Fraud Alert

Individuals have been fraudulently posing by mail as "representatives" of the ESCO Technologies Foundation. These individuals are using the Foundation's name without authorization and have contacted people in order to defraud them. The mailing often includes a "check" payable to the recipient. The individuals may follow up on the mailing via a phone call, text message, email or other communication to the recipient asking for personal information and/or funds. If the recipient attempts to cash the "check," it will not be honored by the receiving bank.

These communications are fraudulent. These mailings are a scam and an illegal misrepresentation of the Foundation and the important grant-making work that we do.

The ESCO Technologies Foundation and its authorized representatives do not:

- Send checks to a grantee except <u>after a grant request has been received and approved</u>.
- Offer employment, advertising or investment opportunities.
- Sponsor lotteries of any kind.
- Solicit donations of any kind from the general public.
- Ask for any personal information, such as a Social Security number or an online account password.
- Approach individuals offering grant opportunities or scholarships.
- Require/request grantees to pay insurance, deposits, or delivery and administrative fees for grant funds.
- Request funds through mail, email, text, phone or social media, such as Facebook. Twitter, Instagram or Instant Messenger.
- Request conference fees or fees to apply for jobs.
- Ask that you to click a link to resolve a problem, win a prize or access a service.

If you receive any form of communication that appears to be from the ESCO Technologies Foundation requesting any type of payment or personal and/or financial information, or if you receive a communication seemingly from the Foundation that you feel is suspicious, please disregard that communication. We would appreciate your reporting any fraudulent communications to us at: <u>legalnotices@escotechnologies.com</u>. Victims of such scams may also report them to their local law enforcement authorities for appropriate action.

When reporting fraudulent communications, please include copies of the communication and any other information you may have from the contact.