



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

March 1, 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 (Rev. 1)

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. CISA notes that the current geopolitical conflict may have consequences for our Nation's critical infrastructure and every organization should be prepared to respond to disruptive cyber activity. On February 26, 2022, CISA issued Alert AA22-057A, "Destructive Malware Targeting Organizations in Ukraine" (<https://www.cisa.gov/uscert/ncas/alerts/aa22-057a>), which describes the use of malware against Ukrainian targets in January and February 2022 to render targeted devices inoperable.

While there are not currently any specific or 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 revised security advisory to its licensees and Agreement States in response to reports of continued denial of service and destructive malware attacks affecting Ukraine and other countries in the region, and to reinforce the importance of reviewing CISA's alerts and recommended mitigative actions.

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 regularly review CISA's "Shields Up" Web site for the latest threat and mitigation information, as well as CISA Alert AA22-011A, "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure"

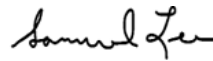
(<https://www.cisa.gov/uscert/ncas/alerts/aa22-011a>), and take appropriate mitigative actions in accordance with licensee procedures and cyber security plans, as applicable.

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 (888) 282-0870 or central@cisa.dhs.gov, or to the Federal Bureau of Investigation (FBI) via your local FBI field office or its 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.).



Signed by Lee, Samuel
on 03/01/22

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

SITUATIONAL AWARENESS—GEOPOLITICAL TENSIONS AND THE CURRENT CYBER THREAT ENVIRONMENT (Rev 1.) DATE March 1, 2022

DISTRIBUTION:

ADAMS Accession No.: ML22056A180

* via email

OFFICE	NSIR/DPCP/CSB	NMSS/MSST /MSEB	NSIR/DSO/SOSB	NSIR/DPR
NAME	BYip <i>BY</i>	DWhite <i>DW</i>	JKeene <i>JK</i>	RJohnson <i>RJ</i>
DATE	Feb 28, 2022	Feb 28, 2022	Feb 28, 2022	Feb 28, 2022
OFFICE	NMSS/DFM	NRR/DORL	NRR/DANU	NMSS/DFM
NAME	CRegan <i>CR</i>	BPham <i>BP</i>	BSmith <i>BS</i>	SHelton GMiller for <i>GM</i>
DATE	Feb 28, 2022	Feb 28, 2022	Feb 28, 2022	Feb 28, 2022
OFFICE	NMSS/MSST	NMSS/DUWP	OGC/GCRPS /HLWFCNS/NLO*	NRR/DANU
NAME	KWilliams TClark for <i>TC</i>	JMarshall <i>JM</i>	JMaltese <i>JM</i>	MShams JBowen for <i>JB</i>
DATE	Feb 28, 2022	Feb 28, 2022	Feb 28, 2022	Feb 28, 2022
OFFICE	NSIR/DSO/ILTAB	NSIR	NSIR/DPCP/RSB	NSIR
NAME	RRichardson <i>RR</i>	SLee <i>SL</i>	MSampson JBeardsley for <i>JB</i>	MGavrilas CErlanger for <i>CE</i>
DATE	Feb 28, 2022	Feb 28, 2022	Feb 28, 2022	Mar 1, 2022
OFFICE	NSIR			
NAME	SLee <i>SL</i>			
DATE	Mar 1, 2022			

OFFICIAL RECORD COPY