

State Releases International Narcotics Control Strategy Report

Early in March 2013, the Department of State Bureau for International Narcotics and Law Enforcement Affairs (INL) released the 2013 “International Narcotics Control Strategy Report” (INCSR). The INCSR provides an overview of counternarcotic efforts by the governments of over 90 countries and several U.S. departments and agencies to reduce illicit narcotics production, trafficking, and use in 2012. The two-part report documents efforts to combat all aspects of the international drug trade in 2012, with volume I covering drug and chemical control, and volume II covering money laundering and financial crimes.

Volume I identifies Afghanistan, The Bahamas, Belize, Bolivia, Burma, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Haiti, Honduras, India, Jamaica, Laos, Mexico, Nicaragua, Pakistan, Panama, Peru and Venezuela as major drug transit and/or major illicit drug producing countries. The report also highlights Bolivia, Burma, and Venezuela as countries that have failed demonstrably during the previous 12 months to adhere to their obligations under international counternarcotic agreements and implement the measures set forth by the Foreign Assistance Act of 1961.

Volume I also focuses attention on international counternarcotic training programs that are managed by INL. The INL training is implemented by a variety of U.S. government and law enforcement entities, including the Drug Enforcement Administration, the Federal Bureau of Investigation, Immigration and Customs Enforcement, Customs and Border Patrol, and the U.S. Coast Guard.

Money laundering and other financial crimes are covered in volume II of the INCSR, which lists over 60 countries as major money laundering countries in 2012. This volume also highlights the most significant steps countries and jurisdictions have taken to improve their anti-money laundering/counter-terrorist financing regimes. Volume II also details U.S. government counter-money laundering efforts by the Federal Reserve System as well as the Departments of State, Treasury, Homeland Security, and Justice. **IAJ**

New Directive Addresses Critical Infrastructure Security

In February 2013, the White House released the “Presidential Policy Directive on Critical Infrastructure Security and Resilience” (PPD-21). PPD-21 advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure, and tasks various government entities with securing U.S. critical infrastructure against both physical and cyber threats.

The directive refines and clarifies functional relationships across the federal government to advance national unity of effort to strengthen critical infrastructure security and resilience, while enabling efficient information exchange by identifying baseline data and systems requirements for the federal government. The directive will also implement an integration and analysis function to inform planning and operational decisions regarding critical infrastructure.

The directive also assigns roles and responsibilities to several government departments and entities. Among their specified duties under PPD-21, the Secretary of Homeland Security is responsible for identifying security and resilience functions that are necessary for effective public-

private engagement with all critical infrastructure sectors. The Secretary also develops a national plan in coordination with Sector-Specific Agencies (SSAs) and other critical infrastructure partners, and integrates and coordinates Federal cross-sector security and resilience activities.

SSAs have a variety of duties and roles in addressing threats to each critical infrastructure sector. Among these duties is coordinating and cooperating with DHS and other SSAs, including the Departments of Justice, State, Defense, Commerce, and Interior, as well as the Director of National Intelligence. **IAJ**

White House Releases Executive Order for Improving Cybersecurity

On February 12, the Obama Administration released their Executive Order for improving critical infrastructure cybersecurity. The order creates a policy for addressing cyber intrusions into U.S. critical infrastructure, and enhances the security and resilience of that infrastructure. Critical infrastructure includes national security, economic security, and public health and safety systems. The order also increases the volume, timeliness, and quality of cyber threat information sharing between intelligence and law enforcement entities, while protecting intelligence and law enforcement sources, methods, operations, and investigations.

The new order increases intergovernmental and interagency cooperation, and strengthens U.S. government partnerships with private sector entities. It also establishes a consultative process that requires the coordination of relevant councils, critical infrastructure owners and operators, various agencies, universities, experts, and state, local, territorial, and tribal governments. **IAJ**

Interagency Health Operations Essential to National Security

In a recent interview, Dr. Charles Beadling, director of the Department of Defense Center for Disaster and Humanitarian Assistance Medicine, stated that global health operations have an important role in U.S. national security. “We do feel that there is a strong link between global health engagement and security,” said Beadling, who noted that such efforts reduce insurgency and terrorism.

The Center focuses on the development end of the “three Ds” – diplomacy, defense, and development – and operates under the premise that health is “a global common good.” Beadling also stated that while the Center is still in its early stages of development, it is imperative that they work in close coordination with the U.S. State Department, U.S. Agency for International Development, the United Nations, and nongovernmental organizations to achieve the Center’s mission.

The Center’s Emergency Management and Preparedness Program implemented their first program in Mozambique, in December 2012. **IAJ**