From:	Everly, JKeith
To:	Bartlett, Matt
Subject:	FW: Summary of January 27, 2022 Closed Call with LES Regarding IATO conditions
Date:	Wednesday, February 9, 2022 8:31:56 AM
Importance:	High

On Thursday, January 27, 2022, the NRC staff consisting of Mike Mangefrida (OCIO/GEMSD/CSB/CSOT), Keith Everly (NSIR/DSO/ISB), and Matt Bartlett (NMSS/DFM/FFLB), held a call with representatives of Louisiana Energy Services, LLC , doing business as Urenco USA (UUSA). The NRC staff discussed the proposed request from UUSA to extend the Interim Authority to Operate (IATO) through July 31, 2022. The NRC staff also discussed the conditions UUSA must meet to retain the IATO. The IATO includes both General and Specific conditions.

The UUSA's progress on the POAMs is conditional on their receiving NRC approval of their Risk Assessment submitted via letter dated October 7, 2021 (Accession No. ML21286A133 Non-Public) and supplemented via letter dated January 24, 2022 (Accession No. ML22027A611 – Non-Public). The Risk Assessment is in the early phase of NRC review and has not yet been accepted for formal review. The UUSA staff proposed revising the dates in their POAMs to be dependent upon the date of approval of their Risk Assessment. The NRC staff stated willingness to consider this option. The UUSA staff will only submit revised dates to the POAMs if needed.

The UUSA staff also requested clarity with the wording of items (e) and (f) in the Generic conditions of the IATO. These conditions state:

> e. "All system changes must be reported to the AO and CISO at least 90 days prior to implementation for assessment and approval."
>
> f. "All security related events relative to the systems are to be reported to the AO and CISO within 24 hours of discovery."

The UUSA staff requested clarity on the meaning and scope of the phrase "all system changes" in (e) and "all security related events" in (f). The NRC staff agreed that additional clarity is needed and would be provided in this summary, see below.

General conditions (e) and (f) are referring to all substantive items. The following guidance can be used to distinguish between substantive and non-substantive.

Substantive:

Substantive changes or events can be considered as those changes or events that, when they occur, affect the current operational security of a system.

Examples of substantive changes include technology refreshments, operating system upgrades, device rebuilds that do not follow a documented baseline image, installation of new network devices, adding software not on an approved site list, significant replacement of hardware and/or software due to technical refresh, and significant network reconfiguration actions.

Non-Substantive:
Minor, non-substantive changes or events can be those changes or events that, when they occur, have little or no impact to the current operational status or security posture of the systems.

Examples of minor non-substantive changes include patching; updating antivirus signatures; upgrades to existing office products such as Microsoft Office, Adobe, etc. (defined by site); adding, updating, and removing users; adding software from an approved software list; replacement of a few components due to hardware or software failure as repair actions; and configuration change to a system component or a few components.

Sincerely,

Matt Bartlett
Project Manager
NMSS/DFM/FFLB
301-415-7154