Interagency Cooperation Important to Border Security

From March 18 to March 19, law enforcement professionals gathered in Phoenix, Arizona to take part in the Border Security Expo. The Expo included keynote addresses from high ranking representatives from the Department of Homeland Security, U.S. Customs and Border Protection, U.S. Border Patrol, and U.S. Immigration and Customs Enforcement.

The event also comprised a number of panel sessions that covered a variety of border security topics, including managing and securing the U.S.-Mexico border and strategic partnerships for intelligence sharing.

During these panels, speakers credited interagency cooperation and information sharing with recent high-profile arrests. Panelists also stressed the important role interagency cooperation has in securing U.S. borders, even saying that such cooperation should possibly be federally mandated.

The 2015 Border Security Expo will be held on April 21 and 22, and will focus on countering transnational organized crime. ***IAJ***

Army Pamphlet Calls for Interagency Partnerships

Earlier this year, the Department of the Army released a pamphlet on the subject of engagement. U.S. Army Training and Doctrine Command Pamphlet (TP) 525-8-5, The U.S. Army Functional Concept for Engagement expands on the ideas of TP 525-3-0, The U.S. Army Capstone Concept and TP 525-3-1, The U.S. Army Operating Concept.

The pamphlet includes a section on special warfare activities which, among other things, calls for Soldiers to be trained to work with host nation security forces, host nation governments, international government organizations, nongovernmental organizations, and interagency partners. The pamphlet also focuses on the interdependence of the Army and their unified action partners, including joint, interagency, and multinational partners.

The pamphlet incorporates building partner capacity tenets and establishes a common framework to capitalize on the integrative opportunities all of the warfighting functions provide to future land operations. ***IAJ***

CSO Evaluates Two Years of Engagement

Early in March, the State Department's Bureau of Conflict and Stabilization Operations (CSO) published a report detailing CSO's efforts in its first two years of operations. CSO was established in 2011 to improve the effectiveness and coherence of the U.S. government in conflict situations, and break cycles of violence through locally grounded analysis that focuses on a top-priority opportunity to address conflict.

CSO set three goals when it began: 1) make an impact in three or four countries important to the United States; 2) build a respected team of trusted partnerships; and 3) be innovative and agile. These goals would be met by working with other State Department and interagency partners to understand and reduce conflict.

The report details many examples of CSO's success in addressing conflict in four top-priority countries, including CSO's contribution to more peaceful elections in Kenya and Honduras,

and CSO's role in generating defections from the Lord's Resistance Army. The report also cites partnerships with host governments, civil society, NGOs, the U.S. Agency for International Development, the Department of Defense, and other bureaus within the State Department as being beneficial to CSO's mission. ***IAJ***

GAO Assesses State and USAID Contracting

In February 2014 the Government Accountability Office (GAO) released a report assessing the progress made by the Department of State and the U.S. Agency for International Development (USAID) in addressing issues related to the contracting of other entities, including government agencies, in contingency operations.

GAO's report, GAO-14-229, stems from a mandate in Section 850 of the Fiscal Year 2013 National Defense Authorization Act (NDAA) that requires State and USAID to assess their organizational structures, policies, and workforces related to contract support for overseas contingency operations. It also requires GAO to report on the progress State and USAID have made in identifying and implementing improvements related to those areas.

In their Section 850 report to Congress, the State Department cited actions needed to improve acquisition planning, contract oversight, and interagency coordination, but concluded that its organizational structure was generally adequate to support overseas contingency operations. USAID focused their report to Congress on agency-wide policies, identifying room for improvement in contractor performance evaluations and in data collection, inventory, and reporting. However, GAO notes that in focusing on policy, USAID may have missed opportunities to leverage its knowledge and skills to better support future contingencies.

While both State and USAID have made strides to improve their role in contingency operations, GAO recommends that both agencies continue to assess how the suggested and intended changes will effect contingency contracting and each agency's objectives. ***IAJ***

Cybersecurity Framework to Protect U.S. Critical Infrastructure

On February 12, the National Institute of Standards and Technology released the Framework for Improving Critical Infrastructure Cybersecurity. The framework was developed by hundreds of companies, several federal agencies, and many international contributors as a how-to cybersecurity guide for organizations in the business of running the nation's critical infrastructure, which includes facilities that generate and transmit electricity, as well as those that manage telecommunications, drinking and waste water, food production, and public health, among others.

The framework is a key deliverable from President Obama's 2013 Executive Order on Improving Critical Infrastructure Cybersecurity, and is described by the president as "a great example of how the private sector and government can and should work together to meet this shared challenge." The framework provides a roadmap to improving cybersecurity as well as a way to better communicate with chief executives and suppliers about managing cyber risks.

The framework has three components—core, profiles, and tiers. The core is a set of cybersecurity activities and references that are common across critical infrastructure sectors; the profiles can help an organization align its cybersecurity activities with business requirements, risk tolerances and