Addressing a Spectrum of Threats: Interagency Challenges to Mitigating Threats and Safeguarding Liberties

by Harry Phillips

> ***"In my judgment the most important political rules are: never relax vigilance; expect nothing from the magnanimity of others; never abandon a purpose until it has become impossible, beyond doubt, to attain it; hold the honor of the state as sacred. The time is yours; what its fulfillment will be depends upon you."***
>
> ***Karl von Clausewitz***

The relevance of Clausewitz's admonition has never been more relevant to the security of the U.S. With myriad threats both overseas and at home, it is vital for national security efforts to encompass the spectrum of threats, both domestic and international. The realities of the modern, global security environment warrant incorporating complementary strategies for securing national security interests at home and abroad. This article explores the growing complexity of threats to U.S. international and domestic security interests as they relate to the need for integrated information sharing while simultaneously protecting the civil liberties of U.S. citizens.

U.S. national security interests face a wide range of threats both at home and abroad. Many of these threats overlap and interact with, as well as influence, each other. The activities of transnational organized crime groups, international drug trafficking organizations, terrorist groups, and homegrown violent extremists have the potential for intersecting in ways that undermine U.S. national security interests. Cyber events, terrorism, drug trafficking, and other criminal activities combine to challenge U.S. national security and law enforcement capabilities. Rapidly changing threats where nation states and non-state actors are capable of inflicting harm on vital

Lieutenant Colonel Harry V. Phillips, U.S. Army, Ret., is a former military intelligence officer who currently works for the FBI. He earned a Masters of Strategic Studies from the U.S. Army War College and a Masters of Military Arts and Science from the U.S. Army Command and General Staff College. He is the FBI's Senior Intelligence Liaison to the Pennsylvania State Fusion Center.

U.S. interests warrant the ongoing development of interagency intelligence information-sharing systems. These activities are critical to the future security needs of the U.S. in terms of proactive information sharing among federal, state, and local agencies responsible for protecting U.S. interests at home and abroad.

From national-level capabilities to those at the local level, cohesion has never been more important...

In an era of increasingly diverse and complex threats to the homeland, the U.S. needs an enhanced interagency coordination mechanism to detect and prevent terrorist attacks on the homeland. The integration of the capabilities available to all levels of jurisdiction (federal, state, and local) is necessary for an effective counterterrorism program. From national-level capabilities to those at the local level, cohesion has never been more important in terms of securing America's national security interests. Success requires the interaction among agencies at all levels to be coordinated, proactive, and when necessary disruptive to those intending to harm U.S. interests at home and abroad. Drawing on the capabilities of agencies at every level forges the ability to adapt to a rapidly changing threat environment in a cohesive manner. Improving the ability of the interagency to detect and disrupt threats is integral to U.S. counterterrorism efforts.

Improving interagency cohesion by integrating state and local agencies serves to facilitate predictive intelligence in support of mitigating terrorist threats and facilitates decision making and determining resource allocation. Conversely, the reluctance to share information inhibits leveraging cross jurisdiction capabilities and limits the ability of a key component of the interagency counterterrorism effort, state and local law enforcement agencies. Inhibiting access to intelligence information degrades the ability of state and local agencies to provide for the public's safety. Sharing intelligence information in a proactive manner enhances the ability to coordinate all levels of jurisdiction and facilitates:

- Proactive engagement with local communities to identify threats.
- Intelligence analysis and dissemination of actionable intelligence.
- Deliberate planning vice working in crisis action mode.
- Effective integration of operations with intelligence.

At the heart of the challenge for the U.S. interagency is an inherent unwillingness to share investigative information among agencies. The ability to identify and quickly respond to emerging threats requires agencies across all jurisdictions to share information. By doing so, they serve the needs of an entire community, rather than the parochial interests of a single agency. Preventing attacks such as those on September 11, 2001, and at the Boston Marathon on April 15, 2013, requires an integrated national security strategy and intelligence-sharing capability. Creating such a capability is an imperative in the face of increasingly complex threats that are adapting and changing more rapidly than at any time in history.

Enhancing national intelligence information-sharing capabilities that integrate federal, state, and local law enforcement may potentially alleviate the gaps in knowledge that challenged counterterrorism efforts in the past and facilitate greater situational awareness about potential threats. Threat information shared across jurisdictions is vital to enhancing

the ability of agencies at all levels to detect and disrupt potential threats. State and local law enforcement agencies would benefit from having federal information and vice versa. Such information, in turn, could help to facilitate focusing resources at the right place and time in the effort to disrupt a potential threat.

The challenge for the U.S. interagency is to integrate overlapping domestic and international security strategies into a cohesive national endeavor. The threat environment today impacts U.S. interests globally, with a view toward undermining its Constitutional foundation. International threats include terrorist organizations, rogue states, instability in key regions, international drug trafficking organizations, and non-state actors and rising peer competitors on the global stage. Domestically, law enforcement agencies work to disrupt violent gangs, crimes against children, drug traffickers, transnational organized crime, home grown extremists, and domestic terrorists. Both sets of threats, which at times may overlap, combine to influence national security decision making. Today's threats require the interagency to understand how overlapping threats impact both domestic and foreign policy within the context of an overall national security strategy.

In a speech before Norwegian government officials on July 8, 2014, U.S. Attorney General Eric Holder addressed the issue of individuals traveling to Syria to fight and then returning home intent on conducting terrorist acts in their home countries.[1] Holder's remarks served to underscore the importance of international cooperation to combat increasingly complex international threats to domestic security. In his speech Holder stated, "…we need the benefit of investigative and prosecutorial tools that allow us to be preemptive in our approach to combating this problem." He emphasized protecting the privacy of U.S. and non-U.S. persons, noting recent information-sharing agreements with the European Union prioritize adhering to data privacy principles. He encouraged nations that share fundamental views about privacy to act collaboratively in the exchange of terrorism-related intelligence, with a view toward protecting individual privacy.

The challenge for the U.S. interagency is to integrate overlapping domestic and international security strategies into a cohesive national endeavor.

In his speech he went on to outline a multilateral strategy for countering violent extremism. The four elements of the strategy include:

- Ensuring laws are in place to allow governments to effectively police threats.
- Using law enforcement investigative tools that protect individual rights.
- Strengthening information sharing to facilitate disrupting threats.
- Integrating public engagement and community outreach.

Holder's Oslo speech referenced the "Rabat Memorandum of the Global Counterterrorism Forum." He quoted the memorandum stating, "Because terrorism often transcends national boundaries, timely and effective international cooperation is indispensible to a criminal justice response to terrorism." The Rabat Memorandum outlines practices for effective counterterrorism, which by their nature fit with U.S. interagency counterterrorism protocols.[2] These practices include:

- Protecting individuals involved in counterterrorism cases.

- Encouraging cooperation among domestic counterterrorism agencies.
- Providing legal frameworks and measures for counterterrorism investigations.
- Adopting incentives to induce cooperating in counterterrorism investigations.
- Enacting measures to protect sensitive information on terrorism cases.
- Providing for lawful pre-trial detention of terrorist suspects.
- Providing professional development for individuals involved in terrorism cases.
- Developing and using forensic evidence to identify those involved in terrorist acts.
- Encouraging international cooperation.

[The QDR] puts forth the notion that the best way to disrupt threats is to prevent them from happening.

Secretary of Defense Chuck Hagel commented on the enormity of international threats in his June 18, 2014, testimony to the Senate Appropriations Committee. Hagel stated, "With this budget, we are repositioning the military for the new strategic challenges and opportunities that will define our future: new technologies, new centers of power, and a world that is growing more volatile, more unpredictable, and in some instances more threatening to the United States."[3] His statement conveys the complexity of threats emanating from the international arena with respect to the mission of the Department of Defense (DoD) to deter those threats in support of U.S. interests both at home and abroad.

In the 2014 Quadrennial Defense Review (QDR), DoD identifies the three strategic pillars of its national security strategy. The first is "defending the homeland."[4] The QDR emphasizes Hagel's concerns about a "rapidly changing security environment."[5] The QDR highlights two areas essential to the interagency counterterrorism effort—intelligence, surveillance, and reconnaissance (ISR) and counter terror and special operations. It also recognizes threats are increasingly enabled by technologies that were once the purview of nation states and identifies the need for the U.S. to adapt more quickly in the face of the ever-growing complexity of threats originating from around the globe. The rapidity of change to global security concerns will be compounded by how threats "intersect and influence one another."[6]

The QDR asserts "the homeland is no longer a sanctuary…and we must anticipate the likelihood of an attack on U.S. soil."[7] It puts forth the notion that the best way to disrupt threats is to prevent them from happening. To do so requires the U.S. interagency to respond proactively with a diversified, collaborative, and networked counterterrorism effort of its own. As the QDR states, DoD will collaborate with its interagency partners to "sustain a global effort to detect, disrupt, and defeat terrorist plots."[8]

Similarly, Federal Bureau of Investigation (FBI) Director James Comey articulated the necessity for partner engagement during his November 14, 2013, testimony to the Senate Committee on Homeland Security and Governmental Affairs. Comey stated, "These diverse threats illustrate the complexity and breadth of the FBI's mission and make clear the importance of its partnerships. We cannot do it alone. To accomplish its mission, the FBI relies heavily upon its partners around the globe." He went on to say that the Bureau

has built partnerships with just about every federal, state, local, tribal, and territorial law enforcement agency in the nation, and its agents and staff work closely with law enforcement, intelligence, and security services in foreign countries, as well as international organizations such as Interpol.[9]

Like Sparta's warriors of old, U.S. military and law enforcement professionals are rugged, highly-trained experts in their fields. They come from all backgrounds and serve the U.S. through their efforts every day. The myriad threats each must be ready to face are diverse and global in scale. It is not unusual for FBI personnel to be deployed into military theaters of operation. It is also not unusual for military and DoD personnel to work with FBI Special Agents in support of mitigating threats across the U.S. There is a complementary synergy among the military, Departments, the FBI, and the rest of the U.S national security establishment. Law enforcement working in collaboration with the military strengthens America's ability to protect its interests both at home and abroad.

The synergy between domestic law enforcement and the military creates opportunities for leveraging each other's capabilities against increasingly complex domestic and international threats. National security strategy should include domestic security considerations along with those in the international arena. The U.S. should enhance interagency efficiencies by implementing reforms that create a holistic national security strategy that addresses the spectrum of threats facing the U.S., both within its borders and at the far reaches of the globe.

Statements by Holder, Hagel, and Comey convey the complexity of the threats to the U.S. and the need for a cohesive interagency coordinating mechanism to address those threats across federal, state, and local jurisdictions. Threats in the international and domestic realms may overlap in a manner requiring proactive interaction among federal, state, and local agencies. Information developed by the DoD on an issue overseas may have implications for a local police department somewhere in the U.S. In this regard, tactical or operational information developed in a foreign land may have consequences of a strategic nature here at home. Given these circumstances, proactive interagency coordination among federal agencies, international partners, and state and local agencies is an imperative for protecting domestic security interests. In doing so, there is also an imperative for ensuring such coordination upholds the liberties of U.S. citizens as guaranteed by the processes articulated in the Constitution.

From the earliest beginnings of the U.S., the issue of providing for its security has been addressed through the lens of civil liberties.

From the earliest beginnings of the U.S., the issue of providing for its security has been addressed through the lens of civil liberties. In *Federalist Paper No. 3*, John Jay wrote, "Among the many objects to which a wise and free people find it necessary to direct their attention, that of providing for their safety seems to be the first."[10] This basic notion of providing security spans today's interagency from the vantage point of both domestic and international security concerns. Whether it is a drug cartel planning a shipment of heroin, a self-radicalized individual intent on doing harm, or a foreign-government-backed entity writing code to hack into the U.S. banking system, the range of threats necessitates cohesive interagency coordination for purposes of identifying and disrupting threats before they can impact the safety and security of U.S. citizens.

As the Founders of the Republic began their discourse on what constitutes security, they debated the need for security relative to safeguarding liberty. In *Federalist Paper No. 51*, James Madison wrote, "In forming a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the place oblige it to curtail itself."[11] Madison understood the need for a government to exert its power in its efforts to defend the security of its citizens. He also realized the potential for those same powers to be abused and as such argued for placing limits on the extent the government could impose itself over its citizens. The issue is just as important today with respect to how to conduct interagency coordination and information sharing without infringing on the rights of the people. In short, the dilemma is how to balance the need for security while simultaneously safeguarding constitutionally guaranteed liberties.

...the dilemma is how to balance the need for security while simultaneously safeguarding constitutionally guaranteed liberties.

Maintaining vigilance is an essential function of the U.S. interagency.[12] From combating gangs and violent criminals through the use of local and regional task forces, to monitoring terrorist organizations and destabilizing international events, a cohesive interagency approach is necessary to identify, evaluate, and mitigate threats. The imperative for doing so should be undertaken with a view toward protecting life, liberty, and the pursuit of happiness. The government's power to protect includes understanding a threat to security is a threat to liberty.

In a letter to James Monroe in July of 1790, Thomas Jefferson wrote, "Whatever enables us to go to war, secures our peace."[13] This statement underscores Jefferson's understanding of national security relative to those liberties ingrained in the Constitution. He understood the preeminence of the federal government to both the protection against physical threats as well as safeguarding liberty. Within the context of U.S. interagency coordination, the issue importantly comes to light with respect to intelligence gathering and information sharing. The better integrated intelligence programs are at all levels of government, the better they can serve the imperative to support and defend. When performed in a manner that complies with legal restrictions necessary to safeguarding liberties, the more they facilitate the interagency mandate to protect against all enemies foreign and domestic.

The relationship of security to liberty is perhaps best explained through the manner in which technology supports both. In the U.S., where individual freedom is considered paramount, the Constitution provides for freedom of speech and the press. Individuals and entities intent on attacking U.S. interests at home and abroad use the same technologies available to law-abiding citizens. The open networks enjoyed by U.S. society at large are vulnerable to exploitation by the nefarious actors intent on causing harm to the U.S. These technical capabilities are being exploited by criminal groups, individual extremists, rogue states, non-state actors, and others in their efforts to damage vital U.S. national security interests. An important interagency consideration is the notion modern technology will serve to simultaneously enhance society, facilitate threats, and impose technological limits on national power. To this end, successful interagency coordination requires mechanisms in place to ensure the proactive exchange of information without infringing on personal

freedoms.

28 Code of Federal Regulations (CFR), part 23, "Criminal Intelligence Systems Operating Policies," ensure criminal intelligence systems are "utilized in conformance with the privacy and constitutional rights of individuals."[14] The CFR provides a template for creating an integrated system that could serve the needs of U.S. interagency counterterrorism efforts at the federal, state, and local levels. 28 CFR, part 23 recognizes criminal activities "often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area."[15] A criminal intelligence system is defined as "the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information."[16] The operating principles for such a system include:

- Reasonable suspicion of criminal activity.
- No inclusion of 1st Amendment information.
- Identification of a criminal predicate.
- Adherence to federal, state, and local laws.
- Dissemination of information based on need to know.
- Adherence to information handling safeguards.
- Does not limit disseminating information when there is danger to life or property.
- Incorporates safeguards and audits to insure against unauthorized use.
- All retained information has relevance and importance.
- Information is not used to interfere with lawful activities.

The Nationwide Suspicious Activity Reporting Initiative (NSI) is a collaborative effort led by the U.S. Department of Homeland Security (DHS) and the FBI.[17] It represents a type of program which, if properly integrated, could serve U.S. interagency counterterrorism efforts across all jurisdictions. The NSI helps "law enforcement and homeland security agencies in preventing terrorism and related criminal activities by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing terrorism related information."[18] Other similar systems include the FBI's e-Guardian[19] and Law Enforcement Online (LEO) [20] programs, which facilitate sharing state and local information with federal agencies. LEO also provides for the exchange of unclassified information from the federal to the state and local levels. A similar initiative by the DHS is the Homeland Security Information Network (HSIN).[21]

The rapid invention and application of new technologies offer a wide range of avenues for both legitimate and criminal enterprise.

The rapid invention and application of new technologies offer a wide range of avenues for both legitimate and criminal enterprise. Free market enterprise and healthy market forces ensure the continued evolution of information technology into smaller and increasingly more powerful devices. The ability to transmit and receive information on a global scale is unprecedented and promises to increase with the development of new, more powerful technologies.

Just as technology enhances society, so to it provides opportunities for nefarious actors both at home and abroad. Information technology

is both a boon and a bane with regard to how the U.S. interagency addresses the challenge of protecting national security interests and civil liberties. In order to be successful, the interagency must go beyond leveraging technology in support of its traditional ways of identifying and responding to the broad range of threats it is responsible for monitoring. It must determine the best manner to remedy the main interagency coordination problem of how to proactively address threats while safeguarding liberties.

Instead of relying on segregated systems based on agency-specific applications, a comprehensive, integrated, and unified system could serve to enhance understanding of the relationships between threats at home and abroad.

The interagency must work to develop a unified system with the potency to identify, evaluate, and mitigate threats. It must do this within the constraints and limitations imposed on it by constitutionally-based legislative restrictions. Establishing a unified interagency network permits law enforcement and defense agencies to maintain autonomy in an integrated manner. This in turn facilitates decision making at all levels while facilitating operational and tactical coordination both at home and abroad. Such integration provides for rapidly identifying, evaluating, and mitigating all manner of threats across the security spectrum. Implementing such a network would serve to enhance interagency responses by facilitating the provision of resources in a timely manner.

A unified interagency technical construct could theoretically enhance joint coordination between law enforcement and defense agencies. It could serve to enhance situational awareness, providing increased fidelity in support of emergency-response operations. Instead of relying on segregated systems based on agency-specific applications, a comprehensive, integrated, and unified system could serve to enhance understanding of the relationships between threats at home and abroad. Through an integrated system, inclusive of federal, state, and local agencies, the interagency could better prepare for and respond to threats more rapidly.

Despite the opportunities such a system presents for identifying, evaluating, and mitigating threats, there remains the need to protect civil liberties. There are vulnerabilities and risks associated with such a system, yet the potential for greater interagency cohesion is an advantage worth advocating for. By enhancing knowledge-based interagency coordination to leverage the instruments of national power, the U.S. stands to better protect its national security interests, while simultaneously protecting civil liberties. A cohesive and coordinated interagency information-sharing network will provide advantages for confronting the wide range of threats both domestically and abroad. The traditional forms of information sharing along agency-specific lines would be enhanced, allowing for greater awareness and more proactive responses to ongoing and emerging threats.

The benefit gained by technically integrating interagency coordination includes enhanced understanding of threats at home and abroad and their relationships. The interagency would benefit through a more thorough understanding of the threats and the ability to more rapidly share actionable intelligence. It would have the means for enhancing intelligence gathering and information sharing in a number of areas.

The pervasive nature of the threats at home and abroad requires the U.S. to have a proactive approach to deterring those threats. Proactive, well coordinated intelligence gathering and

information sharing across multiple jurisdictions will facilitate the ability to mitigate and monitor threats. Combining such a capability with stringent oversight for following applicable laws and statutory guidelines to protect civil liberties will ensure compliance with constitutionally-mandated processes.

Leveraging the capabilities of federal, state, and local agencies into a combined platform to enhance situational awareness supports threat mitigation efforts. Policy at the federal level should strive to integrate state and local capabilities, where applicable, in support of thwarting domestic threats. Often state and local agencies have a better understanding of threats their federal partners may not be attuned to. As such, incorporating state and local agencies into such a system should become a priority for the interagency.

By implementing a cohesive, interagency-coordinating system that includes federal, state, and local agencies, the U.S. stands to benefit in the following areas:

- Proactively allocating resources to intelligence gathering and information sharing.
- Gaining synergies through integrating agencies across multiple jurisdictions.
- Rapidly identifying, evaluating, and mitigating threats.
- Facilitating decision making.
- Integrating strategic, operational, and tactical considerations.
- Ensuring the protection of constitutionally guaranteed liberties.

Using federal resources to identify potential threats and providing information to state and local law enforcement promises to produce long-term dividends, especially if the information facilitates engagement with local communities. Through state and local outreach efforts, federal information can be used to solicit information about potential threats. By doing so, local law enforcement can integrate even the most remote community into the hunt for potential threats. Such an effort would give federal, state, and local law enforcement an advantage with respect to the amount of lawful opportunities they would have to detect and prevent a terrorist attack. The interagency would in turn benefit by taking advantage of the community engagement resources of state and local law enforcement.

Integrating a cohesive interagency counterterrorism capability across all jurisdictions will enhance the effectiveness of coordination and promote the ability to detect and disrupt threats, which would have been very useful in the prelude to the September 11 and Boston Marathon attacks. Failing to proactively share information may result in terrorist events taking place that otherwise may have been prevented.

By enhancing the manner in which interagency coordination is conducted in relation to intelligence gathering and information sharing, the U.S. will be better positioned to address long-term threats both at home and abroad. Such an effort would benefit the interagency through more focused decision making with respect to how to resource efforts against specific threats. Creating a cohesive interagency coordination system that protects civil liberties will contribute to operational and tactical effectiveness in interagency efforts against a wide spectrum of threats impacting the U.S., both at home and abroad. ***IAJ***

NOTES

1 Attorney General Eric Holder, "Remarks Urging International Effort to Confront Threat of Syrian Foreign Fighters," speech, Department of Justice, July 8, 2014, <http://www.justice .gov/iso/opa/ag/speeches/2014/ag-speech-140708.html>, accessed on July 16, 2014.

2 Global Counterterrorism Forum, Criminal Justice Sector/Rule of Law Working Group, "The Rabat Memorandum on Good Practices for Effective Counterterrorism Practice in the Criminal Justice Sector," May 24, 2012, <http://www.thegctf.org/documents/10162 /19594 /Rabat +Memorandum+on+Good+Practices+for+Effective+Counterterrorism+Practice+in+the+Criminal+Justice+Sector>, accessed on July 10, 2014.

3 Secretary of Defense Chuck Hagel, statement to the Senate Appropriations Committee-Defense (Budget Request), June 18, 2014, <http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1861>, accessed on July 14, 2014.

4 Department of Defense, "Quadrennial Defense Review 2014." DOD prioritizes three strategic pillars: protect the homeland, deter and defeat attacks on the U.S., and support civil authorities in mitigating the effects of potential attacks and natural disasters.

5 Ibid.

6 Ibid.

7 Ibid. DoD's strategy includes a "layered" approach to defending the homeland amidst a "varied, multifaceted, and growing set of threats." The strategy includes support to civil authorities when required and explicitly states, "U.S. forces will abide by applicable laws, policies, and regulations that protect the privacy and civil liberties of U.S. persons."

8 Ibid.

9 FBI Director James Comey, statement before the Senate Committee on Homeland Security and Governmental Affairs, November 14, 2013, <http://www.fbi.gov/news/testimony/homeland-threats-and-the-fbis-response>, accessed on July 14, 2014.

10 John Jay, "Concerning Dangers from Foreign Force and Influence," *Federalist Paper No. 3*.

11 James Madison, "The Structure of the Government Must Furnish the Proper Checks and Balances between the Different Departments," *Federalist Paper No. 51*.

12 Jessica Zuckerman; Steven P. Bucci, PhD; and James Jay Carafano, PhD, "60 Terrorist Plots Since 9/11: Continued Lessons in Domestic Counterterrorism," Heritage Foundation, "Special Report #137 on Terrorism," <http://www.heritage.org/research/reports/2013/07/60-terrorist-plots-since-911-continued-lessons-in-domestic-counterterrorism>, accessed on July 18, 2014.

13 Thomas Jefferson, "Letter to James Monroe," July 11, 1790, in Paul Leicester Ford (ed.), *The Works of Thomas Jefferson in Twelve Volumes*, Federal Edition, <http://memory.loc.gov/cgi-bin/query/r?ammem/mtj:@field(DOCID+@lit(tj060047))>, accessed on July 10, 2014.

14 Code of Federal Regulation 28, part 23, "Criminal Intelligence Systems Operating Policies."

15 Ibid.

16 Ibid.

17 Nationwide Suspicious Activity Report (SAR) Initiative (NSI), NSI homepage, <http://nsi.ncirc.gov>,

accessed on July 22, 2014.

18 Ibid.

19 Federal Bureau of Investigation, "Privacy Impact Assessment for the eGuardian System," <http://www.fbi.gov/foia/privacy-impact-assessments/eguardian-threat>, accessed on July 22, 2014.

20 Federal Bureau of Investigation, "Law Enforcement Online (LEO)," <http://www.fbi.gov/about-us/cjis/leo>, accessed on July 22, 2014.

21 Department of Homeland Security, "Homeland Security Information Network," <http://www.fbi.gov/about-us/cjis/leo>, accessed on July 22, 2014.