Savannah River
NUCLEAR SOLUTIONS
FLUOR • NEWPORT NEWS NUCLEAR • HONEYWELL

September 23, 2015

ALERT

Savannah River Nuclear Solutions (SRNS) has become aware of a targeted attack involving fraudulent credit requests and purchase orders (POs) being submitted to vendors using names and email addresses that impersonate SRNS personnel. The fraudsters use realistic looking letterheads and POs with the SRNS logo, write reasonably convincingly and appear to have an understanding of the public sector procurement process. While there has been no specific pattern to these messages, vendors should be wary of the following:

- Emails from addresses formatted similar, but not identical to "john.doe@srs.gov". The fraudsters are using email addresses that are very similar to legitimate SRNS email addresses and make phone calls and speak with suppliers;
- Messages from an individual purporting to be an SRNS employee requesting the placement or confirmation of an unusual order on credit;
- Orders where the requested shipping address is not the Savannah River Site located in Aiken, SC; and.
- Suspicious requests for rush orders.

We are not aware of how many vendors have been targeted as we have only learned of each instance through vendors contacting us questioning suspicious POs of vendors contacting us seeking payment as the result of having sent equipment to the fraudsters and not having received payment.

This scam does not appear to come from any sort of information breach or computer compromise at SRNS.

If you are a vendor who believes it has been contacted or impacted by these fraudsters, please contact **1-800-888-7986.**