1-2006

Practicing CPA, vol. 30 no. 1, January 2006

American Institute of Certified Public Accountants (AICPA)

The Practicing CPA

PCPS AICPA Private Companies Practice Section

www.pcps.org

THE NEWSLETTER OF THE AICPA PRIVATE COMPANIES PRACTICE SECTION

Inside

Wrestling With the Wireless World

Wireless technology has many obvious benefits, among them freedom from the constraints of the desktop. Furthermore, associated reduced cost benefits are attractive — consider the savings of not having to wire the office, and if your firm is new, of being up and ready in a hurry. In addition to these benefits, using wireless technology offers the cachet of being forward-looking. However, some risks accompany these benefits. To help CPAs and their clients to understand the benefits and risks of using wireless technologies in their home offices, public places, and throughout their business enterprises, the AICPA Information Technology Section published A CPA's Guide to Wireless Technology and Networking *(New York: AICPA 2005). The following article, adapted from the book, focuses on the risks associated with wireless technology. The author is Michael R. Dickson, CPA, CITP, a technology consulting and solutions practice manager in the Southfield, MI, office of Plante & Moran, PLLC. In this publication, he discusses radio wave frequencies used by wireless devices, types of wireless networks, wireless devices and network adapters, and wireless standards. In addition to describing wireless security risks, Dickson suggests best practices for securing a wireless network. The products, standards, and practices referred to are based on Dickson's knowledge and experience, as of spring 2005.*

Wireless technologies exist all around us, opening up new ways to communicate and work. Today's wireless technologies enable us to connect with our home and business computer systems from any location around the planet, including offices, beaches, backyard pools, cars, trains, and local coffeehouses. Congress is even discussing opening up wireless networks on board aircraft at cruise altitudes.

Wireless technology is fascinating and can improve the productivity of people and the efficiency of processes. It facilitates the extension of computer networks to areas in which wired networks are cost prohibitive or the business process cannot be supported by a wired connection. Wireless technology is being integrated into core business processes in nearly every industrial sector. In the accounting profession, wireless technologies are deployed by audit teams at client sites, providing instant collaborative networks that support automated working papers and access to client data stored back in the CPA firm's data repository.

Every enabling technology has benefits, costs, and risks. Wireless technology certainly has its share of all three. The cost of wireless technology is falling dramatically, and the capability of wireless devices is improving exponentially. It is easy to predict that, as these two trends combine, the use of wireless technologies will

continued on next page

become the status quo, rather than the leading edge of networking technology. Nevertheless, the true value of these advantages must be weighed within the context of the increased risk associated with the use of wireless technology. To help you better understand wireless technologies, we must discuss their unique risks.

Wireless network security

The security risks in a wired world continue to exist in a wireless environment. Going wireless, however, increases security risks significantly. The advantage of wireless is that any device within 300 feet can be connected, which is also a danger if a device within a wireless perimeter is not authorized to access the wireless network. The sections that follow describe some, but not all of the risks of using wireless networks. These risks apply to most of the wireless standards and network types discussed.

Unauthorized access

In a wired network, the risk that an unauthorized person could gain access to the network is mitigated by physical security controls. Examples of such physical access controls include locating wiring closets in nonpublic, secure locations; restricting access by unauthorized persons from areas of the building in which active network ports exist; and disabling network ports except on a specific as-needed basis in public areas. Although these controls are generally considered quite effective for wired networks, they may not be effective for a wireless network. Locating wireless access points (APs) in a locked closet is good practice to prevent theft or tampering with the device itself, but, because of the nature of the wireless medium, the network signals are likely to be broadcast beyond the physical location of your home or business. If you are in a multitenant office building, how do you prevent people you cannot see from receiving the radio transmissions that are going into their suite? Likewise, how do you restrict your neighbor, someone across the street in a high-rise building, or someone just driving down the street from accessing your network? There is no single answer on how to prevent unauthorized access to your wireless networks; however, some tips and suggested practices are provided in the following discussion.

Data transmissions easily intercepted

As discussed above, the risk that wireless data could be broadcast to unintended users is significant in a wireless network. Therefore, additional precautions may be necessary to protect the confidentiality and integrity of data. The practice of encrypting data to prevent an unauthorized user from seeing or being able to change data is a desirable practice in most wired enterprise networks, but it is absolutely necessary in a wireless network to protect the confidentiality and integrity of the data being transmitted wirelessly.

Denial of service attacks

You must understand the risk of denial of service (DoS) attacks against a wireless network AP. Most DoS attacks involve hackers calling upon hundreds or thousands of compromised PCs to attempt to connect to a target mail or Web server at a specific date and time. Because of Internet protocols, the default response for each hacker inquiry is to send an acknowledgment. If a target computer receives hundreds or thousands of requests that require an acknowledgment in a short period of time, the target machine's processing capability is overloaded, thus preventing other legitimate users from logging in.

In the wireless world, you are unlikely to have hundreds or thousands of wireless hackers trying to attack your AP because the attackers need to be within 300 feet of the AP to attempt a connection. But, the wireless AP is vulnerable to DoS attacks initiated from wireless devices within the enterprise and from other "wired users" attacking unprotected wireless local area network (WLAN) facing ports.

Unauthorized access points

One reason why wireless networking has been so widely adopted is that it is so easy to install. Anyone can create a quick wireless network simply by plugging an AP into an available network port. The devices are very low cost (some under $50) and their default configurations right out of the box will self-configure a working wireless network. Moreover, if you have an 802.11 (see box) wireless-enabled device in range, your computer will likely automatically establish a connection with the AP, all without user intervention. Not only is it easy to set up, but unless your network administrators have enabled some advanced security features on the WLAN, they may not even be able to detect that an unsecured wireless network has just been directly connected to the enterprise network.

> 802.11 is a family of specifications for wireless LAN technology developed by the Institute of Electrical and Electronics Engineers (IEEE). It represents the most widely implemented WLAN standard because of its range and speed characteristics.

continued on next page

The Practicing CPA **(ISSN 0885-6931) January 2006, Volume 30, Number 1. Publication and editorial office: Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311-3881. Copyright 2006 AICPA. Printing and mailing paid by PCPS/The AICPA Alliance for CPA firms. Opinions of the authors are their own and do not necessarily reflect policies of the AICPA.**

Editor: **William Moran.**

Because wireless components are so inexpensive, many employees have wireless networks at home. This gives them great confidence that they can plug in an AP to the enterprise network port and move their computer from their desk into the nearby conference room. Employees rationalize that "being wireless enhances productivity," without realizing that they have instantly created a significant breach in the security of the enterprise network.

Loss or theft of wireless devices

Whenever computing resources are distributed throughout an organization, often in distant or remote locations, the risk of "losing" computers or having them stolen is very significant. For wireless devices, the risk of loss or theft is compounded since they tend to be small and mobile. Furthermore, we are not concerned just about the device. Wireless devices provide connections to network resources, and often they contain confidential enterprise data. Remote and mobile devices are more likely to have confidential enterprise data than fixed workstations that are always connected because remote and mobile computers often have to work in both a connected and a disconnected mode. When working in a disconnected state, remote computers need cached (or locally stored) data.

The best example is a laptop computer used by a field marketing representative or a traveling executive. When in the office and connected directly to the enterprise network, the employee may directly access shared files on a server or access a centralized mail server. However, because of the design of remote and mobile applications, large amounts of data may be downloaded to the laptop. If the employee is on a cross-county flight or in client facilities where access to the files back at the office is not possible, he or she will have the data stored on the local machine that allows him or her to be productive. This capability is the essence of the breakthrough vision of applications like Lotus Notes, whereby developers wanted users not connected to enterprise networks to be able to do everything they could when they were connected! Indeed, Microsoft's Outlook also works this way; server-based files are replicated and synchronized on the portable computer so that the user can read messages and attachments when disconnected.

A wireless network can be secured. A wide range of security products are available, but they are an additional cost. As we have seen, most technology becomes less expensive and more robust. Nevertheless, CPA firms and their clients need to decide whether the ease of installing and deploying wireless technology offsets the investment and associated risks.

Resources on Wireless Technology

A CPA's Guide to Wireless Technology and Networking **by Michael R. Dickson, CPA, CITP (To obtain this, visit *www.cpa2biz.com*, or call 1-888-777-7077 and ask for product no. 889585. AICPA member price: $29; nonmember price: $36.25.**

Note: Members of the AICPA Information Technology Section were sent a gratis copy of this publication as a member benefit.

SANS (SysAdmin, Audit, Network, Security) Institute White Papers
Understanding Wireless Attacks and Detection
www.sans.org/rr/whitepapers/casestudies/1633.php

Security Vulnerabilities and Wireless LAN Technology
www.sans.org/rr/whitepapers/casestudies/1629.php

PCPS Firm Practice Center Unlocks Premium Web Content

The PCPS Firm Practice Center (http:// www.aicpa.org/pcps) has temporarily opened its premium content, to everyone, including nonmembers. The premium content covers a variety of practice management topics and comes from noted professionals in the field. Through mid-May, visitors to the site can view articles, tools, technical updates, and other resources (all marked with a padlock icon) previously available to PCPS members only. While at the Firm Practice Center, visitors can also look at descriptions of numerous AICPA and PCPS products and events.

The normally restricted content is free to all for now, but if CPAs would like to continue their access to these resources, their firms will need to join PCPS. To learn more, visitors can go to *http://pcps.aicpa.org/Memberships/Join+PCPS.htm* or click the "Join PCPS" button on the Firm Practice Center's home page. Membership costs $35 annually per CPA, up to a maximum of $700. Firms can also contact 1-800-CPA-FIRM or pcps@aicpa.org.

Once the premium content is restricted again, those firms that are already PCPS members can continue to view it for free.

Corporate Fraud Increases in Number and Types

Fraud is increasing. That's the bad news coming out of a recent PriceWaterhoueCoopers' survey on economic crime. The good news is that the detection of fraud may be increasing also. More bad news: Companies may be underestimating their vulnerability and are not anticipating ways to foster corporate integrity and fraud prevention. In addition, despite the success of whistle blowing programs in detecting fraud, relatively few companies have implemented them.

According to the widely reported PWCs' Global Economic Crime Survey 2005, rising economic crime poses a growing threat to companies. Nearly half of all organizations worldwide, including U.S. companies, report that they've been the victims of economic crime in the past two years. Globally, the number of companies reporting fraud increased from 37% to 45% since 2003, a 22% increase. The cost to companies was an average U.S. $1.7 million in losses from tangible frauds, those that result in an immediate and direct financial loss, such as asset misappropriation, false pretences, and counterfeiting.

The survey also showed increases in the various types of fraud that can affect a company, from asset misappropriation to counterfeiting. Globally, there has been a 140% increase in the number reporting financial misrepresentation, a 133% increase in the number reporting money laundering, and a 71% increase in the number reporting corruption and bribery.

According to PWC, the 22% increase in companies reporting economic crime since 2003 may be attributed to:

- More incidents of economic crime being committed
- Increased economic crime reporting due to tighter regulations requiring increased transparency
- The introduction of risk management controls to detect economic crime
- A "confess and remedy" environment among regulators that encourages economic crime reporting

Regardless of size, no company or industry, regulated or unregulated, was found to be immune to fraud. (Surveyors focused on a random selection of the largest thousand companies in a country.)

Letters to the Editor

The Practicing CPA **encourages readers to write letters on practice management and on published articles. Please remember to include your name and telephone and fax numbers. Send your letters by e-mail to pcpa@aicpa.org.**

Economic crime detection

Internal controls fail to detect economic crime 60% of the time in the United States; however, internal audit is cited as the single most effective control mechanism, detecting just over 30% of the reported cases in North America and 26% of the reported cases globally.

A false sense of security?

Despite the growing number of companies reporting fraud around the world, nearly 80% did not consider it likely that their company would suffer fraud over the next five years. "Companies may have a false sense of security when it comes to fraud. More companies are reporting financial crimes, they're reporting a higher number of incidents, and most cases are detected by accidental means," said Steven Skalak, PWC's Global Investigations Leader,

Contrary to the optimistic view of the 80% of PWC respondents, the 2005 Oversight Systems Report on Corporate Fraud concludes, "while most fraud examiners view the Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley or SOX) as an effective tool in fraud identification, few think it will change the culture of business leaders." A further conclusion of Oversight Systems' survey of fraud examiners is, "although respondents agree that SOX serves to identify fraudulent activity, they do not believe that the recent cultural change among U.S. business leaders toward institutional integrity and fraud prevention in the wake of accounting scandals will stick." Only 17% of respondents believed that business leaders will maintain interest in company integrity and fraud prevention. (The Oversight Systems report is available on the AICPA Web site's AICPA Antifraud and Corporate Responsibility Center. See the sidebar on page 5 for the Web address.)

FYI

PCPS, the AICPA alliance of the CPA firms, represents more than 6,000 local and regional CPA firms. The goal of PCPS is to provide member firms with up-to-date information, advocacy, and solutions to challenges facing their firms and the profession. Please call 1-800-CPA-FIRM for more information.

continued on next page

PWC's conclusions that a "confess and remedy" culture contributes to fraud detection and that most cases are detected by accidental means are supported by the results of a 2004 study conducted by the Association of Certified Fraud Examiners (ACFE). The study involved 508 cases investigated by certified fraud examiners (CFE), many of whom are CPAs. In a presentation at the AICPA National Fraud and Litigation Services Conference in Dallas on September 29–30, 2005, Toby Bishop, CPA, CFE, FCA, president and CEO of ACFE discussed the role of whistleblower programs in contributing to corporate environments that may foster fighting fraud or other wrongdoing. Citing the "ACFE 2004 Report to the Nation on Occupational Fraud and Abuse," Bishop reported that the method of initial detection of occupational frauds was most frequently an employee tip. Such tips accounted for 39.6% of initial detections. Other detection methods included internal audit (23.8%), accidental discovery (21.3%), internal controls (18.4%), external audit (10.9%), and police notification (0.9%). Bishop also cited evidence that employee hotlines and other means to report fraud anonymously can reduce fraud losses by half. According to the survey, in 2004, the median loss in organizations without a hotline was $135,500, more than twice the median loss of $56,500 in companies with hotlines.

Implementation of hotlines lags

Despite the effectiveness of anonymous hotlines as an anti-fraud or fraud detection method, only 36.8% of companies surveyed in 2004 had an anonymous hotline. An effective whistleblower program, according to Bishop, requires, in addition to the hotline itself, educating employees, vendors, customers, and others about the hotline and its purpose. Inclusion of others in a comprehensive ongoing education program results in 50% more calls. Other channels for reporting wrongdoing should also be available, such as the organization's Web site or a post office box.

Another critical element is a program for evaluating the calls received. Such a program should include a case management tracking system and established protocols for investigating complaints, as well as protocols for distributing reports of action, and a system for automatically informing the board and the audit committee of major issues

Profile of the Fraudster

In the United States and North America, the PWC survey found that 79% of corporate "fraudsters" are males between the ages of 31 and 40 who have college or higher degrees; 60% were employed by the defrauded company, 47% were in a managerial capacity.

Fraud and Commercial Crime Resources

AICPA Web site
AICPA Antifraud and Corporate Responsibility Center
www.aicpa.org/antifraud/homepage.htm

Publications
The CPA's Handbook of Fraud and Commercial Crime Prevention by Ted Avey, CPA, CFE, CA, Ted Baskerville, CA, and Alan Brill, CISSP. (New York: AICPA), one-volume loose leaf.
Price: $180 AICPA members;
$229 nonmembers. Product no. 056504
To order: call 1-888-777-7077 or visit ***cpa2biz.com***

Anonymous Submission of Suspected Wrongdoing (Whistleblowers): Issues for Audit Committees to Consider
www.aicpa.org/audcommctr/spotlight/jan_05_whistleblower.htm

White Paper: Best Practices in Ethics Hotlines
www.ethicsline.com/news/default. asp

"Fraud Hotlines: Early Warning Systems," The Practicing CPA (November 2003)
http://www.aicpa.org/pubs/tpcpa/nov2003/fraud.htm

Fraud Surveys
A copy of the PWC report can be found at:
www.pwc.com/crimesurvey.
Other surveys include:
2004 Report to the Nation on Occupational Fraud and Abuse
www.cfenet.com/resources/rttn.asp

2003 KPMG Fraud Survey
www.us.kpmg.com/services/content.asp?11id=10&12id=30&cid=1695

PCPS
AICPA Private Companies Practice Section
Update

Dear PCPS Members:

Happy New Year!

As we kick off a new year of fresh possibilities and opportunities, we plan to build on the many accomplishments of 2005, as well as our 28 years of history serving CPA firms.

2005: The Year in Review

PCPS had one of its most successful years in 2005. As the AICPA's community for firms, PCPS launched a brand new online Firm Practice Center at *www.aicpa.org/pcps*; rolled out several major initiatives around succession planning, financial literacy and staffing; appointed a number of talented new practitioners to the Executive Committee; and changed its name back to Private Companies Practice Section. PCPS has never been better positioned to offer its 6,000 member firms a wealth of management resources and innovative, informative conferences and symposiums. PCPS achieved a great deal in 2005 to fulfill its tenet of making CPAs and their firms successful.

Here are the highlights of the many resources PCPS offered its members in 2005:

Valuable Products and Services

We presented a broad array of tools and programs for practices throughout the year, including the following:

- A New Community for Firms on the Web: PCPS unveiled its new Firm Practice Center (*www.aicpa.org/pcps*) in June. The center provides practices with a more comprehensive collection of management tools, news, and resources and is specifically designed for local and regional firms. It contains a wide range of information on everything from recruiting and retention to marketing and practice growth to Network Groups. You'll not only find the latest articles on the industry's hottest issues, but also great new tools and checklists, free downloadable brochures, and more. Also, to increase membership, along with access activation to the site by current members, we have unlocked the premium content for a limited time so that all visitors can view it. Once we relock it, those members who already have activated their access will continue to be able to view the premium content.

If you haven't already activated your access, please do so today by contacting the AICPA Service Center at 1-888-777-7077 or service@aicpa.org.

- The Succession Planning Initiative: PCPS released an extensive series of succession planning tools in 2005, including these:
  - —A comprehensive book by noted firm consultant Bill Reeb, CPA, titled *Securing the Future: Building a Succession Plan for Your Firm.*
  - —A CPE Course (DVD and manual) titled *"Succession Planning: Strategies to Protect the Value of Your Firm,"* also from Reeb.
  - —Webcasts such as *"Succession Planning for Valuation Services Firms," "Succession Planning: Positioning Your Firm for Successful Transition"* and *"Succession Planning: Strategies to Facilitate Transition & Increase Firm Value."*
  - —Preparing for Transition: *The State of Succession Planning and How to Handle the Process in Your Firm*, a white paper that has been among the most popular resources at the PCPS Web site. Nearly 10,000 CPAs downloaded the paper when it was unveiled in September. You can find it at ***pcps.aicpa.org/Resources/Succession+Planning/.***
  - —A wide range of other succession content at the Firm Practice Center.
- Help for Hurricane Victims: Together, PCPS and the AICPA established an online Firm Volunteer Center to provide resources for firms affected by Hurricanes Katrina, Rita, and Wilma. Approximately 400 firms volunteered such resources as office space and supplies, along with accommodations for affected firms' staff and clients. If your practice was affected by one of the hurricanes, go to ***pcps.aicpa.org/Community/Firm+Volunteer+Center.htm*** to access the Firm Volunteer Center. Select the resource you need and you will see a list of volunteer firms.
- 360 Degrees of Financial Literacy: To enhance the AICPA's 360 Degrees of Financial Literacy program in 2005, PCPS offered a free "Primer to Financial Literacy," a customizable turn-key PowerPoint presentation that firms can offer to their clients' employees. The presentation is designed to make it easy for practices to offer a free two-hour course on this subject. The presentation is available in the "Resources" section of the PCPS Firm Practice Center at ***www.aicpa.org/pcps***. Click the "Resources" tab, then the "Financial Planning" link, then the "Personal" link.

continued on next page

Membership in PCPS is more valuable than ever. Join now for $35 per CPA, up to a maximum of $700, by visiting ***pcps.aicpa.org/Memberships/Join+PCPS.htm*** or by going to ***www.aicpa.org/pcps*** and clicking the "Join PCPS" button on the home page.

If you are already a member but haven't activated your access to the online Firm Practice Center or haven't shared your unique activation link (sent to you this past summer) with others in your firm, now is the time to do so. Contact the AICPA Service Center at 1-888-777-7077, Option 3, or at ***service@aicpa.org*** for assistance or for more information.

continued from page 7

- **The CPA Exam:** Because participation in the CPA Exam dropped 37% in 2004 (the first year of CBT, or computer-based testing), PCPS set out to reverse that trend in 2005. In working to do so, we created and e-mailed a number of resources for member firms' managing partners to use and pass on to others, including the following:
  - —An e-mail encouraging firms to encourage their new employees to take the exam early
  - —A spreadsheet for firms to track which employees have taken and passed the exam
  - —A sample exam policy that firms could adapt to encourage their new employees to take the exam
  - —A revised flier PDF on CBT with 10 reasons to take the exam, plus information on how to schedule. (This PDF was also shared with the AICPA teams that work with colleges.)
  - —A reminder e-mail that will go out quarterly to alert firms of the time needed for candidates to register for the exam, now offered two of every three months instead of just twice yearly. From initial application to testing, the registration process can take six to eight weeks.

  You can view these exam resources at ***pcps.aicpa.org/Resources/Staffing/Management+Issues/CPA+Exam.htm.***
- **PCPS MAP Network Groups:** Continuing its popular MAP Network Group program in 2005, PCPS held meetings for small, medium-sized, and large practices and introduced a second small firm group this fall. These meetings provide CPAs with an excellent forum for in-depth practice management discussions and the chance to exchange information on firm operations and professional issues. For example, the second small firm group, which met in Atlanta this past November, featured an in-depth "getting to know you" session, discussions about alliances and disaster planning (including not only natural catastrophes, but also the loss of key clients, staff, etc.) and a talk with CPA Jack Oppie of Mississippi, who shared his personal story about Hurricane Katrina. The meeting also included discussions on practice continuation agreements and billing rates, along with a best practices breakout session. To learn more about the Network Groups, visit ***pcps.aicpa.org/Community/Firm+Size+Network+Groups.htm.***
- **A New Recruiting and Retention White Paper:** We released *Best Practices in Recruiting and Retaining Talented Staff*, a white paper based on the findings from a recent survey of nearly 500 CPA firms. The paper is rich with information about staffing, the biggest management challenge facing firms. Visit ***pcps.aicpa.org/Resources/Staffing/Recruiting+and+Retention/Best+Practices+in+Recruiting+and+Retaining+Talented+Staff.htm*** to download a free copy of the paper. You can benchmark your efforts against those of your peers and take away a number of actionable tips for smaller firms.
- **PCPS/TSCPA National MAP and MAP Top 5 Surveys:** This year marked some changes for the PCPS/TSCPA National MAP Survey. PCPS decided to conduct it in even years only, in order to reduce the administrative burden on firms. Therefore, the next National MAP Survey will be in 2006. However, the research team identified new ways to mine the data we already have to create additional, useful extracts during the off-years for practitioners. The latest such report, completed in November, covers hiring season issues. The original extracts are available at ***www.aicpa.org/pcps***. Just click on the "Resources" tab and then the "National MAP Survey" link.

In October, PCPS rolled out its 2005 Survey of Top 5 Practice Management Issues to local and regional CPA firms across the nation, requesting them to rank the most important management challenges facing them today. The Top 5 issues are as follows in this order:

- Finding and retaining qualified staff
- Keeping up with changes and complexity of laws
- Seasonality/workload compression
- Client retention
- New regulations' effect on smaller firms and businesses.

Full results will be posted to the PCPS Firm Practice Center.

Representation

Besides offering numerous products and services, PCPS continued to engage in several advocacy activities for all CPA firms this past year. The programs and projects included:

- **The Private Company Financial Reporting Task Force:** Bill Balhoff, former chair of the PCPS Executive Committee and director at Postlethwaite & Netterville of Louisiana, has joined the AICPA/FASB working group exploring the process of improving private company financial reporting standards. Specifically, the working group will identify criteria for potential differences in accounting and the processes in which to make consideration of those differences happen. The AICPA expects to have a set of recommendations to present at the regional Council meetings this spring.
- **A Tax Update:** After extensive discussion, the PCPS Executive Committee determined that it does not support SSTS No. 9, Proposed Exposure Draft on Tax Standards, which would require CPAs to develop a written quality control system for preparing tax returns. The general consensus is that SSTS No. 9 is a very good set of best practices but should not be an enforceable standard. The AICPA Tax Section Executive Committee met at the end of October and voted unanimously to expose SSTS No. 9 from December 31, 2005, through August 31, 2006. Comments will be reviewed in September of the

continued on next page

continued from page 7

coming year. The Tax Section Executive Committee plans to vote on finalizing the standard at its November 2006 meeting and hopes for it to be final and published December 31, 2006, with a June 30, 2007, effective date.

- **The Technical Issues Committee (TIC):** The Technical Issues Committee is charged with representing local firms and their private-company, not-for-profit and government clients to standard setters and regulators. This committee worked hard on behalf of smaller firms in 2005, issuing more than 13 comment letters for the year—with six in August alone. For 2004, TIC issued 11.

TIC also recently announced its new members:

- Kenneth Osborn, Gordon, Harrington & Osborn, P.C., in North Andover, Mass.
- Rodney Rice, RubinBrown LLP in St. Louis, Mo.
- Former PCPS Executive Committee member Ray Roberts, Accounting & Consulting Group in Carlsbad, N.M.
- Darrell Wates, Tucker, Scott & Wates, LLC, in Decatur, Ala.

The new members joined TIC at its November meeting. Additionally, continuing TIC member Edward Knauf of DeJoy, Knauf & Blood, LLP, in Rochester, N.Y., has been named chair of the group.

2006: The Year Ahead

We welcome your input regarding the areas where your firm could use support as we embark on a new year. We use data from our membership survey to help guide our decisions, but we also depend on your firsthand feedback.

PCPS is here to help you and your firm succeed. Call 1-800-CPA-FIRM or e-mail *pcps@aicpa.org* to let us know your greatest concerns, as well as the benefits you see from us now and would like to see from us moving forward.

From all of us at PCPS, we wish you a happy and healthy New Year!

Regards,
Rich Caturano, CPA
Chair
PCPS Executive Committee

PCPS/The AICPA Alliance for CPA Firms
Harborside Financial Center
201 Plaza Three
Jersey City, NJ 07311-3881
(201) 938-3005
Fax (201) 938-3404

ADDRESS SERVICE REQUESTED

ISO Certified

Non-Profit Organization
U.S. POSTAGE
PAID
American Institute of
Certified Public Accountants