U.S. DEPARTMENT OF STATE OFFICE OF INSPECTOR GENERAL

INVESTIGATIONS

FRAUD ALERT 2021-01

Electronic Equipment Scheme Utilizes Fake Government RFQs

The Office of Inspector General (OIG), Office of Investigations (INV) for the U.S. Department of State (DOS) has become aware of a scam involving disguised or "spoofed" email addresses.

Individuals claiming to be members of the Office of Procurement Executive (A/OPE) for DOS procurements or the Office of Contracts for U.S. Agency for Global Media (USAGM) for USAGM procurements have used such addresses to solicit fraudulent Requests for Quotations (RFQs). The fraudsters seek RFQs for electronic equipment (Apple iPhones, Samsung Galaxy phones, laptops, tablets, and other electronic devices) via "spoofed" email addresses.

These "spoofed" emails appear to originate from government email domains, including state.gov and usagm.gov, but have non-government domain extensions such as ".net" or ".com." Additionally, when a U.S.-based business responds to the RFQ, the scammer replies using an email address that is similar to a legitimate government email address but has a non-government email domain extension.

The fraudulent RFQs also appear nearly identical to legitimate RFQs used by DOS and USAGM, often using the names of real agency officials. However, the fraudulent RFQs have illegitimate contact information, including email addresses and phone numbers that send any correspondence back to the fraudsters and not to any legitimate government entity.

If a business entity responds to the RFQ, the fraudster will accept the quote and the business is provided with an address to which they can ship the devices. Payment is guaranteed within 30 calendar days of the goods having been received ("Net 30").

The shipping addresses vary but are typically commercial addresses accessible by the public, such as short-term storage companies. However, when the U.S.-based business submits an invoice for payment to the affected government agency, the invoice is rejected, or no response is provided to the business because the government agency has no records of the fraudulent procurement.

To prevent being victimized, government vendors should consider verifying RFQs and shipping addresses with agency officials by using publicly available contact information. This information can be found here:

Department of State:
https://www.state.gov/about-us-office-of-the-procurement-executive/

USAGM:
https://www.usagm.gov/work-with-us/contract-opportunities/

Government vendors can also carefully review email header information and confirm it is from a valid government domain, such as **state.gov** or **usagm.gov**.

If you have information about fraud, waste, abuse, mismanagement, or other crimes or violations of federal laws, rules, and regulations relating to Department or USAGM programs and operations, please report it to the OIG Hotline. You can submit your complaint at **stateoig.gov/hotline**. The Hotline may be used for unclassified information only. To submit classified information, contact the Hotline at (800) 409-9926 or (202) 647-3320 for further instructions.