JOINT INTELLIGENCE BULLETIN

8 January 2020

(U//FOUO) Escalating Tensions Between the United States and Iran Pose Potential Threats to the Homeland

(U) Scope

(U//FOUO) This *Joint Intelligence Bulletin* (*JIB*) is intended to assist federal, state, local, tribal, and territorial counterterrorism, cyber, and law enforcement officials, and private sector partners, to effectively deter, prevent, preempt, or respond to incidents, lethal operations, or terrorist attacks in the United States that could be conducted by or on behalf of the Government of Iran (GOI) if the GOI were to perceive actions of the United States Government (USG) as acts of war or existential threats to the Iranian regime. The GOI could act directly or enlist the cooperation of proxies and partners, such as Lebanese Hizballah. The FBI, DHS, and NCTC had assessed any kinetic retaliatory attack would first occur overseas. In the event the GOI were to determine to conduct a Homeland attack, potential targets and methods of attack in the Homeland could range from cyber operations, to targeted assassinations of individuals deemed threats to the Iranian regime, to sabotage of public or private infrastructure, including US military bases, oil and gas facilities, and public landmarks. USG actions may also provoke violent extremist supporters of the GOI to commit attacks in retribution, with little to no warning, against US-based Iranian dissidents, Jewish, Israeli, and Saudi individuals and interests, and USG personnel.

IA-41117-20

(U//FOUO) Immediate Response in Homeland Could Take Form of Cyber Operations

(U//FOUO) The FBI, DHS, and NCTC assess an immediate GOI response in the Homeland could take the form of attempted cyber operations against USG facilities and networks, including US military systems, and critical private sector functions, given that such operations could be attempted by Iran-based cyber actors without the necessity of establishing a US presence. The US Intelligence Community has assessed that Iran continues to prepare for cyber attacks against the United States and allies. It is capable of causing localized, temporary disruptive effects during a cyber attack on victim networks. Historically, Iran has shown the capability to carry out disruptive and destructive cyber attacks against public and private business networks, such as extended distributed denial-of-service (DDoS) campaigns and data deletion attacks.

(U//FOUO) Iran represents a cyber espionage and attack threat, using increasingly sophisticated cyber techniques and attempting to deploy cyber capabilities that would enable attacks against critical infrastructure in the United States. Tehran's overall risk calculus for a cyber response likely will change based on the US strike, which Iranian leaders have vocally portrayed as escalatory, and offensive cyber operations are likely to be considered as retaliatory options. Malicious activity and reconnaissance may not necessarily occur from Iranian Internet Protocol (IP) space, as actors may use midpoint infrastructure in other countries. As such, traffic from Iranian IP addresses may not be indicative of malicious activity. The FBI, DHS, and NCTC stress good cyber hygiene such as patching systems and educating personnel to guard against commonly used cyber actor techniques such as social engineering and spear-phishing.

(U//FOUO) Potential for GOI-Directed Lethal Attacks in the Homeland

(U//FOUO) In recent years, the USG has arrested several individuals acting on behalf of either the GOI or Lebanese Hizballah who have conducted surveillance indicative of contingency planning for lethal attacks in the United States against facilities and individuals.

» (U//FOUO) An agent of the GOI arrested in 2018 had conducted surveillance of Hillel Center[USPER] and Rohr Chabad Center[USPER], Jewish institutions located in Chicago, including photographing the security features surrounding the Chabad Center.

» (U//FOUO) Three Lebanese Hizballah External Security Organization (ESO) operatives arrested between 2017 and 2019 had conducted surveillance of US military and law enforcement facilities, critical infrastructure, private sector venues, and public landmarks in New York City, Boston, and Washington, DC.

(U//FOUO) The GOI also has a history of conducting assassinations and assassination attempts against individuals in the United States it deems a threat to the Iranian regime. The GOI assassinated the US-based former spokesman for the Shah of the Iran in 1980 and plotted to assassinate the Saudi Arabian ambassador to the United States in 2011. In August 2018, the USG arrested two individuals for acting as agents of the GOI by conducting covert surveillance of Iranian dissidents in New York City and Washington, DC, and the aforementioned security features of Jewish facilities in Chicago.

(U) Outlook

(U//FOUO) The FBI, DHS, and NCTC advise federal, state, local, tribal, and territorial government counterterrorism, cyber, and law enforcement officials, and private sector partners, to remain vigilant in the event of a potential GOI-directed or violent extremist GOI supporter threat to US-based individuals, facilities, and networks consistent with previously observed covert surveillance and possible pre-operational activity targeting opponents of the Iranian regime, Israeli and Jewish interests, Saudi interests, public venues, and USG infrastructure and personnel. The FBI, DHS, and NCTC urge state and local authorities and private sector partners to promptly report suspicious activities related to terrorism, including but not limited to potential material support to foreign terrorist organizations. Additionally, because Iran has shown the capability and intent to carry out disruptive and destructive cyber attacks against public and private business networks, the FBI, DHS, and NCTC advise federal, state, local, tribal, and territorial governments to report cyber-related activity including attacks such as DDoS, ransomware and data theft or deletion or other unauthorized uses.

(U) Report Suspicious Activity

(U) To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement. Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit http://nsi.ncirc.gov/resources.aspx.

(U) **The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch).** Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@fbi.gov.

(U) When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

(U) Administrative Note: Law Enforcement Response

(U//FOUO) Information contained in this intelligence bulletin is for official use only. No portion of this bulletin should be released to the media, the general public, or over nonsecure Internet servers. Release of this material could adversely affect or jeopardize investigative activities.

(U) For comments or questions related to the content or dissemination of this document, please contact the Counterterrorism Analysis Section by e-mail at FBI_CTAS@ic.fbi.gov.

(U) Tracked by: HSEC-8.1, HSEC-8.2, HSEC-8.3, HSEC-8.5, HSEC-8.8