UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

February 18, 2022

**SECURITY ADVISORY FOR POWER REACTORS, INCLUDING THOSE UNDER CONSTRUCTION; NONPOWER PRODUCTION AND UTILIZATION FACILITIES; DECOMMISSIONING REACTORS, INCLUDING THOSE THAT ARE PERMANENTLY DEFUELED BUT HAVE NOT TRANSITIONED TO DECOMMISSIONING; FUEL FABRICATION, ENRICHMENT, AND CONVERSION/DECONVERSION FACILITIES; INDEPENDENT SPENT FUEL STORAGE INSTALLATIONS; LICENSEES POSSESSING SPECIAL NUCLEAR MATERIAL UNDER TITLE 10 OF THE *CODE OF FEDERAL REGULATIONS* PART 70; LICENSEES REGULATED UNDER TITLE 10 OF THE *CODE OF FEDERAL REGULATIONS* PART 37; AND ALL RADIATION CONTROL PROGRAM DIRECTORS AND STATE LIAISON OFFICERS**

**SA 2022-04**

**SUBJECT: SITUATIONAL AWARENESS—GEOPOLITICAL TENSIONS AND THE CURRENT CYBER THREAT ENVIRONMENT**

The U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (DHS/CISA) and its partners have issued a series of cyber security products to ensure that U.S. critical infrastructure sectors are aware of and prepared to mitigate and respond to cyber security threats to their most critical assets. While there are not currently any specific credible threats to the U.S. homeland, CISA is mindful of the potential for threat actors to use cyber attacks against critical infrastructure to escalate or destabilize the current geopolitical environment. Therefore, CISA has been working closely with its critical infrastructure partners to ensure awareness of potential threats and mitigative actions. The U.S. Nuclear Regulatory Commission (NRC) is issuing this security advisory to provide situational awareness to its licensees and Agreement States and to ensure they are aware of CISA's alerts and other related products.

CISA has consolidated its cyber security guidance related to the current threat environment at a central Web site, "Shields Up" (https://www.cisa.gov/shields-up). This Web site contains recommended actions for U.S. critical infrastructure: (1) take steps to quickly detect a potential cyber intrusion; (2) ensure that the organization is prepared to respond if an intrusion occurs; and (3) maximize the organization's resilience to a destructive cyber incident. The NRC recommends that all addressees review CISA's "Shields Up" Web site, as well as CISA Alert AA22-011A, "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure" (https://www.cisa.gov/uscert/ncas/alerts/aa22-011a), and take appropriate mitigative actions in accordance with applicable licensee procedures and cyber security plans, as applicable.

Suspicious activity reporting is important to the U.S. Government's security mission. The NRC encourages its licensees to remain vigilant and report cyber-related suspicious activity to CISA at central@cisa.gov and to the Federal Bureau of Investigation's 24-hour Cyber Watch at (855) 292-3937 or cywatch@fbi.gov. Licensees subject to Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, "Protection of digital computer and communication systems and

networks," are reminded of their obligation to report to the NRC certain cyber-related events under 10 CFR 73.77, "Cyber security event notifications."

If you have any questions concerning this advisory, contact the technical point of contact below.

**Backfit Analysis Statement:** This security advisory does not amend or impose new requirements or constitute a new or different regulatory staff position interpreting Commission rules and, therefore, does not constitute backfitting as defined in 10 CFR 50.109, "Backfitting," or 10 CFR 70.76, "Backfitting," or 10 CFR 72.62, "Backfitting." Consequently, the staff did not perform a backfit analysis.

**Paperwork Reduction Act Statement:** This security advisory does not contain information collections and, therefore, is not subject to the requirements of the Paperwork Reduction Act of 1995 (Title 44 of the *United States Code*, Section 3501, et seq.).

Johnson, Dante signing on behal
of Lee, Samuel
on 02/18/22

Approved by: _____
Samuel S. Lee, Acting Director
Division of Security Operations
Office of Nuclear Security
and Incident Response

Technical Contact: NRC Cyber Assessment Team
cyber@usnrc.onmicrosoft.com

SA 2022-04 "Situational Awareness – Geopolitical Tensions and the Current Cyber Threat Environment"
DATE February 18, 2022

DISTRIBUTION:

**ADAMS Accession No.: Memo ML22047A230** *** via email**

| OFFICE | NSIR/DPCP/CSB | ADM/DRMA* | NMSS/MSST/MSEB | NSIR/DSO/ILTAB |
|---|---|---|---|---|
| NAME | BYip *BY* | KAzariah-Kribbs *KA* | DWhite *DW* | RRichardson *RR* |
| DATE | Feb 16, 2022 | Feb 16, 2022 | Feb 16, 2022 | Feb 16, 2022 |
| OFFICE | OCIO/GEMSD /FLICB/ICT | NSIR/DSO | NSIR/DPCP/RSB | NSIR |
| NAME | DCullison *DC* | SPrasad *SP* | MSampson JBeardsley for *JB* | SLee *SL* |
| DATE | Feb 16, 2022 | Feb 16, 2022 | Feb 17, 2022 | Feb 16, 2022 |
| OFFICE | NSIR/DPR | NRR/DANU | NRR/DORL | NMSS/DUWP |
| NAME | RJohnson GWarnick for *GW* | MShams JBowen for *JB* | BPham *BP* | JMarshall ARoberts for *AR* |
| DATE | Feb 17, 2022 | Feb 17, 2022 | Feb 17, 2022 | Feb 17, 2022 |
| OFFICE | NRR/DANU | OGC/GCRPS /HLWFCNS/NLO* | NMSS/MSST | NMSS/DFM |
| NAME | BSmith *BS* | JMaltese *JM* | KWilliams TClark for *TC* | SHelton *SH* |
| DATE | Feb 17, 2022 | Feb 17, 2022 | Feb 17, 2022 | Feb 17, 2022 |
| OFFICE | NMSS/DFM | NSIR* | NSIR | |
| NAME | CRegan PMcKenna for *PM* | MGavrilas *MG* | SLee DJohnson for *DJ* | |
| DATE | Feb 17, 2022 | Feb 18, 2022 | Feb 18, 2022 | |

***OFFICIAL RECORD COPY***