FOR IMMEDIATE RELEASE
June 23, 2025
Contact: Kaitlyn Palatucci, kpalatucci@it-isac.org

No Cyber Attacks Confirmed, But Heightened Threat Remains: Updated Joint Statement from the Food and Ag-ISAC and IT-ISAC on Potential Cybersecurity Impacts of the Conflict in the Middle East

On the evening of Saturday, June 21, the U.S. carried out "Operation Midnight Hammer", a military strike on Iranian nuclear facilities. In the wake of the strike, Iranian state media condemned the action and issued warnings of retaliation. As such, the Food and Agriculture Information Sharing and Analysis Center (Food and Ag-ISAC) and the Information Technology-ISAC (IT-ISAC) continue to urge U.S. organizations to prepare for the possibility of increased cyber attacks from Iranian-aligned actors.

At this time, we have not seen or know of any confirmed cyber attacks from Iran on any specific U.S. company, including member companies of either ISAC. These statements aim to raise awareness among companies nationwide, helping them prepare and enhance their cybersecurity posture.

"From experience and history, we know that geopolitical tensions often come with increased cyber activity and threats," said Scott Algeier, Executive Director of the Food and Ag-ISAC and IT-ISAC. "While we have not seen any evidence of direct targeting of U.S. companies, the evolving nature of this underscores the importance of cyber preparedness."

Iran's playbook often includes cyber operations as a method of retaliation. Iranian state-sponsored actors, pro-Iran hacktivist groups, and financially motivated cybercriminals have previously launched cyber attacks against U.S. organizations during periods of heightened conflict, as outlined in our initial joint statement on Friday, June 13.

Iranian cyber actors are known to employ a wide range of tactics, techniques, and procedures (TTPs), including targeting known vulnerabilities, phishing, and credential harvesting. Both ISACs remain actively engaged in monitoring the threat landscape and will provide further updates should new intelligence emerge. We have and will continue to recommend that companies remain alert, take steps to evaluate their cyber readiness, and prepare for potential threats.

###

About the Food and Ag-ISAC: Founded in 2023, the Food and Agriculture-Information Sharing and Analysis Center (Food and Ag-ISAC) provides threat intelligence, analysis, and effective security practices that help food and agriculture companies detect attacks, respond to incidents, and share indicators so they can better protect themselves and manage risks to their companies and the sector.

For more information about the Food and Ag-ISAC, please visit www.foodandag-isac.org.

X: x.com/foodandagisac LinkedIn: www.linkedin.com/company/food-agriculture-isac

About the IT-ISAC: Founded in 2000, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) is a non-profit organization that augments member companies' internal capabilities by providing them access to curated cyber threat analysis, an intelligence management platform, and a trusted forum to engage with senior analysts from peer companies. We serve as a force multiplier that enables collaboration and sharing of relevant, actionable cyber threat intelligence, effective security policies, and practices for the benefit of all.

For more information about the IT-ISAC, please visit www.it-isac.org.

X: x.com/itisac LinkedIn: www.linkedin.com/company/it-isac