Statement By

Lieutenant General Michael D. Barbero
Director
Joint Improvised Explosive Device Defeat Organization
United States Department of Defense

Before the

United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies

July 12, 2012

Chairman King, Chairman Lungren, Ranking Member Clarke, and members of the Subcommittee, thank you for inviting me to speak with you today on the efforts to protect our troops from improvised explosive device (IED) attacks and share some lessons the U.S. military has learned that could be applied to the homeland.

In 2006, the Department of Defense (DoD) established the Joint Improvised Explosive Device Defeat Organization (JIEDDO) to focus on the IED threat in Iraq and Afghanistan. JIEDDO's mission is to lead the Defense Department's actions to rapidly provide counter-IED (C-IED) capabilities in support of combatant commanders through rapid acquisition, tactical operations-intelligence fusion and pre-deployment training. JIEDDO is singularly focused on this problem and exists to rapidly field capabilities to reduce the effectiveness of this asymmetric weapon.

It is clear the IED is the primary weapon of choice for threat networks globally and is one of the enduring operational and domestic security challenges for the foreseeable future. The global proliferation of IEDs and associated technology is pervasive and continues to threaten U.S. interests at home and abroad. Since 2007, IED incidents outside of Iraq and Afghanistan have increased to more than 500 IED events per month, with Colombia having the greatest number of IED events followed by Pakistan, India, the United States, and Syria, which recently moved into the top five[1]. Since January 2011, there have been more than 10,000 global IED events occurring in 112 countries, executed by more than 40 regional and transnational threat networks[2].

The domestic IED threat from both homegrown extremists and global threat networks is real and presents a significant security challenge for the United States and our international partners. In the early 1980s, the Provisional Irish Republican Army used ammonium nitrate-based IEDs in multiple attacks in London. The United States witnessed firsthand just how deadly ammonium nitrate can be in the 1995 Oklahoma City bombing that claimed the lives of 168 American citizens. Most recently, we saw the devastating effects in Mumbai, India, and Oslo, Norway, both attacks used ammonium nitrate as an explosive. Throughout the world these devices and the networks that use

[1]Worldwide IED Database, Institute for Defense Analysis, June 2012
[2]Worldwide IED Database, Institute for Defense Analysis, June 2012

IEDs will remain a threat for decades to come.

Since the successful attacks on September 11, 2001, externally based global threat networks have attempted numerous failed attacks such as the underwear bomb aboard Northwest Airlines fight 253 on Christmas day in 2009, the failed Times Square car bombing in 2010, and the ink cartridges packed with explosives aboard two separate cargo planes in 2010. These attempts clearly demonstrate the commitment of these threat networks to continue to employ IEDs against our homeland in traditional as well as new and creative ways. The use of advanced IED technology and sophisticated tactics, techniques, and procedures provide individuals and transnational networks with cheap and easily accessible means to achieve high visibility effect.

The extremist networks that employ IEDs have proven to be resilient, adaptive, interconnected, and extremely violent. Globalization, the Internet, and social media have extended the reach of these organizations, providing platforms for recruiting, technical exchanges, training, planning, funding, and social interaction. We see IED tactics and techniques used by insurgents increase in sophistication and proliferate globally. Wherever we see turmoil or insecurity we see the spread of these networks and the spread of IEDs.

Today's IEDs are relatively simple, low-tech devices, which routinely use command wire, pressure plates, or radio-controlled triggers. Many readily available components such as cell phones, agricultural fertilizers and simple electronic transmitters and receivers have legitimate commercial uses, but are easily and increasingly adapted for illicit purposes in manufacturing IEDs. The dual-use nature of IED components poses unique challenges in our ability to regulate and limit terrorist access to IED precursors and trigger components.

Future bomb makers will incorporate such enhancements as ultra-thin and flexible electronics; advanced communications mechanisms such as blue-tooth, Wi-Fi, and broadband; optical initiators; and highly energetic metals. In addition to more sophisticated technology, threat networks will develop enhanced IED concealment techniques and may even combine IED use with concurrent cyber attacks.

Today and in the future, U.S. forces will operate in an IED environment. While IEDs cannot stop our units or deter our commanders from taking the fight to the enemy, these devices are the greatest source of combat casualties this decade. The cumulative effects of casualties, both killed and wounded in action, inflicted on our force and magnified by insurgent information operations have made IEDs a challenge for the United States and a top priority for DoD.

To counter the IED and threat networks that employ these devices, JIEDDO focuses our activities along three lines of operation: Defeat the Device, Train the Force and Attack the Network. To enable a successful C-IED program, these lines of operation must work in harmony.

Our first line of operation, defeating the device, is the immediate and most obvious approach to protecting our service members from IEDs. As hard as we try, we cannot stop every IED from being employed. However, once the IED finds its way to the battlefield, we have fielded a wide spectrum of initiatives to detect the components, neutralize the triggering devices, and mitigate the effects of an IED blast. DoD has developed and rapidly deployed a comprehensive portfolio of capabilities, such as mine rollers, electronic countermeasures (jammers), robotics, handheld detectors, pelvic protection garments, and aerial and ground surveillance systems, to name a few. We do not rely on just one capability. Our warfighters are provided an arsenal of tools to customize and apply to the IED threat.

Defeating the device is critical to lowering effective attacks and casualties. If we fail in this task, we could experience an unacceptable level of causalities, resulting in the loss of will and ultimately mission failure. While defeating the device is important it is not decisive. Focusing solely on defeating the device relegates us to playing defense and surrenders the initiative to the enemy.

The second area in which we focus our efforts is training. The Train the Force line of operation brings our deploying warfighters up to speed on the full range of available C-IED tools and the latest tactics, techniques and procedures emerging from theater. A well-trained warfighter is our best C-IED weapon. A comprehensive pre-

deployment training approach is required to ensure our force has adequate time to understand the integration of all aspects of the C-IED fight before deploying to theater.

The third line of operation, Attack the Network, is the decisive endeavor. It encompasses all the material and non-material C-IED enablers to attack the network by first identifying, and then exploiting, critical enemy network vulnerabilities. Attacking the network is the most complex line of operation, but it is how we achieve decisive results.

JIEDDO has built a deep base of knowledge in data fusion and visualization to enable operational intelligence analysis. This analysis, in turn, enables military and interagency customers to attack violent extremist networks by using more than 180 data sources and numerous government and commercial off-the-shelf analysis tools. We have five intelligence agencies embedded within our organization to cross train on the various tools, processes and best practices.

The key enabler for achieving seamless sharing of information begins with applying new techniques to enhance data processing upon intake. The better we can sort or mine data, the faster our analysts can manipulate this information to produce actionable intelligence for our leaders and actionable evidence for our interagency partners. The speed at which these threat networks operate mandates our ability to produce faster analytical assessments of emerging operational environments to support rapid exploitation. This requires us to think differently and expand our community of action to share and fuse information among domestic and international partners.

Today, JIEDDO is working with an expanded community of action for C-IED that did not exist previously. We have established an interagency forum consisting of U.S. intelligence and interagency partners, federal law enforcement, the Five Eyes (United States, United Kingdom, Canada, Australia, and New Zealand) community, and forward-deployed forces to achieve a more transparent and broader whole-of-government effort to disrupt threat networks employing IEDs against U.S. and Coalition forces globally.

We recognize no single government department or international partner has the ability to fully limit access to IED precursors, so we are integrating our efforts to go after the threat networks that distribute these materials. Our U.S. government partners bring

expertise in: defeating and prosecuting criminal networks; applying financial pressures by going after the assets of IED network members, financers, and distributors; enacting export controls and treaty compliance efforts that lead to the interdiction of IED components; advancing C-IED objectives through public diplomacy and policy and regulatory changes; advising on legitimate agricultural requirements; and coordinating and executing domestic C-IED efforts through the Department of Justice Joint Program Office. This is by no means a comprehensive list of the actions our interagency partners are applying to the C-IED fight, but it should give you an idea of the collaboration that is occurring on all levels.

To provide a couple of specific examples, the U.S. Department of Commerce added 152 persons to the Entity List because of IED-related matters. This designation stops U.S. companies from trading with these entities — companies, organizations, persons — who violated U.S. export laws. Since October 2010, the U.S. Department of Treasury has imposed economic sanctions on 33 Afghanistan-Pakistan IED facilitators. Through coordinated efforts and strong partnership across the U.S. government and with our international partners, we are going after these nefarious actors and effectively countering the networks that use IEDs.

During the past eight years, JIEDDO in conjunction with the military services, U.S. interagency, and our multinational partners develop a highly effective process to target extremist networks and defeat the IED. Weapons Technical Intelligence (WTI) evolved from "traditional technical intelligence"[3] and leverages law enforcement techniques as well as forensic and biometric technology to collect, exploit, and analyze IED-related materials and other weapons systems[4]. This process coordinates and integrates various DoD and Federal organizations and programs to facilitate everything from the onsite collection of IED material to the analysis of IED components in national laboratories. This analysis is then delivered to our military commanders to support

[3] "Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages. Also called TECHINT." Joint Publication 1-02, 15 January, 2012.

[4] WTI is "a category of intelligence and process derived from the forensic and technical exploitation of improvised explosive devices (IEDs), associated components, improvised weapons, and other weapons systems." WTI IED Lexicon, Edition 3.1, July, 2011.

targeting, track IED materials to their source, aid in host nation criminal prosecution, and enhance force protection for our nation's warfighters.

The WTI process has proven its utility in defense of the homeland as well. An example of this is the 2011 arrest and indictment of two Iraqi nationals, Waad Ramadan Alwan and Mohanad Shareef Hammadi, on federal terrorism charges in Bowling Green, Kentucky. The Federal Bureau of Investigation (FBI) had an ongoing counterterrorism investigation that identified the two subjects as having supported the activities of insurgents in a specific part of Iraq from 2003-to-2006. The Terrorist Explosive Device Analytical Center, operated by the FBI in partnership with JIEDDO and other governmental stakeholders, supported the ongoing FBI counterterrorism investigation by using biometric data collected by U.S. forces and forensic techniques to definitively link Alwan to components collected from an unsolved IED event in Iraq during that time period. This is a textbook example of how WTI enables the military to contribute to a whole-of-government solution to a transnational threat. It further illuminates the importance of a seamless integration, U.S. forces operating outside of the United States collecting intelligence that is placed into a shared database used by law enforcement to protect the homeland.

The benefit of the WTI process has unlimited potential and applicability to defeat improvised weapon systems that provide our enemies an asymmetric advantage. Our commanders increasingly focus operations to collect biometric data, and several have referred to it as a game-changer. Biometric, forensic, and technical exploitation remove a violent extremist's greatest defense — anonymity — and makes them vulnerable to attribution. The WTI process provides a valuable framework for collecting, exploiting, analyzing, and disseminating data in a timely manner to those who need it most.

Emerging technologies such as standoff biometric collection, rapid DNA processing, and real-time latent fingerprint matching hold enormous potential to advance the WTI process into the next generation of protection. These capabilities will allow security personnel to identify threats before they reach checkpoints and to instantaneously attribute criminal and illicit activities to the perpetrators.

Moving forward, we will continue to face an ever-present threat from the overlapping consortium of threat networks employing IEDs as their weapon of choice. Mitigating the global IED threat requires a whole-of-governments approach. We must continue to synchronize C-IED and counter-threat network capabilities and actions among national, international, and other security stakeholders. These adaptive and constantly evolving threat networks require an agile and responsive counter-threat network to defeat them.

It is imperative we capture and institutionalize the lessons of a decade of combat operations. These lessons may help fill some current domestic-capability gaps which would strengthen our protection of the homeland. There is no silver bullet to defeat an emplaced IED; our best defense is a warfighter or first responder with the right intelligence, training, and equipment. Chairman King, Chairman Lungren, Ranking Member Clarke, members of the Subcommittee, again, thank you for the opportunity to appear before you today. I look forward to your questions.