

## FOR INFORMATION PURPOSES

June 27, 2019

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

In April 2019, the National Archives and Records Administration (NARA) Office of Inspector General (OIG), Office of Investigations (OI), received information concerning a potential fraud scheme in which unknown individuals were impersonating NARA procurement officials to obtain computer equipment from private vendors. The OI conducted a preliminary inquiry and determined that this type of scheme has been ongoing since at least 2016, and has affected multiple Federal agencies.

#### **Fraud Scheme**

The fraudsters identify Federal government solicitations for computer equipment such as laptops, tablets, hard drives, thumb drives, smart phones, projectors, and printer toner. They spoof the official government email address of agency procurement officials with domain names such as “nara-gov.org” and “nara-gov.us,” and email fraudulent Requests for Quotations (RFQ) to government vendors nationwide. The vendor’s email From header displays a valid domain, “nara.gov,” which makes it look legitimate to the vendors. However, when a vendor replies to the email the Reply-To header reveals the non-government email address.

The RFQs use the name of legitimate government procurement officials, but include a phone or fax number associated with the fraudsters. Furthermore, when the fraudsters receive a Quotation from a vendor responding to the RFQ, they submit a Purchase Order and include a delivery address for commercial storage units across the United States. The equipment is then either shipped overseas to be resold by the fraudsters, or it is resold in the United States.

The vendors never receive payment for the goods.

#### **Prevention Measures**

If you receive an RFQ for electronic equipment that appears to come from the National Archives, 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; and
- Beware of typographical errors, unusual language not typical of native English speakers, and distorted U.S. government seals and other graphics.

Anyone who believes they may have been a victim of this fraud scheme is encouraged to call the NARA OIG Hotline (1-800-786-2551) or file a complaint online by emailing, [oig.hotline@nara.gov](mailto:oig.hotline@nara.gov).