U.S. DEPARTMENT OF THE TREASURY

Press Center

Fact Sheet: New Executive Order Targeting Human Rights Abuses Via Information Technology

4/23/2012

WASHINGTON – Today the President announced an Executive Order, "Blocking the Property and Suspending Entry into the United States of Certain Persons with Respect to Grave Human Rights Abuses by the Governments of Iran and Syria Via Information Technology" ("the GHRAVITY E.O." or the "Order"). The Order targets, among others, persons determined to have operated, or to have directed the operation of, information and communications technology that facilitates computer or network disruption, monitoring or tracking that could assist in or enable human rights abuses by or on behalf of the Government of Syria or the Government of Iran. Pursuant to this order sanctions were imposed on the Syrian General Intelligence Directorate (GID), the GID's Director Ali Mamluk, Iran's Ministry of Intelligence and Security (MOIS), Iran's Islamic Revolutionary Guard Corps (IRGC), Iran's Law Enforcement Forces (LEF), the Iranian Internet service provider Datak Telecom, and the Syrian communication firm Syriatel.

The GHRAVITY E.O. sends a clear message that the United States condemns the continuing campaigns of violence and human rights abuses against the people of Syria and Iran by their governments and provides a tool to hold accountable those who assist in or enable such abuses through the use of information and communications technology.

The following individual and entities are listed in the Annex to the GHRAVITY E.O, and any property in the United States or in the possession or control of U.S. persons in which they have an interest is blocked and U.S. persons are prohibited from engaging in transactions with them:

Ali Mamluk and the Syrian General Intelligence Directorate

Ali Mamluk, through the GID, has overseen a communications program in Syria which was directed at opposition groups. The program included both technological and analytical support from Iran's MOIS. Mamluk worked with the MOIS to provide both technology and training to Syria, to include internet monitoring technology. Mamluk has also requested MOIS training and assistance on social media monitoring and other cyber tools for the GID.

The GID has been implicated in serious human rights abuses in Syria, including arbitrary arrests, mistreatment of detainees, and the death of detainees while in GID custody. In one example from July 2011, GID officers arrested and beat surrendered oppositionists after a firefight at a school in Bukamal, Syria. The bodies of the prisoners were later disposed of, some of which had bullet wounds and appeared to have been mutilated with holes drilled into their arms, legs and shoulders.

The GID and Mamluk were originally listed in the annex to Executive Order 13572 of April 29, 2011, "Blocking Property of Certain Persons With Respect to Human Rights Abuses in Syria" ("E.O. 13572").

Syriatel

The Syrian government has directed Syriatel to sever network connectivity in areas where attacks were planned and it also records cell phone conversations on behalf of the Syrian government. Syriatel controls approximately 55% of Syria's cellular phone market.

Syriatel was previously designated in August 2011 under E.O. 13572.

Iran's Ministry of Intelligence and Security

The MOIS has sought to identify members of opposition groups and monitor their activities by obtaining their passwords. MOIS agents have been responsible for the beatings, sexual abuse, prolonged interrogations, and coerced confessions of prisoners following the June 2009 elections in Iran.

MOIS was previously designated in February 2012 under E.O. 13572, E.O. 13553, "Blocking Property of Certain Persons With Respect to Serious Human Rights Abuses by the Government of Iran", and E.O. 13224, "Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism."

Iran's Islamic Revolutionary Guard Corps

The IRGC's Guard Cyber Defense Command (GCDC) includes a special department called the Center for Inspecting Organized Crimes (CIOC). The CIOC focuses on ensuring the regime's vision of cyber security. The CIOC's official website is called Gerdab (www.gerdab.ir), which is a Farsi word meaning whirlpool. The IRGC's CIOC has openly admitted that it would forcefully suppress anyone seeking to carry out "cultural operations" against the Islamic Republic via the Internet and that it monitors Persian-language sites for what it deems to be aberrations.

The CIOC has taken an active role in identifying and arresting protesters involved in the 2009 post-election unrest, particularly those individuals active in cyber space.

The IRGC's CIOC uses extensive methods to identify Internet users, including through an identification of their Internet Protocol (IP) addresses. The Iranian regime has identified and arrested many bloggers and activists through the use of advanced monitoring systems, and the CIOC inspects forwarded emails to identify those critical of the regime. The IRGC's cyber police focus on filtering websites in Iran, monitoring the email and online activity of individuals on a watch list, and observing the content of Internet traffic and information posted on web blogs. Individuals on the watch list included known political opponents and reformists, among others.

Individuals arrested by the IRGC have been subjected to severe mental and physical abuse in a ward of Evin Prison controlled by the IRGC.

The Department of the Treasury previously designated the IRGC in June 2011 under E.O. 13553 and in October 2007 under E.O. 13382 "Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters."

Iran's Law Enforcement Forces

Following the 2009 postelection protests, during which opposition activists used the Internet and social media to document police crackdowns, the Iranian regime identified and arrested many bloggers and activists through the use of advanced monitoring systems. In January 2012, the LEF issued new regulations requiring owners of Internet cafes to install closed circuit television cameras and to register the identity and contact details of users before allowing them to use their computers. Given the LEF's history of serious human rights abuses, its efforts to monitor the Iranian public can reasonably be assumed to assist in or enable human rights abuses by or on behalf of the Government of Iran.

The Department of the Treasury has previously designated the LEF in June 2011 under E.O. 13572 and 13553.

Datak Telecom

The Iranian Internet service provider Datak Telecom ("Datak") has collaborated with the Government of Iran to provide information on individuals trying to circumvent the government's blocks on Internet content, allowing for their monitoring, tracking, and targeting by the Government of Iran. Datak regularly collaborated with the Government of Iran on testing surveillance techniques.

Over the last two years, Datak facilitated ongoing technical surveillance on Iran-based users of a popular commercial email service, designed to monitor and track the activities of its users. Datak undertook plans to carry out this type of attack on a larger scale, to potentially include surveillance of millions of Iranian users.

Moreover, Datak has demonstrated the intent and specific planning to purchase intercept equipment for Internet and voice communications.

Identifying Information
Individual: Ali Mamluk
DOB 1947
POB Amara, Damascus, Syria
Major General
Director, Syrian General Intelligence Directorate

Entity: Syrian General Intelligence Directorate
AKA: IDERAT AL-AMN AL-'AMM

Entity: Syriatel
A.K.A. Syriatel Mobile
A.K.A. Syriatel Mobile Telecom
A.K.A. Syriatel Mobile Telecom SA

Address: Doctors Syndicate Building, Al Jalaa Street, Abu Roumaneh Area, PO Box 2900, Damascus, Syria

Entity: Iranian Ministry of Intelligence and Security
AKA: MOIS
AKA: VEZARAT-E ETTELA'AT VA AMNIAT-E KESHVAR
AKA: VEVAK
Address: Headquarters located in Tehran, Iran; bounded roughly by Sanati Street on the west, 30th Street on the south, and Iraqi Street on the east.
Address: Ministry of Intelligence, Second Negarestan Street, Pasdaran Avenue, Tehran, Iran.

Entity: Islamic Revolutionary Guard Corps
AKA: AGIR
AKA: Iranian Revolutionary Guard Corps
AKA: IRG
AKA: IRGC
AKA: Islamic Guard Corps
AKA: PASDARAN
AKA: PASDARAN-E ENGHELAB-E ISLAMI
AKA: PASDARAN-E INQILAB
AKA: Revolutionary Guard
AKA: Revolutionary Guards
AKA: SEPAH
AKA: SEPAH PASDARAN
AKA: SEPAH-E PASDARAN-E ENQELAB-E ESLAMI
AKA: The Army of the Guardians of the Islamic Revolution
AKA: Iranian Revolutionary Guards
Address: Tehran, Iran

Entity: Law Enforcement Forces of the Islamic Republic of Iran
AKA: Iran’s Law Enforcement Forces
AKA: NAJA
AKA: Niruyih Intizamiyeh Jumhuriyih Iran
AKA: Iranian Police

Entity: Datak Telecom
Address: No. 14, Enbe E Yamin Street, North Sohrevardi Ave., Tehran, Iran

###