U.S. DEPARTMENT OF COMMERCE
OFFICE OF INSPECTOR GENERAL

FRAUD ALERT

The Department of Commerce Office of Inspector General (OIG) is aware of a sophisticated business email compromise scam, which has resulted in the diversion of federal grant payments into fraudulent bank accounts.

In several common schemes, criminals gain access to and hijack government employee, grantee, or contractor/vendor email accounts and insert themselves into an existing payment conversation without the victim's knowledge. The criminals claim that the victim grantee/contractor has changed banks or no longer accepts checks and provide new automated clearing house (ACH) or wire instructions—sometimes supported by a fraudulent W-9 or other authentic-looking bank documents.

Because the message appears to come from a known contact and fits an ongoing transaction, the recipient may send federal funds to an account controlled by the criminals.

These schemes often create urgency and rely on familiarity. A request to change payment instructions, accelerate a payment, bypass normal controls, or provide payment confirmation should be treated as high risk until independently verified through another trusted contact method, such as via phone or video teleconferencing.

Protect Yourself and Federal Funds:

- Independently verify every request to change banking or payment information by calling/videoconferencing a known contact using a previously established method of communication—not a number contained in the request.
- Require dual approval and separation of duties for grantee/contractor payment setup, banking changes, grant drawdowns, checks, ACH transfers, and wire payments. For Commerce bureaus, use an established funding mechanism, such as the Treasury Automated Standard Application for Payments (ASAP) system, to send payments to recipients.
- Inspect the sender address, reply-to address, domain spelling, email headers, and unexpected changes in tone or payment instructions. A familiar display name does not confirm the sender's identity.

Report Fraud:

If you believe you have received fraudulent payment instructions or federal funds have been diverted, immediately contact the involved financial institutions and report the incident 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.