The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have released two joint cybersecurity advisories on widespread advanced persistent threat (APT) activity:

1. Joint Cybersecurity Advisory: AA20-296A Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets

2. Joint Cybersecurity Advisory: AA20-296B Iranian State-Sponsored Advanced Persistent Threat Actors Threaten Election-Related Systems

AA20-296A updates a previous joint CISA-FBI cybersecurity advisory and provides information on Russian state-sponsored actors targeting U.S. state, local, tribal, and territorial (SLTT) government networks, as well as aviation networks. In limited instances, this activity has resulted in unauthorized access to IT systems used by U.S. election officials.

AA20-296B details Iranian APT actors working to influence and interfere with the U.S. elections to sow discord among voters and undermine public confidence in the U.S. electoral process. These actors have taken part in spear-phishing campaigns, website defacements, and disinformation campaigns to spread obtained U.S. voter-registration data, anti-American propaganda, and misinformation about voter suppression, voter fraud, and ballot fraud.

Both joint cybersecurity advisories contain information on exploited vulnerabilities and recommended mitigation actions for affected organizations to pursue.

Intergovernmental Affairs
Department of Homeland Security
DHS.IGA@hq.dhs.gov