Published on *The National Law Review* https://natlawreview.com

Russian Government Officials Charged with Hacking U.S. Energy Infrastructure

Article By:

Linn F. Freedman

The U.S. Department of Justice (DOJ) unsealed indictments against four Russian government officials on March 24, 2022, alleging that they hacked into networks that controlled energy systems in the U.S.

According to the DOJ, the attacks took place between 2012 and 2018, and included physical damage to infrastructure, as well as embedding malware for later use. The indictment detailed how the threat actors gained access to networks through spearphishing attacks "targeting more than 3,300 users at more than 500 U.S. and international companies and entities, in addition to U.S. government agencies such as the Nuclear Regulatory Commission."

One concerning example cited is the successful intrusion into the Wolf Creek Nuclear Operating Corp., which operates a nuclear power plant.

Although the four Russian defendants are not in U.S. custody, the State Department is offering rewards of up to $10 million "for information leading to the identification or location" of the accused.

Contemporaneously with the unsealing of the indictments, the FBI, the Cybersecurity and Infrastructure Security Agency, and the Department of Energy issued a joint advisory highlighting "historical tactics, techniques, and procedures (TTPs) used by adversaries to target U.S. and international Energy Sector organizations" warning that "state-sponsored Russian cyber operations continue to pose a threat to U.S. Energy Sector networks" and urging critical infrastructure organizations "to apply the recommendations listed in the Mitigation section of this advisory and Appendix A to reduce the risk of compromise."

National Law Review, Volume XII, Number 91