entry. Citing a hypothetical situation that is a definite possibility is not misleading. Furthermore, using a VeriChip as a means of access control is very similar to using a proximity card, such as the Exxon Mobile gas pass cited

as a security breach example. Once again, proximity cards use cryptographic techniques to prevent them from being cloned, making them much more difficult to clone than a VeriChip.

2. **Rule 14a-8(i)(7):** The Company argues that the Proposal deals with matters relating to ordinary business operations. The arguments presented are extremely confusing. On the one hand, the Company claims that the "Proposal is excludable because it directly relates to the Company's compliance with laws and regulations," stating that it is requesting the Board of Directors "to prepare what could be an extremely detailed and technical report 'on the harm that continued sale and use of RFID chips could have to the public's privacy, personal safety, and financial security.'" On the other hand, the Company claims that the Proposal does not seek to address significant social policy concerns because the Proposal's references to the "public's privacy, personal safety and financial security" are merely "cursory". Which is it? Is the Proposal's intent to protect the "public's privacy, personal safety and financial security" superficial? Or is it the subject of a report that could be "extremely detailed and technical"?

Obviously, the Company is attempting to have its cake and eat it too. In actuality, the Proposal is asking for a report on the adverse impacts the use of RFID chips could have on the public. Since this is the substance of the resolved clause, it could hardly be considered 'cursory." In addition, the resolved clause does not make any mention of legal compliance or financial assessment. No such demands are made on the Board. The only place the Proposal refers to the assessment of legal and financial impacts is in the supporting statement in reference to the shareholders. While shareholders might be interested in the public's safety as humanitarians and certainly their own safety as members of the public, they would definitely be concerned about the legal and financial consequences of negative social impacts as owners of the Company. It seems reasonable for the Company to provide a report on just what those impacts may be.

In Staff Legal Bulletin No. 14C (CF) issued on June 28, 2005, it states, 'To the extent that a proposal and supporting statement focus on the company engaging in an internal assessment of the risks or liabilities that the company faces as a result of its operations that may adversely affect the environment or the public's health, we concur with the company's view that there is a basis for it to exclude the proposal under rule 14a-8(i)(7) as relating to an evaluation of risk." This Proposal does not ask the Company to engage in any internal assessment of risks. It is only asking for a report on adverse public impacts.

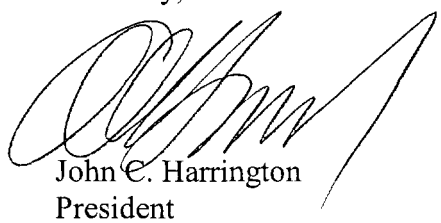
This year it appears to be very fashionable for companies to argue that a shareholder proposal is excludable as ordinary business because it "relates to the Company's compliance with Laws and Regulations." All companies and all individuals are subject to rules and regulations. The FDA does regulate medical products and devices; however, RFID microchips are a completely new technology which bears ethical considerations not normally dealt with by the FDA. The potential for abuse is so high that this product requires more than merely traditional technical review.

The "public's privacy, personal safety and financial security" are not cursory references. They are the focus of the Proposal. They are also the focus of the media and the legislature in regard to RFID usage; RFID legislation has been introduced in several states, including New Hampshire, California., Alabama, Illinois, Missouri, New York and Washington. Asking for a report on adverse impacts on the "public's privacy, personal safety and financial security" is not ordinary business; there could not possibly be more of a public policy issue than the use of RFID microchips.

3. **Rule 14a-8(i)(10):** The Company asks the Commission to omit the Proposal pursuant to this rule because they claim they have already "substantially implemented" the elements of the Proposal, listing initiatives undertaken for privacy protection. However, a report to shareholders on the potential impacts of RFID technology is not included anywhere on this list. In fact, the information page on the Company's website explaining the privacy policy mentioned in the list is very general and contains misleading information (i.e., "VeriChip subscribers are able to have their chip removed and discontinued at any time."). Clearly, shareholders concerned about the threat these products may pose to the public, and, therefore, their company, deserve more detailed and accurate information.

I respectfully urge the Commission to allow shareholders of Applied Digital Solutions the right to vote on this important policy issue at its 2006 Annual Shareholders' Meeting.

Sincerely,



John C. Harrington
President

Cc: Michael Krawitz, General Counsel, Applied Digital Solutions, Inc.

Wired News
Friday, May 22, 1998

&

Pirates Cash In on Weak Chips

by James Glave, james@wired.com

An extensive and well-organized phone-card piracy scam that came to light this week in Germany has proven a multimillion dollar lesson in the perils of hiding sensitive data rather than encrypting it, a German computer security group said.

"What I think people can learn from this is how expensive 'security by obscurity' can be", said Andy Mueller-Maguhn, spokesman for the Chaos Computer Club.

Earlier this week, the German weekly newsmagazine *Focus* reported that scam artists from the Netherlands had flooded Germany with millions of illegally recharged telephone debit cards. The cards, designed for Deutsche Telekom payphones, use a simple EEPROM chip, developed by Siemens Corp., that deducts value from the card as minutes are used up.

Ordinarily, once the credit balance reaches zero, the cards are thrown away or given to collectors. But the Dutch pirates found a way to bypass the simple security and recharge the cards without leaving any physical evidence of tampering. The pirates bought up thousands of spent cards in bulk from collectors, recharged them, and resold them cheaply to tobacco shops and other retail outlets across Germany.

The magazine said that the German association of tobacconist wholesalers assesses the losses at DM60 million, or US$34 million dollars.

With revenues last year of close to US$38 billion, Deutsche Telekom AG is Europe's largest telco and the third largest carrier worldwide.

But according to Mueller-Maguhn and other card experts, the Dutch piracy operation is only the latest, albeit the most widespread, scam against Deutsche Telekom, which has encountered security problems with its cards since they were introduced in the 1980s.

A spokesperson for Deutsche Telekom handling the card piracy issue did not return Wired News phone calls. It is not known if the pirates are in custody or still at large.

According to Marcus Kuhn, a smart-card physical security expert at Cambridge University in the United Kingdom, the first generation of phone cards did not include any encryption, and were easily modified.

"Anyone who observed, with a logic analyzer, the data traffic between a card and a public phone could fully understand the protocol and implement it on a simple microcontroller plus very little auxiliary logic", said Kuhn.

Kuhn and Mueller-Maguhn said the flawed card was replaced in March 1995 with the current model, which contains another Siemens chip, the SLE4433 -- commonly known as the "Eurochip". Though the Eurochip does contain some simple cryptography, the pirates soon heard about a bug hidden in the hardware that could allow the stored value to be reset.

"[The Eurochip] has a bug in the chipmask, allowing [a cracker] to reload almost all the bits using an

Exhibit A

normally unused counter", said Mueller-Maguhn.

Kuhn said that he examined the flawed Eurochip under a microscope about six months ago, and saw what he described as "a typical lowest-cost cryptoalgorithm".

Siemens declined to speak with Wired News for this story, other than to release a brief statement.

"Siemens has devoted considerable resources to the development of leading-edge chip card technology, as well as to cutting chip development cycle time in an ongoing effort to identify possible security issues in next-generation technology", the statement said.

Mueller-Maguhn and other sources made it clear that the Dutch pirates were not technically adept crackers or hackers. Rather, he said, they were con men who likely bought the know-how, or hired the person who discovered the bug, and then bought spent phone cards from collectors to reload them in the Netherlands.

"Codebreaking is not an adequate description for this kind of attack, as it relies on simple electrical engineering errors in the chip layout and not on cryptoanalysis", said Kuhn.

"These people weren't hackers, they did it solely for the money", added Andreas Bogk, another member of the Chaos Computer Club.

In the meantime, there is little Deutsche Telekom can do to stop the scam, because cracked cards are indistinguishable from the real thing, and the costs of tracking the pirate cards are prohibitive. Siemens and Deutsche Telekom are reportedly working on a new version of the Eurochip, called Eurochip2.

But Mueller-Maguhn said that he isn't holding his breath that the companies will get it right on the third time.

"Deutsche Telekom doesn't seem to learn about this in the chip-card business", he said. "They used [security by obscurity] in the first technique, then changed to security by obscurity in the second technique and now [will likely] do it the third time", Mueller-Maguhn said.

"We'll have fun engineering the bugs in the Eurochip 2", he added.

PCWORLD Computing Center

About

Does Your Car Key Pose a Security Risk?

RFID chips in keyless entry systems and ExxonMobil's Speedpass can easily be hacked, study finds.

Erin Biba, Medill News Service

WASHINGTON-- Security and convenience don't always go hand in hand. That may be the painful lesson for people who use an ExxonMobil Speedpass to purchase gas or keyless entry systems to get into their cars.

It may be cheap and easy to hack a widely used RFID chip created by Texas Instruments and installed in a variety of car keys, including models made by Nissan and Toyota, and Ford models from 2003, 2004, and 2005, a recent study found. That RFID chip is also used in the ExxonMobil Speedpass, a key-tag that wirelessly completes transactions at gas pumps. According to Texas Instruments, almost 150 million chips exist in car keys and key-tags throughout the country.

The study was conducted by Johns Hopkins University and RSA Laboratories, and came about simply because researchers were curious. "One of us had a Speedpass and wondered how secure it was," says Avi Rubin, professor of Computer Science at Johns Hopkins University's Information Security Institute. In the end, Rubin says, the group was surprised by what they found.

RFID Security Is Weak

With just "a few hundred dollars worth of equipment," Rubin says his team was able to wirelessly interact with car keys and payment tags at close range, and obtain enough information to crack their security system. They could then create a clone of the device, he says. This clone would allow someone to purchase gas on a victim's key-tag or disable a car's alarm system, but would not allow you to unlock a car's doors, Rubin says.

The chips tested during the study were more advanced than those that exist in older cars, Rubin says. "The one that we broke is the latest and greatest," he says, adding that older cars have weaker security systems that could be easier to hack into.

No Intention to Change

ExxonMobile acknowledges the potential security problems with the Speedpass device. "Bottom line, we are aware of it," says Don Turk, a company spokesperson. Still, the company does not have any plans to change the internal Texas Instruments chip or upgrade their current security systems at this time, he says.

"There are additional security protections for our consumers in the Speedpass system," says Turk. Unlike a credit card, a Speedpass does not store consumer data, so thieves would not have access to personal information, he says.

ExxonMobil Speedpass also guarantees that consumers will not be held liable for any fraud committed against their accounts, Turk says.

According to Texas Instruments, consumers have little cause to be concerned. The

Exhibit B

company has made upgrades to the RFID chip that the Johns Hopkins researchers tested, says Gary Silcott, an RFID spokesperson for Texas Instruments.

"We're evolving beyond that product," he says. Additionally, Silcott says, "There's a much greater security threat and a much greater instance of fraud on magnetic-stripe credit cards."

A Simple Fix?

Ultimately, Rubin and his fellow researchers say the best way to fix the problem would be for developers to "just design their future systems more securely." However, Rubin says, there is recourse for consumers who already have the devices.

"The best thing we could think of was to wrap your Speedpass in foil or metallic covering," Rubin suggests. "It's kind of a silly recommendation, but I think it would work." The foil would, of course, have to be removed before using the Speedpass at a gas pump.

Rubin says the same method would work for a car key: "If somebody can't send a signal to your key, then they won't be able to get a response back," and in turn will not be able to crack its security measures.

To print: Select File and then Print from your browser's menu

News Story

French Banks Hacked

By: Sylvia Dennis, Newsbytes
March 11, 2000
URL: http://www.computeruser.com/news/00/03/11/news4.html

An unknown hacker or group of hackers caused havoc in French banking circles late this week after the 96-digit encryption algorithm underlying the Cartes Bancaires system was posted on the Internet.

Some sources suggest that the code was posted to several Usenet group conferences, with widespread pickups by the media and other interested parties in France.

Cartes Bancaires (CB) has assured its customers - which include the majority of banks and their smart card bank card users in France - that the system is still safe.

However, Newsbytes' sources suggest otherwise. The release of the encryption code effectively allows fraudsters to create dummy smart card bank cards that contain account details that match the checksum system applied to the interbank card system.

Similar, but much lower security, checksum protection systems are seen on the Visa and MasterCard card systems. On these cards, the card verification value (CVV) - the three digit "extra" number printed on the Visa/MasterCard signature strip - is the most obvious result.

On the CB system, however, the checksum and other encrypted protection code is buried deep within the smart card's processor and allied chipset.

This has caused many banks and merchants using the CB to rely on the checksum and system integrity far more than when using the conventional magnetic stripe Visa/MasterCard series of cards.

CB has assured bank customers that their money is safe in their accounts, but Newsbytes' sources suggest that forged cards - which can draw money out of random accounts - could be created and used for making small "offline" transactions, such as when buying train tickets, making phone calls or paying for parking tickets.

Herve de Lacotte, a spokesperson for CB, is quoted by the Reuters newswire as saying that, for the first time since the CB system was created a decade ago, a lock has been sprung.

"But springing a lock will not necessarily open the door and let you in. There is a theoretical risk of fraud but the problem concerns banks, not consumers or shops," he said.

Newsbytes' security sources, who wish to remain anonymous, confirmed this assertion, saying that the majority of CB card numbers which can be generated using the system hack, will not represent real bank accounts at all.

"This is where the online/offline aspect of the system comes into play. For small value transactions, the CB card is offline, but for larger values, the transaction is authorized online. If the account details are not genuine, the online transaction will be refused," said the source.

Today's French press, however, takes a different view, with many reports saying that as many as 75 percent of France's 34 million CB/smart card-enabled bank cards could be compromised.

Exhibit C

Sefe Humpich, the crypto expert who last month got off with a suspended prison sentence for demonstrating how easy it was to create forged cards, said that the release of the code on the Internet meant that a chip card kit costing under $400 could generate many different CB cards.

Humpich narrowly escaped a jail sentence in late February after a public demonstration of his techniques in 1998 led to his arrest.

The 26-year-old computer engineer, who had earlier offered his security consultancy services to the GIE-CB organization, escaped with a suspended prison sentence, following his 1998 arrest in which he publicly demonstrated it was possible to buy 20 Paris Metro subway tickets using a self-manufactured card.

In earlier court appearances, Humpich became something of a folk hero as he battled against GIE-Carte Bleue in what soon became a "David and Goliath" case.

The computer engineer said that he had discovered a major flaw in the smart card payment system that would allow him to draw as much as $10,000 an hour from French cash machines for an indefinite period - as long as the cash machines were full, of course.

GIE-CB brought the fraud proceedings against Humpich after it realized that his actions could bring down the French payment card system.

Reported by Newsbytes.com

Click to **Home Page** | **Daily News** | **Dictionary** | **Current Issue** | **Prior View**

DIVISION OF CORPORATION FINANCE
INFORMAL PROCEDURES REGARDING SHAREHOLDER PROPOSALS

The Division of Corporation Finance believes that its responsibility with respect to matters arising under Rule 14a-8 [17 CFR 240.14a-8], as with other matters under the proxy rules, is to aid those who must comply with the rule by offering informal advice and suggestions and to determine, initially, whether or not it may be appropriate in a particular matter to recommend enforcement action to the Commission. In connection with a shareholder proposal under Rule 14a-8, the Division's staff considers the information furnished to it by the Company in support of its intention to exclude the proposals from the Company's proxy materials, as well as any information furnished by the proponent or the proponent's representative.

Although Rule 14a-8(k) does not require any communications from shareholders to the Commission's staff, the staff will always consider information concerning alleged violations of the statutes administered by the Commission, including argument as to whether or not activities proposed to be taken would be violative of the statute or rule involved. The receipt by the staff of such information, however, should not be construed as changing the staff's informal procedures and proxy review into a formal or adversary procedure.

It is important to note that the staff's and Commission's no-action responses to Rule 14a-8(j) submissions reflect only informal views. The determinations reached in these no-action letters do not and cannot adjudicate the merits of a company's position with respect to the proposal. Only a court such as a U.S. District Court can decide whether a company is obligated to include shareholder proposals in its proxy materials. Accordingly a discretionary determination not to recommend or take Commission enforcement action, does not preclude a proponent, or any shareholder of a company, from pursuing any rights he or she may have against the company in court, should the management omit the proposal from the company's proxy material.

April 25, 2006

Response of the Office of Chief Counsel
Division of Corporation Finance

Re: Applied Digital Solutions, Inc.
Incoming letter dated March 31, 2006

The proposal requests that the independent directors of the company's board prepare a report, at reasonable cost and omitting propriety information, on the harm the continued sale and use of RFID chips could have to the public's privacy, personal safety, and financial security.

There appears to be some basis for your view that Applied Digital Solutions may exclude the proposal under rule 14a-8(i)(7) as relating to its ordinary business operations (i.e., product development). Accordingly, we will not recommend enforcement action to the Commission if Applied Digital Solutions omits the proposal from its proxy materials in reliance on rule 14a-8(i)(7). In reaching this position, we have not found it necessary to address the alternative bases for omission upon which Applied Digital Solutions relies.

Sincerely,

Ted Yu
Special Counsel