OpenVoiceNews U.S.

Transparent. Unbiased. Yours.

US Denounces ‘Smear Campaign’ as Pro-Iran Hackers Threaten to Leak Trump Emails

July 2, 2025

— Categories: Defense & Security

WASHINGTON, D.C. – Federal authorities are condemning what they describe as a deliberate attempt by pro-Iran hackers to damage the reputation of former President Donald Trump and sow division in the United States.

The hackers claim to have stolen thousands of emails tied to Trump’s advisers, including former chief of staff Susie Wiles and adult film actress Stormy Daniels. They say they plan to release the material unless certain demands are met.

Officials say there is no evidence proving the emails are real. The Cybersecurity and Infrastructure Security Agency (CISA) called the threat “nothing more than digital propaganda.”

“A hostile foreign adversary is threatening to exploit stolen and unverified material to distract, discredit, and divide,” CISA spokeswoman Marci McCarthy said on Wednesday. “These criminals will be found, and they will be brought to justice.”

The hackers contacted Reuters directly, saying they planned to release a steady stream of documents. Their claims surfaced just as CISA, the FBI, and the National Security Agency issued a joint warning about possible Iranian cyberattacks on American infrastructure.

Officials say the groups supporting Tehran could try to disrupt power grids, transportation networks, banks, and defense contractors, especially those with ties to Israel.

“Iranian-backed hackers have tried to target American campaigns and businesses before,” McCarthy said. “This is part of a larger effort to undermine confidence in our democratic institutions.”

Last year, federal prosecutors charged three Iranian nationals with hacking into Trump’s 2020 campaign and attempting to access Democratic campaign networks as well. Those efforts largely failed, but experts say the threat has not gone away.

While hackers linked to Iran have damaged websites and tried ransomware attacks on US companies, they have not yet caused widespread harm. Still, authorities are urging all organizations to be prepared.

Security agencies recommend updating software regularly, using strong passwords, and turning on multi-factor authentication to reduce the risk of attacks.

National security analysts warn that even the claim of stolen data can be enough to create distrust.

“This is a clear example of information warfare,” said Mark Jennings, a former Defense Intelligence Agency analyst. “The goal is to make Americans doubt each other and their institutions.”

Officials say any material released by the hackers should be treated with caution and verified before being shared or reported.