NOTICE TO SUPPLIERS

Fraudulent Quote Requests/Purchase Order E-Mail Activity

The Consolidated Nuclear Security (CNS) Supply Chain Management department wants to alert suppliers to an active email scam involving request for quotations and issuance of purchase orders that purport to originate from CNS but are in fact fraudulent. While CNS cannot prevent this illegal activity, we want to inform our supplier community and promote awareness of such events.

We can share some common traits or themes of these fraudulent emails that may help reduce risk to your company in becoming a financial victim of this scam:

- The email message may be poorly written, with misspellings and awkward sentence structure.
- The senders email address is not the same as CNS standard email address domain. The email address domain for Y-12: xxx@y12.doe.gov, for Pantex: xxx@pantex.com.
- The message and purchase order requests shipment/delivery of products to non-CNS facilities.
- The message will include an attachment that is designed to look like a purchase order, and includes a logo or other graphic, and a signature that may look legitimate.
- The message and/or purchase order may even include a signature that looks legitimate, representing one of our management team or buyers.

If you believe you have received a fraudulent email that appears to be from CNS, please forward the message to procurement@y12.doe.gov, or procurement@pantex.com, in order to verify its legitimacy before responding to the email or fulfilling the order. CNS will not be responsible for invoices for products ordered under this scam.

Suppliers should also contact their local law enforcement if they suspect that they are a victim of this scam. If you have received confirmation that the email is fraudulent, you may also file a complaint directly with the Internet Crime Complaint Center (IC3) at IC3.gov. The IC3 is a partnership between the FBI and National White Collar Crime Center.