INTERNATIONAL FEDERATION OF
PROFESSIONAL & TECHNICAL ENGINEERS
AFL-CIO & CLC

501 3rd Street, NW, Suite 701, Washington, DC 20001
202-239-4880 • FAX 202-239-4881 • www.ifpte.org

MATTHEW S. BIGGS
President

GAY HENSON
Secretary-Treasurer

2024 IFPTE Issue Brief ***118th Congress***

Ensuring Secure On-Site Operations for Army Corps of Engineers Hydroelectric Dams and Navigational Locks and Dams

Cybersecurity threats to critical infrastructure are evolving rapidly. Recent advances in artificial intelligence (AI) are increasing the risk that malicious cyber threats from hostile governments and non-state actors will pose a substantial and enduring threat to federal critical infrastructure.

With these threats to critical infrastructure in mind, we ask Congress to protect our nation's inland waterways and federal hydroelectric dams that are under the control of the U.S. Army Corps of Engineers (USACE).

Right now, the USACE is in the process of implementing remote operations at navigational lock and dam sites and hydroelectric dams. Remote operations introduce new cyber security vulnerabilities created by operating locks and dams and hydroelectric dams remotely over communications networks. It will also reduce public safety and the security of the physical infrastructure, since remote operations will remote or reduce onsite federal personnel who are trained to safely operate USACE infrastructure 24 hours a day, 7 days a week.

We cannot overstate these ever-present threats and we urge Congress to heed Cybersecurity and Infrastructure Security Agency (CISA) Executive Director Brandon Wales's warning:

> "It is very clear that Chinese attempts to compromise critical infrastructure are in part to pre-position themselves to be able to disrupt or destroy that critical infrastructure in the event of a conflict, to either prevent the United States from being able to project power into Asia or to cause societal chaos inside the United States — to affect our decision-making around a crisis."[1]

Reliability is at the Heart of the Success of the USACE Inland Waterway Transportation and Power Systems. Throughout the U.S., some 1,500 inherently governmental federal employees work to ensure 24/7 operations at over 230 USACE locks and dams on 41 waterways and river systems and 75 federal hydropower plants. These workers, many of whom work in rural communities and are veterans, are the eyes and ears on these critical infrastructure systems. They support the safe transit of 630 million tons of cargo each year, across 11,000 miles of inland waterways and operate USACE hydropower plants that generate 25% of our nation's clean renewable hydroelectric power.

The USACE's plan to operate locks and dams and hydroelectric dams through remote operations will expose our top critical infrastructure to hostile adversaries who intend to shut down the power grid, disrupt commerce and navigation on the inland waterways, and harm the U.S. economy and public safety.

[1] China's Cyber Army is Invading Critical U.S. Services, Washington Post, Dec. 11, 2023.

A cyber-attack that disables operations of USACE navigational locks and hydroelectric dams would have a tremendous impact on our economy. The inland waterways play an outsized role in transporting agriculture, fertilizers, coal and petroleum, ore and minerals, construction aggregates, and other key commodities, and the USACE provides 25% of our nation's hydroelectric power. A 2017 study prepared for the U.S. Maritime Administration and the National Waterways Foundation, showed the far-reaching economic impact of an unscheduled lock outage at four key locks, which would exceed at least $1 billion for each lock and ripple through critical supply chains regional economies in several states.[2]

Reducing or eliminating the number of trained onsite federal employees who operate USACE locks and dams and hydroelectric dams also opens the door to threats such as weather hazards, trespass and tampering with federal property, a loss of communication and remote operational control, or any other anomalous situation that may result in a public safety or possible national security concern. Trained lock and dam operators provide commercial and recreational vessels information and instruction over radio communications and in face-to-face communications to ensure safe transit and assist mariners in distress. These inherently governmental workers are essential to reliable operations, and reliability is at the heart of the success of the inland waterway transportation system.

Bottom line: Our homeland security must take precedence. The USACE is moving forward with a plan that risks exposing our top federal critical infrastructure, the supply chains, and the public to dangers from continuing and expanding cybersecurity threats. Converting federal hydro dams and navigational locks and dams from responsive secure operations with 24/7 on-site federal personnel to operations dependent on computer control off-site remote operation is a cybersecurity disaster in the making. Remote operations will degrade "continuity of operations" and create new threat scenarios in which the President and the Secretary may be unable to secure federal dams and the inland waterways during a national emergency. Further, remote operations open the door for eventually replacing all human decision making on these inherently governmental functions with AI-enabled automated decision making. Congress should prohibit USACE from implementing remote operations and reducing or removing onsite federal on these critical infrastructure sites.

Proposed Language:

Sec.___. SAFEGUARDING CORPS OF ENGINEERS CRITICAL INFRASTRUCTURES.

(a) Secretary, acting through the Army Corps of Engineers
  (1) shall maintain local on-site operations of any Corps of Engineers Civil Works critical infrastructure, as identified under Section 2321(a) of Title 33, and
  (2) shall not operate any standing hydroelectric dams and navigation locks and dams through remote offsite operations or automated operations, and
  (3) shall not convert new any hydroelectric dams and navigation locks and dams to remote offsite operations or automated operations, and
  (4) ensure any new control system on critical infrastructure as identified under Section 2321(a) of Title 33, does not result in the reduction of federal employees supporting inherently governmental functions.

(b) Definition. – in this section:
  (1) the term "remote offsite operations" means the operation of any infrastructure, as identified under Section 2321(a) of Title 33, by any control system or interconnecting network system that enables human operation or automated operation of one or several infrastructure sites from a location other than a site located on the physical infrastructure.

[2] U. Tennessee and Vanderbilt University, The Impacts of Unscheduled Lock Outages -- Prepared for: The National Waterways Foundation and The U.S. Maritime Administration, Oct. 2017