NJ Treasury Assures Filers of Online Taxation Data Security Measures

TRENTON – With tax season fully underway, the New Jersey Department of the Treasury would like to assure residents and filers, alike, of the online security measures in place to protect taxation data.

"We want every resident and filer in New Jersey to know that we take the security of their personal information very seriously," said Acting State Treasurer Elizabeth Maher Muoio. "Our personnel go to great lengths to make sure we have the necessary software and protocols in place to protect the transmittal of online data and we urge residents to be cautious and heed these tips as well."

In doing so, the Department of the Treasury's Division of Taxation has posted the following information online to address major areas of concern when it comes to web security:

- New Jersey automatically encrypts sensitive data when it is exchanged on the state's secure websites. The system is designed to protect personal data and messages traveling to and from the state network, protecting the information from unauthorized access if it is intercepted or diverted in transit.
- The web addresses for these secure sites begin with the letters "https." The "s" stands for secure, indicating that the information entered into fields on the website will be encrypted. On some state sites that allow the submission of sensitive data, such as banking and personally identifiable information, a padlock icon will appear either to the left or the right of the web address in the URL field, depending on the web browser. This is a visual indicator to users informing them that traffic to and from the website is encrypted and protected. This use of encryption is designed to prevent hackers and identity thieves from intercepting and accessing the transmitted data. This is the same security method that online shopping websites use to prevent unauthorized access to your payment card information.
- Users are NOT required to have special software or applications to take advantage of this security on state websites. The encryption is done automatically by the systems.
- The state network uses many other systems and tactics to protect data. For example, the state has multiple firewalls in place that screen and filter data sent to and from the state network. Every day, the state uses these firewalls to block millions of potential threats from accessing its systems and to prevent unsecured, private data from leaving state networks.
- New Jersey works with the largest and most respected Internet providers and security firms – as well as national and international online security professionals – to protect the public's identities and privacy.

- To assist in this effort, the public should never send sensitive data, such as Social Security numbers and financial account information, to any state agency or entity in regular, unencrypted emails. Instead, this data should only be provided to the state via the state's secure websites or telephone payment systems.

# # #