WV Executive Branch Privacy Tip
Stay Vigilant Against Bogus IRS Phone Calls and Emails

As you know, the Privacy Office occasionally issues tips to assist you in your "away from work" life. This tip is from the Internal Revenue Service website (www.irs.gov).

IRS Tax Tip 2015-20, February 17, 2015

Tax scams take many different forms. Recently, the most common scams are phone calls and emails from thieves who pretend to be from the IRS. They use the IRS name, logo or a fake website to try to steal your money. They may try to steal your identity too. Here are several tips from the IRS to help you avoid being a victim of these tax scams:

The real IRS **will not**:

- Initiate contact with you by phone, email, text or social media to ask for your personal or financial information.
- Call you and demand immediate payment. The IRS will not call about taxes you owe without first mailing you a bill.
- Require that you pay your taxes a certain way. For example, telling you to pay with a prepaid debit card.

Be wary if you get a phone call from someone who claims to be from the IRS and demands that you pay immediately. Here are some steps you can take to avoid and stop these scams.

If you don't owe taxes or have no reason to think that you do:

- Contact the Treasury Inspector General for Tax Administration. Use TIGTA's "IRS Impersonation Scam Reporting" web page to report the incident.
- You should also report it to the Federal Trade Commission. Use the "FTC Complaint Assistant" on FTC.gov. Please add "IRS Telephone Scam" to the comments of your report.

If you think you may owe taxes:

- Ask for a call back number and an employee badge number.
- Call the IRS at 800-829-1040. IRS employees can help you.

In most cases, an IRS phishing scam is an unsolicited, bogus email that claims to come from the IRS. They often use fake refunds, phony tax bills, or threats of an audit. Some emails link to sham websites that look real. The scammers' goal is to lure victims to give up their personal and financial information. If they get what they're after, they use it to steal a victim's money and their identity.

If you get a 'phishing' email, the IRS offers this advice:

- Don't reply to the message.
- Don't give out your personal or financial information.
- Forward the email to phishing@irs.gov. Then delete it.
- Don't open any attachments or click on any links. They may have malicious code that will infect your computer.

Stay alert to scams that use the IRS as a lure. More information on how to report phishing or phone scams is available on IRS.gov.

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.