OpenVoiceNews U.S.

Transparent. Unbiased. Yours.

Pentagon and DHS Warn: Iran May Launch Cyber-Attacks on U.S. Defense Contractors

July 1, 2025

— Categories: Defense & Security

Washington, D.C., July 1, 2025 – The Pentagon and the Department of Homeland Security (DHS) have issued a joint warning that Iran may soon target U.S. defense companies through cyber-attacks, as tensions between the two nations continue to rise.

According to a government advisory released this week, U.S. intelligence agencies have detected increased cyber activity from Iranian state-backed groups, including efforts to scan networks and gather information on military contractors. These actions suggest that Iranian hackers may be preparing to breach defense systems or steal sensitive data.

“Iran sees cyber-attacks as a way to respond without direct military conflict,” said a senior DHS official. “They’re likely to go after companies that support the U.S. military.”

The warning follows recent U.S. airstrikes on Iranian-linked military groups in the Middle East. In response, Iranian leaders have promised retaliation. Officials believe a cyber response is highly likely, as it allows Iran to cause disruption without using weapons on the battlefield.

Defense companies are an appealing target for cyber-attacks. They manage valuable information about weapons systems, satellite technology, and military communications. While large firms often have strong cybersecurity systems, smaller subcontractors may be more vulnerable.

“Even a small contractor can be a way in for attackers,” said Arjun Rao, a cybersecurity analyst. “If hackers breach one weak point, they could access larger systems or delay important projects.”

The advisory specifically highlights the threat from Iranian-linked hacker groups such as APT39 and MuddyWater. These groups have been involved in cyber-espionage campaigns in the past and are believed to operate under Iran’s intelligence services.

To prevent damage, the Pentagon and DHS are urging all defense-related companies to:

- Strengthen network security
- Monitor for unusual or suspicious activity
- Train employees on phishing scams and access controls
- Prepare emergency response plans

“This is not just a warning for big defense firms,” said the DHS official. “Every company in the supply chain needs to be alert and ready.”

As cyber threats grow, experts say digital security is now a key part of national defense. Iran’s actions are a reminder that future conflicts may play out not only on land, air, or sea but also in cyberspace.