# FRAUD ALERT:
# Fake Government Procurement Schemes

## Attention: Government Vendors

August 2024

**The Office of Inspector General (OIG) for the Department of Commerce is aware of scams involving foreign actors impersonating procurement officials and defrauding small and large businesses alike of items that are easily subject to theft and quick resale (e.g., electronics and communication equipment).**

Scammers impersonating federal government employees or agencies use "spoofed" email addresses to send fraudulent requests for quotations (RFQs). **These solicitations are fake.** Spoofed emails appear to originate from government email domains such as .gov or .mil, but the embedded "Reply To" address is different and nongovernmental. Solicitations also might be sent directly from nongovernmental domain extensions such as .net, .org, or .com. The fake RFQs, which often include agency logos and names of real agency officials, are generally for electronic equipment (cell phones, laptops, tablets, and other electronic devices).

When a business entity responds to the fake RFQ, the scammers will accept the quote and provide a fraudulent purchase order (PO). As with the RFQs, the POs contain copied agency logos, phony digital signatures, and typical contract language and terms, such as "net 30" payment guarantees. To provide an address in the United States, the scammers impersonate logistics companies and defraud commercial warehouses and other businesses to receive shipments with the goal of exporting the goods overseas.

Speed is favored by the scammers. If a procurement seems to be moving too fast (e.g., the contract is awarded immediately after submission, as opposed to after the "submission suspense date" is reached), it is probably too good to be true.

## Protect Yourself and Your Company

- Review any unsolicited RFQs and POs carefully.
- Look up the phone number for the listed procurement official using an independent source, not information provided by the unsolicited emailer. Call or email the official through your independently obtained contact information to help make sure the RFQ or PO is legitimate.
- Make sure that the email address is legitimate. Hover over the email address in the "From" field without clicking on it to check for a valid email domain (government agency, university, hospital, etc.) or view the email headers in the message properties. Government agencies **will not** redirect you to a commercial domain to conduct procurement business.
- Search the Internet for the listed delivery address, and confirm the address is affiliated with the agency, university, or hospital. Beware of addresses that are for an individual residence, self-storage facility, virtual office, or shipping and packing store.
- Be suspicious of any purported procurement officials who refuse to communicate by telephone.

## Fraud Reporting

If you believe you have been either solicited or victimized by one of these procurement scams, report the incident immediately to the FBI's Internet Crime Complaint Center at https://www.ic3.gov/default.aspx.

If you have information about fraud, waste, abuse, mismanagement, or other crimes or violations of federal laws, rules, and regulations relating to Department programs and operations, please report it to the OIG Hotline. You can submit your complaint at https://www.oig.doc.gov/Pages/Hotline.aspx.