From:	b6, b7C USAILC) </O=USA/OU=ILC/CN=RECIPIENTS/CN= b6, b7C >
Sent:	Monday, March 24, 2014 5:01 PM
To:	
Subject:	USAO – Central District of Illinois: Summary on Terrorism, Homeland Security and Crime – March 24, 2014 (U)
Attach:	Summary on Terrorism and Criminal Acts 3-24-2014 u.pdf

Summary on Terrorism, Homeland Security and Crime – March 24, 2014

NATIONAL SECURITY AND TERRORISM NEWS

Abu Ghaith Trial - Bin Laden Associates Show No Remorse in Statements - Closing arguments are set for today in Manhattan in the trial of accused al Qaeda propagandist ***Sulaiman Abu Ghaith***. In public statements made a week apart, ***Khalid Sheik Mohammed***, al-Qaida's self-professed Sept. 11 mastermind and a Kuwaiti imam who met with *Osama bin Laden* in a cave soon after the attacks once again demonstrated that time hasn't softened their *anti-American views*. Mohammed's words emerged a week ago in a written statement responding to more than 400 questions from defense lawyers in their failed bid to win the court's permission to have him testify on behalf of Abu Ghaith, who is on trial on charges that he conspired to kill Americans and aid ***al-Qaida*** after the terrorist attacks.

Mohammed remains devoted to bin Laden, killed in a 2011 U.S. attack, saying the al-Qaida founder was "*very wise in every order he gave us*." And he was especially proud of what he claimed was *al-Qaida's cost to the American economy*. He said "*every state of emergency declared and change of alert level*" on the military and civilian sectors cost the country millions of dollars and the wars waged by the U.S. after Sept. 11 have cost it about a trillion dollars, "*the bleeding of which continues to this day.*" A judge ruled jurors at Abu Ghaith's ongoing trial won't see Mohammed's statement. *But they received a lesson in jihad from the defendant, who took the unusual step of taking the witness stand and — rather than try to distance himself from al-Qaida — described in detail how bin Laden summoned him to his mountain hideout in the hours after the Sept. 11 attacks and enlisted him as the terror group's mouthpiece.* (Associated Press – 3/22)

FBI Officials Describe Boston Marathon Bombing Manhunt in "60 Minutes" Report - CBS' 60 Minutes featured a lengthy report on the Boston Marathon bombings and the FBI's subsequent investigation into the attack and manhunt for the suspected perpetrators, brothers **Tamerlan** and **Dzhokhar Tsarnaev**. The program offered the "*inside story*" of how the FBI led a task force of more than 1,000 Federal, state and local agents. Rick DesLauriers, formerly the head of the FBI's Boston office, took over the biggest investigation of his life just months before his anticipated retirement, and explained that FBI Director Robert Mueller had ordered support for the investigation from every FBI office. DesLauriers was linked to FBI headquarters by executive assistant director Stephanie Douglas, also interviewed for the program, who explained the initial fears of additional attacks not only in Boston but across the country. (CBS' 60 Minutes – 3/23)

Douglas and DesLauriers described the "*turning point*" In the investigation when authorities first noticed a man wearing a white hat placing a backpack on the ground in the middle of a crowd of spectators. Described as the "*eureka*" video, the footage has not been shown to the public and is being held for the trial of **Dzhokhar Tsarnaev**. The FBI stands by its decision to release the photos of the ***Tsarnaev brothers***, despite the death of an MIT police officer, Sean Collier, shortly after their release. Former head of the FBI's Boston office Vincent DesLauriers explained that "*Nobody could have reasonably foreseen that a police officer would have been murdered.*" (CBS News - 3/21; CBS Evening

News - 3/22; Boston Globe)

FBI Agent is cleared in Fatal Shooting of Man Tied to Boston Suspects - An FBI agent who fatally shot a Chechen man with links to the Boston bombing suspects during an interrogation has been cleared of wrongdoing by a prosecutor in Florida and by an FBI internal review. A soon-to-be-completed Justice Department inquiry is also expected to conclude that the agent followed proper guidelines on the use of force when he killed the Chechen, **Ibragim Todashev**. (New York Times – 3/22)

Iran becoming serious Cyber-Warfare Threat - Both government and private cybersecurity experts are increasingly considering Iran as a "*top ten*" *cyber-threat*. Iran's recent activities and its motives have led analysts to rank the country among other cyberspace heavy hitters such as ***Russia*** and ***China***. American officials believed that several recent computer attacks could be traced to Iran. These targets, included several American oil, gas and electricity companies, as well as financial institutions on Wall Street and large systems operations. Further, an official with ties to the DHS told the newspaper that, "*most everything we have seen is coming from the Middle East.*" (Christian Science Monitor – 3/16)

The ***distributed denial of service*** attacks, which characterized much of last year's activity, had abruptly stopped and, following a quiet period, have recently been resumed, but against a much more alarming target — the U.S. military. Recently, attacks have included the US Navy's Intranet, the largest unclassified network in the service's arsenal. It took four months to remove the hackers from the system. It is these much more damaging and costly infiltrations that have officials take a much more apprehensive view of Iran's growing cyber capabilities. (Homeland Security News Wire - 3/24)

FISC Judge says DOJ Failed to Inform Him of NSA Evidence Ruling - Judge Reggie Walton, the chief judge on the *Foreign Intelligence Surveillance Court*, on Friday took the Justice Department to task for failing to inform the court that a federal court in California had issued orders to preserve phone data collected in a government surveillance program. Judge Walton said the Justice Department should have made him aware of the preservation orders, and is demanding a written explanation from government lawyers. (The AP - 3/21)

Report: **NSA Breached Huawei's Servers** - Even as the United States made a public case about the dangers of buying from **Huawei**, the Chinese telecommunications giant, classified documents show that the National Security Agency was creating its own back doors — directly into Huawei's networks. The agency pried its way into the servers in Huawei's sealed headquarters in Shenzhen, China's industrial heart, according to NSA documents provided by the former contractor Edward Snowden. It obtained information about the workings of the giant routers and complex digital switches that Huawei boasts connect a third of the world's population, and monitored communications of the company's top executives. (New York Times – 3/23) **Related**: China's Huawei Condemns Reported NSA Snooping (Reuters) Revelations of NSA Spying Cost U.S. Tech Companies (New York Times)

Russia Evaded U.S. Eavesdropping Ahead of Crimea Incursion - While US military satellites captured images of Russian troops massing on the Crimean border last month, intelligence analysts had not intercepted any communications of Russian officials discussing plans to invade. U.S. officials now believe that Russian military planners may have taken steps to evade U.S. eavesdropping. In response, U.S. intelligence agencies and the military are expanding satellite coverage and communications-interception efforts across the region. (The Wall Street Journal - 3/24)

Another look at a French 'Lone Wolf' - Two years ago, when most media reports were generally parroting French officials' claims that the deadly attack in March 2012 by *Toulouse shooter* ***Mohamed Merah*** was a "*lone wolf*" - type operation by a disadvantaged youth. **Merah** had been trained in Pakistan by a Swiss jihadist named **Moezeddine Garsallaoui**, who was the leader of the *al Qaeda-linked* ***Jund al Khilafah*** until he was killed, most likely by a drone strike, in Miram Shah, North Waziristan, Pakistan in

October 2012. (The Long War Journal - 3/24)

Last December, **Urynbasar Munatov**, a 26-year-old Kazakh arrested in Pakistan in the fall of 2012, found guilty of terrorism and sentenced to 20 years in prison, revealed during questioning that he had discussed the apprentice terrorist (Merah) with **Moez Garsallaoui**, a Belgian-Tunisian who was responsible for ***al-Qaida in Europe***. Garsallaoui had talked of the presence of the French Algerian in his training camp in Pakistan, a camp called Miran Shah located in the province of Waziristan. The camp was dedicated to the training of European jihad candidates. Urnybasar himself had been there. (The Jerusalem Post – 3/23)

Iraq: **Maliki Appears Headed for Reelection** - Despite a gridlocked parliament, sectarian fighting, and his many political enemies, Iraqis are expected to reelect Prime Minister Nouri al-Maliki to a third four-year term on April 30. Maliki's apparent strong position going into the voting is an indication that voters either support him or have few alternatives. While Maliki's support among the Shiite Arab majority has declined, the rest of the field is divided and there is little or no leadership among those who oppose him. (Wall Street Journal - 3/24)

Islamist Militants providing Social Services in Fallujah - Al-Qaida-inspired militants in Fallujah have begun providing social services, policing the streets and implementing Shariah rulings in a bid to win the support of its Sunni Muslim population. As gunmen in ski masks patrol the streets, they also perform a sort of community outreach including repairing damages electricity poles, clearing garbage, and planting flowers. They have also made themselves the law in the city and aim to show they are acting to prevent crime. It is all part of an effort by the ***Islamic State of Iraq and the Levant*** (ISIL) to increase its appeal among the broader Sunni minority in Iraq, where resentment against the Shiite-led government runs deep. (The AP - 3/24)

Turkey Shoots Down Syrian Jet - Turkey's military shot down a Syrian jet Sunday after it allegedly strayed into Turkish airspace during fierce fighting between Syrian rebels and government forces, threatening to escalate tensions between the two countries. There has been *no indication that Syria planned to retaliate for the attack, which marked the first time Turkey has shot down a plane since Turkish Prime Minister Erdogan threw his government's support behind Syria's rebels nearly three years ago*. (Washington Post - 3/24)

Weapons Trafficked Freely in Libya - Libya is awash in millions of weapons with no control over their trafficking. The arms free-for-all fuels not only Libya's instability but also stokes conflicts across the region as guns are smuggled over the borders. The US and Europe are "*alarmed*" about the "*weapons chaos*" and diplomats, including Secretary of State Kerry, "*pressed Libyan officials to reach some political consensus so the international community can help the government collect weapons and rebuild the military and police*." A Western diplomat said the lack of a central government in Libya creates added difficulties for the international community, because Europe and the US simply don't know who to talk to. (The AP - 3/22)

Bomb Explodes on Libyan Airport Runway - A bomb exploded on the runway of Libya's Tripoli International Airport on Friday, according to Transportation Minister Abdelqader Mohammed Ahmed. The airport is considered one of the best guarded locations in the country, but unknown individuals were able to reach the runway, plant the bomb, and detonate it using a timer. (Reuters - 3/22)

Obama Orders Osprey Aircraft, Special Forces to Uganda to Aid Hunt for Kony - The President has ordered a sharp increase in the number of U.S. Special Forces in Uganda and sent U.S. military aircraft there for the first time in the ongoing effort to hunt down *warlord* ***Joseph Kony*** across a broad swath of central Africa. According to Amanda Dory, deputy assistant secretary of defense for *African affairs*, at least "*four CV-22 Osprey aircraft will arrive in Uganda by midweek, along with refueling aircraft and about 150 Air Force Special Forces and other airmen to fly and maintain the planes*." The Ospreys will be used for troop transport and that the rules of engagement for U.S. forces remain the

same as for about 100 Special Operations troops that Obama first sent to help find Kony in October 2011.

U.S. personnel are authorized to provide information, advice and assistance to an African Union military task force tracking **Kony** and his organization, the **Lord's Resistance Army** (LRA), across Uganda, the Central African Republic, South Sudan and Congo. While combat-equipped, they are prohibited from engaging LRA forces unless in self-defense. The LRA poses no threat to the United States, but the administration sees assistance to the A.U. mission as a useful way to build military and political partnerships with African governments in a region where al-Qaeda and other terrorist organizations are rapidly expanding, as well as to demonstrate adherence to human rights principles. (Washington Post - 3/24)

DOMESTIC EXTREMIST THREATS

The Man Bringing Back the Nazi Movement in America - **Andrew Anglin** has built a very popular site for *white supremacists* called the ***Daily Stormer***. In less than a year, his web site has become the premiere news venue online for white nationalists, a veritable Drudge Report for Nazi sympathizers and anti-Semites. Each day, its 29-year-old founder curates a constant stream of stories and events from around the world and repackages them as further testament to society's moral decline, his movement's enduring race war and the country's Jewish problem. (VOCATIV.COM – 3/20)

HOMELAND RESPONSE

7 Leadership Lessons from the SEALs Commander Who Got bin Laden – You're probably not leading troops on a Special Forces raid. But the principles espoused by elite military units can help you become a better leader. Three years ago, U.S. Navy SEALs staged a daring raid into Pakistan, where they caught and killed the world's most-wanted terrorist. The mission to get Osama bin Laden was highly dangerous, and it ranks among the boldest strikes in the history of U.S. special operations. The man who planned and commanded the raid, Admiral William McRaven, is a veteran leader who served at every level of the SEALs and who literally wrote the book on special operations. Recently, McRaven gave a speech at West Point about the top lessons of his 36-year military career. You can click here to read his entire address, but you'll find some of his key points about truly great leadership below. (Inc.com – February 2014)

Malaysia says MH370 crashed into Indian Ocean – Malaysia Airlines Flight MH370 crashed into the southern Indian Ocean, Najib Razak, Malaysia's prime minister, announced on Monday evening. Mr. Najib said that based on new analysis from Inmarsat, a British satellite company, and UK investigators, the Malaysia Airlines flight had flown to a part of the Indian Ocean where there are no places to land. The news comes 16 days after the Boeing 777 passenger jet vanished in the early hours of March 8 after taking off from Kuala Lumpur on a routine red-eye flight to Beijing. (Financial Times – 3/24)

US, UK Providing Australia with Intel for Search - This morning the U.S. and British intelligence agencies provided information that focused the search in the Indian Ocean, according to the Australian military and other sources. The Australian military said Sunday that the UK and the US, in conjunction with Australia, have been "*acquiring and reviewing satellite imagery from a variety of commercial and government sources.*" (Wall Street Journal - 3/24)

CTA train hits O'Hare platform - An eight-car ***Chicago Transit Authority*** (CTA) Blue Line commuter train plowed across a platform and scaled an escalator at an underground station at one of the nation's busiest airports early Monday, injuring 32 people on board. The accident happened around 2:50 a.m., one of the station's lightest traffic times. More than 50 firefighters and paramedics responded to the scene, with rescue workers first scrambling to determine if anyone was trapped underneath the cars. All of the injured, however, were aboard the train and were taken in fair or good condition to four hospitals.

The eight-car train remains wedged near the top of an escalator used by commuters at the airport's Blue Line terminal. The cause of the accident remains under investigation. The train was traveling at a high rate of speed while pulling into the station and officials are trying to determine why. Investigators will be looking at equipment, signals, and human factor.
The National Transportation Safety Board also will investigate the crash. (Chicago Tribune, AP – 3/24)

Georgetown Student Arrested for Possessing Ricin had Previously Threatened Fellow Student - Daniel Harry Milzman, 19, was charged Friday for allegedly making *toxic **ricin*** and storing it in his dorm room, and notes that a recent Georgetown graduate claims she reported Milzman to school authorities for making aggressive online comments toward another student earlier this year. The recent graduate said she was "*alarmed*" when she found messages that he posted on Facebook targeting another student. **Milzman** is facing Federal charges for possession of over *120 milligrams of ricin*. (Washington Post - 3/22)

The ricin was first reported when **Milzman** showed it to his residential adviser, who immediately contacted the school's counseling services. Milzman was interviewed by FBI agents later that day, and the substance was tested at an FBI laboratory to confirm that it did, indeed, contain ricin. Jacqueline Maguire confirmed that Milzman remained in custody Friday pending a hearing on March 25. An FBI affidavit outlining the allegations against Milzman said he researched how to make ricin on his phone and bought the ingredients at local retail stores. Andrew Ames, a spokesman for the FBI's Washington Field Office, again noted that "*Based on our investigation, we do not believe there is any connection to terrorism.*" (Reuters, USA Today)

Wisconsin: Wauwatosa Man Arrested after Explosive Materials Found in Madison Home - Police arrested **Andrew T. Cockerham**, 20, on suspicion of possession of an explosive device, after officers found materials to make an explosive device at a Madison residence. The Madison Police Department says it got a report of suspicious material in an apartment on Saturday afternoon. Officers found items and documents indicating the manufacturing of an explosive device. Police seized the materials and stabilized them. Police did not release any information about intent or motive, but said there is no ongoing threat to the community. The investigation is ongoing. (Wisconsin State-Journal, WISC-TV - 3/22)

Supreme Court to Consider Legality of Warrantless Cell Phone Searches - The Supreme Court in April will hear oral arguments on whether a *police search of a cell phone after an arrest without a warrant runs afoul of the Fourth Amendment's prohibition of unreasonable searches and seizures*. Court observers say it *may signify an early effort by the justices to update old privacy doctrines in light of new technology at a time when privacy and technology – thanks to the disclosure of widespread surveillance by the National Security Agency – are at the forefront of the public consciousness*. Privacy advocates and the law-enforcement community are divided sharply over the societal costs and benefits of limiting the search incident to arrest doctrine. Privacy advocates say warrantless searches of cell phones – in particular smartphones – are far too invasive, chill the use of communications technology and leave too much room for abuse, while law enforcement backers say restricting such searches will seriously impede them. (Newsweek - 3/28)

Police Nationwide Tight-Lipped about Cell Phone-Tracking Technology - Police nationwide may be intercepting phone calls or text messages to find suspects using a technology tool known as ***Stingray***, but they are refusing to turn over details about its use or heavily censoring files when they do. Police say ***Stingray***, a suitcase-size device that pretends it's a cell tower, is useful for catching criminals, but they will not disclose details about contracts with the device's manufacturer, *Harris Corp.*, insisting they are protecting both police tactics and commercial secrets. The secrecy surrounding the technology, at times imposed by nondisclosure agreements signed by police, pits obligations under private contracts against government transparency laws. (The AP - 3/22)

Deadly Chemical Weapons Buried Under U.S. Soil - The United States is still struggling with its

own "*deadly stockpiles*" of chemical weapons, which remain buried and await cleanup at a cost of billions of dollars. The *Redstone Arsenal in Alabama* is the largest of the 249 sites and has been referred to as "*the largest and most challenging*" repository. The cleanup team is scheduled to begin work at Redstone next year, but will not actually begin digging until 2019, with disposal conservatively expected to be completed in 2042. (The Los Angeles Times - 3/22)

Internet-Connected Devices are being used in Elaborate Online Crimes - Household devices that are connected to the Internet are being broken into and taken over by hackers and are then being "*used to spread malicious spam or launch a massive cyberattack – disrupting services or shutting down entire networks.*" Analysts predict that, by 2050, there will be 50 billion Internet-connected devices, or five such gadgets for every man, woman and child on the planet leading to the expectation that these types of attacks will rise as well. U.S. regulators, such as the FTC, are starting to address this issue and *security experts are now calling on manufacturers to build more encryption into these devices and add safeguards that prevent them from running other programs.* (Los Angeles Times - 3/23)

Mastercard, Visa Increase Payment Security Focus - Both Mastercard and Visa are stepping up their focus on *payment security*, including the use of smart card chip technology already in use in Asia, Canada, and Europe. Such cards contain integrated circuits that "*generate a unique code for every transaction, which make it nearly impossible for the cards to be used for counterfeit activity.*" The two card companies already had set October 2015 as the deadline for implementing the technology, but "*the new initiative, which includes banks, credit unions, merchants, manufacturers and industry trade groups, will also work on ways to better protect online and mobile transactions.*" (Los Angeles Times - 3/23)

California DMV Notified of Breach in Card Payment Processing System - Law enforcement authorities notified the California Department of Motor Vehicles of a possible security breach in its credit card payment system, but the agency said it had no evidence that its overall computer system had been breached. The story was broken by Brian Krebs, the same security blogger who broke the story of Target's breach. Krebs said stolen information included "*credit card numbers, expiration dates and three-digit security codes*," although it was *unclear if other sensitive information – such as driver's license or Social Security numbers – was also taken*. Affected transactions apparently took place between Aug 2, 2013, and Jan. 31 of this year. (The Los Angeles Times - 3/23)

Examining the Structure, Organization, and Processes of the International Market for Stolen Data - Over the last two decades, consumers have come to depend on computers and the Internet to engage in commerce and manage their finances. Businesses also rely on these technologies in order to process and maintain consumer data in massive databases. As a result, there has been a substantial increase in the risk of theft and fraud stemming from cybercriminals who can compromise these resources to their advantage. Recent evidence suggests that hackers who acquire sensitive consumer data sell this information to others in on-line forums for a profit. In turn, an underground economy has developed around the sale of stolen data, involving various resources that can be used to convert electronic data into real world currency and engage in various forms of cybercrime.

The market for stolen data is a real threat to consumers and businesses alike. Victims from around the world can be harmed by the sale of personal information to facilitate identity theft, while financial service providers must reimburse victims for economic damages. The massive number of data sellers and the general pricing structures observed suggest that there is no easy or immediate way to disrupt or deter offenders engaged in these markets. Thus, there are a range of policy implications that must be considered in order to increase the efficacy of law enforcement responses and consumer protections. (NCJRS - March 2014)

National, State, and District Criminal Law

Meth Entering U.S. Mainly through California, report says - California has emerged as the *major gateway for methamphetamine* into the country, with *Mexican organized crime groups* smuggling

an estimated *70% of the U.S. supply through state border crossings*, according to a report released Thursday by state Atty. Gen. Kamala D. Harris. The 98-page report on trends in *transnational organized crime* also cites *maritime smuggling*, *money laundering* and *criminal alliances* between *Mexican drug cartels and Southern California gangs* as growing public safety threats. The report's release comes at a time of severe budget cuts at the state Department of Justice. In 2012, the Bureau of Narcotics Enforcement was shuttered, dropping the number of state-led drug task forces from 55 in 2011 to 17 in 2013. (Los Angeles Times – 3/20)

The amount seized at the San Diego ports of entry tripled between 2009 and 2013, to more than 6,000 kilos, or 13,200 pounds. By comparison, about 1,000 kilos, or 2,200 pounds, were seized at border crossings in South Texas in 2013. California's sharp increase is probably related to the rise of the ***Sinaloa drug cartel*** as the dominant organized crime group in Baja California. The organization imports the precursor chemicals from China and India, refines the drug at superlabs in Mexico, then ships it across in vehicles into San Diego. (California Attorney General - Transnational Organized Crime Summary – March 2014)

Illinois: Two Virden men arrested on Meth Charges - On Thursday after officers served a search warrant and walked in on an *active methamphetamine lab*, **Patrick Scroggins**, 53, and **Michael Devries**, 42, were taken into custody. They face possible charges of participation in methamphetamine manufacturing, possession of meth manufacturing materials, unlawful possession of meth and unlawful possession of meth precursor. "*This was an important, successful operation that we hope will put a large dent in the meth problem in the area*," Virden Police Chief Mark Bridges said in a news release. Virden police and the South Central Illinois Task Force served the warrant. (State Journal-Register (IL) - 3/22)

Prosecutors using More Aggressive Tactics against White-Collar Criminals - Former arms sales executive Richard Bistrong's experience as an undercover cooperator in white-collar criminal investigations, notes that *methods previously used in drug and racketeering cases are now being used more frequently in the executive suite*. For two-and-a-half years, Bistrong assisted prosecutors by monitoring meetings and recording conversations, and his efforts contributed to bribery charges against 22 individuals. All went free after the government case fell apart, however, and Bistrong himself was sentenced to 18 months in prison on bribery-related charges. He now hopes to work as a consultant, helping companies avoid ***Foreign Corrupt Practices Act*** violations. (The Wall Street Journal - 3/24)

b6, b7C
District Intelligence Specialist
US Attorney's Office, Central District of Illinois
318 S. 6th Street
Springfield, IL 62701
Direct Line: (217) 492-b6, b7C
FAX: (217) 492-b6, b7C
Email: **b6, b7C** @usdoj.gov