Office of Inspector General
United States Department of State

Ukraine Response Oversight
Fraud Awareness

The following are potential fraud schemes that could compromise the Department of State's role in the Ukraine response and recommended practices to help mitigate fraud vulnerabilities.

Common Fraud Indicators		Mitigation Practices
• Unusually favorable treatment of a contractor or grantee. • Employee acting beyond their scope of duties. • Repeated sole-source awards without documentation. • Split purchases under micro-purchase threshold. • Government employee or relative with ownership interest in contract company.	**Public Corruption**	• Implement unannounced supervisory reviews of records. • Monitor for compliance with relevant laws and regulations throughout all stages of the procurement process. • Hold procurement staff accountable for the proper execution of their duties. • Ensure transparent procurement processes from request for proposal through award. Include checks for conflicts of interest through financial disclosures.
• Prices for contracted services of multiple vendors increase by identical increments. • Bid prices from regular competitors drop suddenly when a new company enters competition. • Qualified bidders do not submit requests for quotes (RFQs) but serve as subcontractors on a rotating basis. • Successful bidder subcontracts to unsuccessful bidder. • Multiple vendors with the same address and phone number. • Repeated sole-source contract awards to the same vendor, with weak justifications.	**Collusive Bidding Vendor Fraud**	• Conduct due diligence research of vendors during the pre-award phases. • Conduct market research to determine common pricing and value. • Establish transparent participation requirements. • Reduce opportunities for communication among bidders. • Report post-award change orders that exceed bid limits. • Raise awareness among staff about the risks of bid rigging. • Review conflict of interest policies with staff.
• Charging more than authorized rates. • Altered timecards or invoices from contract personnel. • Fictitious employees bill for hours "worked" on a contract. • Corporate overhead costs are billed as direct costs to the government. • Claims submitted for contractually required training that was never conducted.	**Cost Mischarging False Claims**	• Do not sign invoices unless all line items are accounted for. • Use the contract vehicle to enforce deficiencies. • Put modifications to the contract in writing. • Conduct spot checks of contract employees, as allowed by the contract. • Trust, but always verify!
• Invoicing personal expenses as business expenses. • Invoicing more than one grant for the same work. • Invoicing for costs that have not been incurred. • Invoicing inflated labor costs or costs for fictitious employees.	**Fraudulent Invoicing**	• Delineate clear oversight responsibilities. • Track and monitor compliance and enforce reporting requirements. • Initiate or recommend audits be performed, as necessary. • Conduct thorough post-award reviews and make appropriate adjustments or disallowances.
• Impostor vendor emails a request to change legitimate vendor banking information and diverts payments to new account. • Change in delivery location from commercial/business address to a residential address.	**Fraudulent Changes to Key Business or Financial Info**	• Verify all changes to banking or delivery information with the vendor in person or a call to a verified phone number to ensure legitimacy. • Check email addresses for accuracy. Report fraudulent vendor email addresses to the legitimate vendor, and OIG. • Ensure up-to-date documentation of vendor responsible parties to ensure former employees and business partners cannot make changes to contact or financial information.

Suspect fraud in the Department of State's Ukraine response effort?
Report it to the OIG Hotline www.stateoig.gov/hotline