KAKIMOTO & NAGASHIMA LLP
CERTIFIED PUBLIC ACCOUNTANTS
CONSULTANTS

NEWSLETTER

Volume 4, Issue 2 July 2006

Inside this issue:

Any Questions?

We are committed to providing our clients with quality and excellent services. If you have any questions or comments, please let us know by either e-mail or phone. Our company profile is available on the internet at:

http://www.knllp.com

Los Angeles Office:
Tel: (213) 439-6800
E-mail: laoffice@knllp.com

South Bay Office:
Tel: (310) 715-9100
E-mail: sboffice@knllp.com

Summary of Articles

SOX Section 404 – Do You Have Things Under Control?

We move forward in a world of globalization; United States securities laws and regulations will have an impact on an international level. In the wake of its own corporate reporting scandals, Japan has recently introduced legislation which embodies, in substance, Sarbanes-Oxley Act (SOX) Section 404. SOX Section 404 is probably the toughest and most costly of the SOX provisions, which will take time and resources to comply with its many requirements. In this issue, we briefly summarize the major provisions of SOX Section 404.

Is your company subject to e-filing?

New temporary regulations for submitting corporate income tax return (Form 1120/1120S) were issued on January 12, 2005 by the Internal Revenue Service (IRS). The temporary regulations require certain large corporations and S corporations to file their income tax returns electronically. It is important that you understand how these new "e-file" requirements may affect your company. In this issue, we will provide a brief summary of the new regulations.

Cutting the cord. How safe is it?

Wi-Fi may be considered the best thing since sliced bread. The ability to roam free without the hassles of cords and wires is a great thing to have. But does this freedom come with dangerous side effects?

The IRS announced that it will stop collecting the federal excise tax on long distance services. Taxpayers will claim this refund on their 2006 tax return. This doesn't affect the federal excise tax on local telephone services. Refund claims will cover all excise tax paid on long distance service over the last three years. Interest will be paid on refunds. The IRS is working on a simplified method for individuals to claim a refund on their 2006 tax returns.

The Sarbanes Oxley Act: Section 404 – It's a Matter of Control

The enactment of the United States Sarbanes-Oxley Act of 2002 (the "Act") has brought forward many changes in how publicly traded companies conduct business. In an effort to mandate and promote corporate governance, the Act puts in place several provisions which require greater accountability for financial reporting practices. Although compliance with all of the Act's provisions have a direct impact on financial reporting practices, probably the toughest and most costly requirements are contained in Sarbanes-Oxley Act (SOX) Section 404.

We move forward in a world of globalization; United States securities laws and regulations will have an impact on an international level. In the wake of its own corporate reporting scandals, Japan has recently introduced legislation which embodies, in substance, SOX Sections 404 and 302/906 (corporate executive responsibility for financial reports/certifications by CEO/CFO).

The first wave of United States SOX Section 404 filers ("accelerated filers", generally companies with market capitalization equal to or greater than $75 million) has passed. "Small-cap" companies ("nonaccelerated filers") have compliance dates effective in fiscal years ending after July 15, 2007. Presently, the SEC is revisiting the possibility of full or partial exemptions from Section 404 for smaller size public companies.

SOX Section 404 highlights the investors' need to have confidence in the underlying processes and controls that are an integral part of producing financial reports issued by publicly held companies. Section 404 is concerned with the internal control over *financial reporting* which can be generally defined as:

> "*a process designed by, or under the supervision of, the company's executive and financial officers, or persons performing similar functions, and effected by the company's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles...*"

It should be noted that Section 404's definition does not encompass the internal control elements that relate to the effectiveness and efficiency of the company's business operations and compliance with applicable laws and regulations, with the exception of compliance with the applicable laws and regulations directly related to the preparation of financial statements.

SOX Section 404 Management Reporting/External Auditor Functions

Management is responsible for including an internal control report in the company's annual report which:

(1) States the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contains an assessment, as of the end of the company's most recent fiscal year, of the effectiveness of the internal control structure and procedures of the company for financial reporting.

The external auditor is responsible to perform the following in relation to a company's internal control over financial reporting (ICOFR):

- Evaluate management's ICOFR assessment methodology
- Evaluation of the effectiveness of the ICOFR system
- Testing of ICOFR processes
- Provide an attestation report on management's assessment of the company's ICOFR
- Audit committee/management communication of deficiencies/ weaknesses

Management Compliance with SOX Section 404

Management's responsibility for maintaining sufficient internal control structure and procedures for financial reporting is expressed in Section 404. Management's responsibility also includes assessing the effectiveness of the company's ICOFR; this assessment is attested to by the company's external auditors. Management should include the following actions in its compliance with Section 404.

Planning

Thorough planning should be involved in making an evaluation of the effectiveness of a company's ICOFR. A few of the planning considerations are:

- Identification of ICOFR
- Assessment process
- Documentation process
- Timelines; targets

Documentation and Evaluation

Documentation of the company's ICOFR system is a significant phase of the whole process. Documentation provides the evidence and support of management's assessment and the effectiveness of its ICOFR.

Testing of the ICOFR

Management should test key controls and document tests made. Deficiencies are to be identified, summarized and evaluated. Response and correction to deficiencies are to be performed.

Coordination of External Auditors/Reporting Requirements

The independent/external auditor will review the ICOFR system which includes the documentation, evaluation and assessment of the system. This will also include tests of the ICOFR for operation and effectiveness. Test results and conclusions are discussed with management and the audit committee. Both management and the external auditors will each prepare a report to be included in the company's annual report ("Form 10-K").

Japan's "Financial Instruments and Exchange Law" ("J-SOX")

Legislation which incorporates SOX Sections 404 and 302/906, in substance, had been introduced to the Japanese Diet on March 13, 2006 and passed on June 7, 2006. Actual procedural and regulatory guidance is anticipated to be issued in the fall of 2006. Companies expected to be affected are publicly-listed companies in Japan including their subsidiaries. Compliance could become effective for fiscal years beginning on or after April 1, 2008.

We encourage management to consider the time and resources required to comply with Section 404; a prompt response is necessary to prepare for and prevent deficiencies in staffing and resources. Please consult us if you should have any questions .♦

E-filing requirement: New Regulations for filing Form 1120 and 1120S

On January 12, 2005, the Internal Revenue Service (IRS) issued temporary regulations that require certain large corporations, including certain S corporations to file their income tax returns electronically beginning with tax periods ending on or after December 31, 2005.
Corporations with assets of $50 million or more and that file 250 or more returns per year (including income tax, excise and employment tax, as well as information returns such as W-2s and 1099s) are required to file their Forms 1120 or 1120S electronically for taxable years ending on or after December 31, 2005. The new e-file system brings benefits for both taxpayers and IRS such as the following:

- The ability to file more quickly, easily, and reliably;
- Faster, more accurate processing, and quicker interactions between IRS and taxpayers;
- Allowing the taxpayers to correct their return before the return is accepted; and
- The requirement to submit duplicate copies of certain forms is eliminated.

The Tax Year 2005 Corporate e-file Program does not accept certain corporate returns, including amended returns, bankruptcy returns, and Prompt assessments.

A waiver from the electronic filing requirement may be requested if the taxpayer demonstrates undue hardship such as technology constraints and financial burden.

To comply with the e-filing requirement, corporations using a tax professional to prepare their electronic income tax return need to check with their tax professional to ensure they are an authorized IRS e-file Provider. For corporations preparing their own returns, there are three different transmission methods.

- Direct Transmission – Filing a corporate tax return directly to IRS with no assistance from another entity.
- Third-Party Transmitter – Sending a corporate return to an authorized IRS e-file Provider and they transmit the return to IRS.
- Online Provider – Creating a corporate return using commercially-available software and transmitting it through the software provider OR creating a return using a software and transmitting via Direct Transmission.

It is recommended that the online registration and e-file Application process be completed at least 45 days before the plan to file the return and 60 days if you plan to transmit your own return.

Frequently Asked Questions:

How does a corporation submit the attachments, explanations, etc. required by Form 1120/1120S instructions and IRS regulations?

In most situations, the software should create supporting data when you input the necessary information. In situations where the data cannot be entered into the software (including signature-required documents), taxpayers must scan the documents and send a PDF file as attachments.

How are refund & balance due returns handled?

When taxpayers are entitled to refunds, they have several options. A corporate income tax refund may be applied to next year's estimated tax; received as a Direct Deposit or paper check; or be split to be applied to be next year's estimated tax and received as Direct Deposit or paper check.
If additional tax is owed, the taxpayer must pay the balance due by the original due date of the return or be subjected to interest and penalties. Taxpayers have several options to pay the balance due. Taxpayers can authorize an electronic funds withdrawal or pay by credit card when a return is filed electronically. They can also pay the balance due by Electronic Federal Tax Payment System (EFTPS) or check in the same way as paper return filers.

What happens if a tax return is rejected by the IRS?

If a corporate return that is e-filed is rejected, an acknowledgement is returned through the transmitter to correct the issue. If it is determined that the rejected electronic return cannot be successfully corrected and e-filed, the taxpayer will then need to file a paper return with a copy of the e-file rejection notice and explanation to the IRS. The corrected return can be retransmitted and considered timely filed if it is accepted within 20 calendar days after the original transmission.

What happens if a corporate taxpayer required to e-file fails to comply?

If a corporation fails to e-file when required, the IRS may determine that the taxpayer has failed to file the return and assess monetary penalties on the amount of underpayments. In addition, any return not in compliance with e-file requirement will be considered to not have been timely filed rendering any elections invalid.

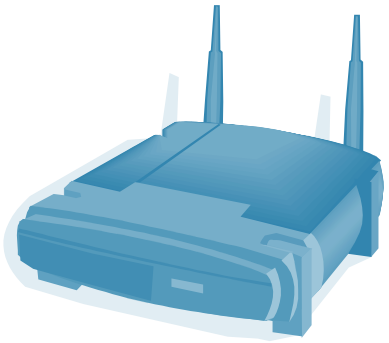
In order to comply with the new regulations, we suggest you start on this new procedure as soon as possible.
The regulation also indicates that the requirement to e-file will apply to corporations with assets of $10 million or more for tax years ending on or after December 31, 2006 .♦

Wi-Fi Protection

Hackers use countless methods in gaining illegal access to computers across the world. Although you may not know it, they may actually be using your own high speed Internet connection to do such deeds, leaving behind a trail that leads straight to your front door.

With the decreasing costs of setting up a wireless home network, it seems more consumers are moving towards this route. It is simple to set up and it lets the consumers do their Internet surfing from anywhere in the home, whether in the bathroom or outside in the backyard. The wireless freedom is a joy to have for you and your family, and the hacker living next door. A hacker within the near vicinity of the wireless router can "steal" your own Internet connection if securities are not put into place. Savvy wireless hackers do not even have to attack your computer to break into it on a wireless connection; they can just sit and wait for you to provide your information to them.

Of course, most Wi-Fi freeloaders are looking for little more than free surf on an open Internet connection. But some can break into an insecure network to read the data stored on a hard drive, plant malicious software on a computer, or commit criminal activity using someone else's computer address.



Here are some easy steps to network security that will not cost much extra time or money. While these will not guarantee laptop safety, they add an extra layer of protection beyond a firewall and antivirus software.

1. **Use your corporate network.** If your company provides you with a laptop that accesses the corporate network, use it for wireless surfing whenever possible. Virtual private networks, or VPNs, hide your communication with the office network. Whenever you are in a public environment, like at a hotel on a business trip, use the company's VPN to make a secure connection to your home office, because anyone who is willing to pay money to use the wireless hotspot can have access to the airspace and all of the unsecured wireless transmissions available.

2. **Keep a clean preferred list.** The preferred list is like a speed dial. Since it puts your most recent network connections at the top, it takes the longest to seek out the first places you visited, typically the relatively secure ones like your home network.

   If you look at the settings for the wireless connection on you PC, you will see a list of wireless devices that your computer can connect to automatically. So just press the "start" key and highlight "settings." From there you can reach your "network connections" and choose your wireless device or connection. After you have highlighted it, click on "wireless properties" and look for the second tab labeled "wireless networks." Your preferred list is tucked all the way inside there.

   Also, when you are surfing in a public place, do not simply turn off your computer and leave when you are finished. Remember to click on the icon that disconnects your computer from the wireless network. Otherwise, that network address will remain in your preferred list. If you have an internet cafe in your list, you might connect to it automatically the next time you go there to work while drinking a latte. Without you noticing, the preferred list might even automatically drop you from your corporate network and put you on the coffee-shop network instead.

3. **Enable security on your router.** When you buy a router for wireless surfing at home, its security does not normally go on automatically. Some providers have online tutorials that describe how you can enable the router's security. Linksys, for example, lists every step in detail at its website.

4. **Change the default password.** Your login information may be available to the public, unless you change it. It is easy for hackers to uncover the default login and passwords for wireless networks by entering the name of their router maker into a simple Google search.

5. **Enable web-mail security.** Call your e-mail service provider to find out how to enable the security for your web-mail. While the security options vary, many do not automatically turn on. The security options may be hard to find. An example would be to look for your preferences folder and look for and turn on the option for "session security". This will prevent wireless hackers from reading your connection with the service provider, essentially hiding the e-mails you receive. You can see the change when the address in your browser changes to "https" from "http."

Of course, nothing you do is foolproof. A well-tooled hacker can break into anything they please. Even if complete security is an unreachable goal, taking a few simple steps is better than doing nothing at all .♦

Questions or comments about this issue or inquiries about our newsletter by e-mail subscription service can be sent to:

newsletter@knllp.com