OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

FOR IMMEDIATE RELEASE July 16, 2019

For Information Contact:
Public Affairs (202) 981-6000

Fraud Alert:
Transnational Fraud Ring Targets U.S. Government Procurement Offices and Vendors

In July 2018, the U.S. Department of Homeland Security (DHS) Office of Inspector General (OIG) discovered that members of a transnational fraud ring based in Atlanta, Georgia, had impersonated a DHS procurement official to obtain computer equipment from private vendors. Further investigation into the ongoing fraud scheme revealed that the subjects were also stealing electronic equipment intended for other Federal agencies, including the Departments of Commerce, Defense, Housing and Urban Development, Justice, Labor, and Transportation; the Federal Deposit Insurance Corporation; the Securities and Exchange Commission; and the Railway Retirement Board. Some of the purchase orders identified were for hundreds of thousands of dollars each.

Fraud Scheme

The fraudsters identify Federal government solicitations for computer equipment—frequently laptops, hard drives, and smart phones. They fax or email fraudulent requests for quotations (RFQ) to government vendors nationwide.

The RFQs use the name of a legitimate government procurement official but include a phone or fax number associated with the fraudsters. They also use email addresses that spoof U.S. government agencies, with domain names such as “rrb-gov.us.” Alternatively, the email’s From header displays a legitimate government email address, but the Reply-To header is a slightly different, non-government email address. In some cases, the fraudsters avoid email and insist on communicating by fax.

The fraudsters respond to any quotations received with fraudulent purchase orders that include delivery addresses chosen by the fraudsters—frequently abandoned commercial properties.

When the fraudsters receive the shipment, the ringleader decides whether to sell the equipment in the United States or ship it to Nigeria for resale.

The equipment enters the black market, and the government vendor never receives payment for the goods.

Prevention Measures

If you receive an RFQ for electronic equipment that appears to come from the U.S. Government, take the following precautions:

- Independently obtain the phone number for the listed procurement official and call them to confirm the RFQ is legitimate before responding to any RFQs received by fax;
- Respond to RFQs received by email only when the sender's domain and the Reply To header end in ".gov";
- Beware of any purported procurement officials who refuse to communicate by email;
- Beware of typographical errors, unusual language, and distorted U.S. government seals and other graphics; and
- Clearly indicate on the outside of all boxes that the contents are the property of the United States Government (in at least one case, a buyer refused to purchase the stolen goods from the fraudster when he saw "U.S. Department of Homeland Security" on the boxes).

Anyone who believes they may have been a victim of this fraud scheme is urged to call the DHS OIG Hotline (1-800-323-8603) or file a complaint online via the DHS OIG website, www.oig.dhs.gov.

###

For more information, visit our website, www.oig.dhs.gov