Urgent Security Alert: Potential Iranian Threats Against US Interests

Geauga IT Stakeholders,

Following recent US military actions targeting Iranian nuclear facilities, intelligence indicates Iran intends to retaliate using a wide array of methods. These threats are immediate, diverse, and serious, potentially affecting all levels of American interests both domestically and internationally.

Source of Intelligence:

We have received this information through the Center for Internet Security Institute for Strategic Dialogue.

The Center for Internet Security (CIS) is a nationally recognized organization dedicated to improving cybersecurity readiness and response through collaborative partnerships and best practices. CIS develops comprehensive standards, guidelines, and benchmarks that are widely adopted by government agencies, including local governments like Geauga County, Ohio. Geauga County is striving to follow CIS compliance standards, ensuring that its cybersecurity measures align with established best practices. By adhering to CIS guidelines, the county strengthens its defenses against cyber threats, safeguards critical infrastructure, and enhances overall security and operational resilience.

This document was specifically provided by Roger Peterson, The Commissioners' Director of Emergency Services and the County Auditor's Association of Ohio. We sincerely thank them for their valuable partnership in intelligence sharing and threat awareness. Here is a rundown of that security briefing.

Key Threat Areas:

1. Direct Military and Intelligence Actions:

- High likelihood of missile or drone attacks targeting US military bases and embassies, primarily in the Middle East (this has been confirmed as a fact).
- Possible assassination attempts targeting senior US officials or Iranian dissidents located in the US or abroad.

2. Cybersecurity Threats:

- Significant risk of cyberattacks on critical infrastructure (water, electricity, transportation) and prominent technology companies (Microsoft, Amazon Web Services, OpenAI).
- Previous cyber incidents have successfully disrupted critical services, showcasing capability and intent.

Based on the intelligence briefing, Iran poses a significant cybersecurity threat that could directly impact local governments like Geauga County, Ohio. Iranian military-led cyber units, including the Islamic Revolutionary Guard Corps (IRGC)-linked cyber actors, have historically targeted critical infrastructure such as water, wastewater systems, and public utilities, causing disruptions and operational failures. Iranian cyber proxies and hacktivist groups, though less sophisticated, retain sufficient capabilities to conduct disruptive attacks on public infrastructure and local government services. Specifically, local systems such as voter databases, emergency response networks, financial and administrative databases, and public utility controls could be vulnerable. These cyber threats could disrupt daily operations, reduce essential services, compromise public safety, and erode community trust and confidence in local governance. Immediate vigilance, robust cybersecurity measures, and enhanced preparedness are essential to mitigate these potential threats.

3. Proxy and Terrorist Activities:

- Iranian-supported proxy groups (e.g., Hezbollah) have networks capable of conducting attacks internationally, including within the US.
- Potential for terrorist attacks, including bombings, vehicle-borne explosive devices, or assassination attempts against high-profile figures.

4. Influence and Inspired Attacks:

- Iran's extensive online propaganda network is actively inspiring individuals globally, including in the US, to carry out cyberattacks, vandalism, and physical violence.
- There is a real possibility of disruptive demonstrations, violent riots, or targeted hate crimes spurred by these influence operations.

Recommended Actions for All Personnel:

- **Stay vigilant** and immediately report suspicious activity.
- **Enhance awareness** regarding phishing and cybersecurity threats.
- **Review security procedures** for public demonstrations, events, and critical infrastructure.

- **Coordinate closely** with security teams to ensure preparedness against potential threats.

This intelligence briefing underscores the seriousness and immediacy of these threats. We must all continue to partner together to remain alert and responsive to potential security incidents.

Our collective vigilance is crucial in protecting Geauga County's network.

Regards,

Frank

Frank Antenucci, Esq.

Deputy Chief Administrator

Geauga County ADP -- DATA, CARE, DARC

Auditor GIS Department

12611 Ravenwood Dr., Ste. 310, Chardon, Ohio 44024

O: (440)279-1993   E: fantenucci@geauga.oh.gov

Service Desk (440) 286-4357 adpsupport@geauga.oh.gov