Evaluating and Teaching Homeland Security Intelligence[1]

James Steiner, Ph.D.

This paper is posted on the AFIO website (www.afio.com) in the Intelligence Study Guide.

When he was Undersecretay for Intelligence at the Department of Homeland Security (DHS), Charlie Allen was fond of saying that virtually all homeland security programs that address threats require intelligence support to be successful. The local firefighter, police officer, and emergency room medical personnel in Boston are just as legitimate intelligence customers as those working overseas for the Federal Bureau of Investigation (FBI), military, and State Department. Unfortunately, even fourteen years after 9/11 these newer, non-traditional customers remain underserved, especially compared to long-term national security intelligence customers.

This deficiency is a major reason why intelligence is a priority area for Homeland Security education and training. The potential student population is massive, including not only undergraduate and graduate students and intelligence professionals but the over 10-million homeland security practitioners, many of whom are still learning what intelligence is and how to use it. Given the size and diversity of this customer set, intelligence education and training is most effective when structured on a customer and mission basis. This helps each student see the potential of intelligence to help them accomplish their specific mission.

Evaluating Homeland Security Intelligence

Intelligence support to federal counterterrorism customers since 9/11 has enabled military, diplomatic, covert action, and law enforcement officers to be successful. The fundamental reason for this strong record is that federal departments and agencies with the lead roles in counterterrorism have decades of experience producing and using intelligence. These customers control their own (relatively) well-funded, well-trained departmental intelligence organizations; have direct input into prioritizing intelligence collection through the Intelligence Community (IC); and are themselves knowledgeable customers who trust and act on the intelligence provided them. As written in texts from the time of Sun Tzu,[2] war fighters, diplomats, and covert action officers all need to acquire and use specific, tailored intelligence to achieve victory consistently.

This criticality of intelligence also applies to success in domestic law enforcement operations. Even before 9/11, the FBI, Drug Enforcement Administration, Immigration and Customs Enforcement, and other federal law enforcement elements had extensive experience in intelligence-driven operations ranging from FBI counterintelligence programs to the takedown of mafia leaders and drug-trafficking organizations. State and local law enforcement are supported with national-level intelligence through the FBI-sponsored Joint Terrorism Task Force (JTTF) system[3] and the Department of Homeland Security (DHS)–sponsored (but

[1] Much of this paper is drawn from the author's textbook., *Homeland Security Intelligence* (Thousand Oaks, CA: CQ Press/SAGE, 2015).

[2] See Sun Tzu, *The Art of War* (New York: Penguin Books, 2002), 95; and Erik J. Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013),184. This is the primary thesis of Dahl's book.

locally owned) fusion centers.[4] These police forces are valued by the FBI as massive and reliable intelligence collectors and, in the case of imminent threats, operational partners.

A handful of state and local law enforcement agencies (with the New York Police Department at the pinnacle) have substantial independent counter-terrorism intelligence and operational capabilities because they face the greatest domestic threat. All state and local law enforcement have benefited from a trend toward intelligence-led policing, begun in the United Kingdom but was well established and growing in the United States long before 9/11.[5]

The US's homeland security enterprise can be proud of the fact that, with the exception of the attacks at Fort Hood and in Boston, there has not been a successful major terrorist attack within the United States since 9/11 although there have been a total of 65 terrorist plots uncovered to date.[6] But this success also means that first responders (and associated government and private-sector executives) have rarely been tested by major terrorist attacks, and it is not clear whether they receive sufficient intelligence support to be prepared if and when such attacks might occur. First responders have been very effective to date, but with only two terrorist successes, we should not reduce our focus on providing first responders with more and better intelligence support.

First responders deal with emergencies every day but almost never come up against a terrorist situation. On the other hand, the consequences of many terrorist attacks are similar to the consequences of criminal activity, and the procedures and capabilities for response are quite similar. For example, the protocols for responding to an active shooter are the same no matter who is shooting—whether a Major Hasan at Fort Hood or a James Holmes at the Century 16 movie theater in Aurora, Colorado. But first responders need intelligence both for situational awareness in the event of an actual attack and for ensuring realism in planning, training, and exercises. This is especially true in training for situations where first responders could become targets.

The use of the terrorism-related planning scenarios derived from the *Strategic National Risk Assessment*[7] provides the intelligence input needed to make training and exercises realistic and to ensure development of response capabilities. But it is not clear that the first responder community is receiving sufficient intelligence support for situational awareness. Most first responders, especially volunteer firefighters, emergency medical personnel, public works departments, and hospital emergency rooms, do not receive intelligence reports on a regular basis. First response is led at the local level, and determining how much time and treasure to spend on preparing to respond to a terrorist incident remains a local decision. Threat intelligence should be provided to state and local government executives—and even

[3] Federal Bureau of Investigation, "Protecting America from Terrorist Attack: Our Joint Terrorism Task Forces," http://www.fbi.gov/about-us/investigate/terrorism/ terrorism_jttfs.

[4] See *2011 National Network of Fusion Centers: Final Report*, May 2012, https://www.dhs.gov/sites/default/files/publications/2011-national-network- fusion-centers-final-report.pdf.

[5] See Marilyn Peterson, *Intelligence-Led Policing: The New Intelligence Architecture* (Washington, DC: U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, September 2005), https://www.ncjrs.gov/pdffiles1/bja/210681.pdf.

[6] April 2015. See http://www.heritage.org/research/reports/2015/04/65th-islamist-terrorist-plot-or-attack-since-911-persistent-terrorism-requires-constant-vigilance.

[7] U.S. Department of Homeland Security, *The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach Toward a Secure and Resilient Nation*, December 2011, http://www.dhs.gov/xlibrary/assets/rma-strategic-national- risk-assessment-ppd8.pdf.

the private sector—so they can make difficult risk-management and resource-allocation decisions.

With the exception of law enforcement and the National Guard, first responders do not own their primary intelligence providers, have no direct impact on national-level intelligence collection, and have only recently begun gaining experience using intelligence—arguably three of the most important characteristics of successful intelligence support to the federal and law enforcement customers.

The DHS Undersecretary for Intelligence has the fundamental responsibility for providing intelligence support to first responders and the governors, mayors, and other elected officials that direct them. There is a clear conduit for producing and providing situational awareness intelligence to these customer sets. The material is produced by the IC (primarily at the National Counterterrorism Center and its Interagency Threat Assessment and Coordination Group, FBI, and DHS), sent to the state or local fusion centers, and then disseminated to state and local government leaders and first responders. Arguably, fusion center analysts are ideally placed to discern what state and local intelligence customers need to know from these national-level intelligence products. They can provide unique added value by tailoring the federal intelligence to their own customer set. For example, at every fusion center, intelligence analysts should routinely add to all federally produced intelligence products a section called "Implications for My City/State," before disseminating them to leaders and first responders.

Today, intelligence support to the owners and operators of the US's critical infrastructure is mixed. DHS has compiled and monitors a list of the roughly two thousand of the most important physical facilities of our critical infrastructure. Because of their size and importance to the economy, these priority facilities receive special attention and support from DHS and their Sector Specific Agencies (SSAs),[8] including the granting to selected personnel of security clearances and access to the actual operational and tactical threat intelligence. Not surprisingly, the highest caliber of support goes to those facilities that have an SSA that is also associated with the IC. The defense industry is supported by the Defense Intelligence Agency and port security personnel receive intelligence support from their SSA, the U.S. Coast Guard.

But it is a mixed bag in other areas. For example, in the commercial facilities sector, large firms such as Wal-Mart have their own corporate intelligence/security programs and work closely with DHS. But what about owners and operators of independent stores and small shopping malls? Recent graduate research concludes that most facilities in the retail sector and other critical infrastructure sectors receive no intelligence on terrorist threats.

In some cases, fusion centers and state and local governments attempt to fill the gaps in providing intelligence (information) support to private facilities, and often provide sanitized versions of operational and tactical threat "information" (rather than classified intelligence) to facility owners and managers. But the effort at the state and local level is mixed, at best. At the federal level, intelligence organizations *push* the intelligence product to the customer; but also knowledgeable customers *pull* intelligence from producers by demanding sophisticated support. This is rarely the case in the private sector or even at the state and local level. Islands of excellent intelligence support can be found in areas that face high threats, but

[8] U.S. Department of Homeland Security, "Critical Infrastructure Sector Partnerships," http://www.dhs.gov/critical-infrastructure-sector-partnerships.

these are the exceptions. The homeland security intelligence enterprise must provide better intelligence to the private sector to improve critical infrastructure protection and especially with cybersecurity.

The Homeland Security Intelligence Education Mandate

The demand for homeland security intelligence comes from both intelligence producers and homeland security customers. A recent mixed methods research paper on designing a graduate curriculum for Homeland Security ranked "intelligence" as the third most important area of emphasis (out of 11 required areas)[9]. Many of the 355 academic institutions[10] that offer degrees and/or certificates in homeland security already include one or more courses in intelligence.

Not surprisingly, most of these courses are traditional surveys and focus on the internals of the intelligence production process: the intelligence cycle and the members of the US intelligence community (IC). Most textbooks for overview courses on intelligence are structured in a similar fashion. A recommended go-to book for teaching courses on the internals of intelligence is Mark Lowenthal's *Intelligence: From Secrets to Policy,*[11] which follows this structure and works well for teaching traditional courses.

But there is a different paradigm – one structured around the intelligence customer and his/her mission rather than on the intelligence production process – that can help current or potential homeland security practitioners. Taking an example from another field, if we were teaching MBA students about the automotive sector, the industrial process focus (analogous to the intelligence production cycle) would work well. We would study the research, development, production, marketing, and sales of vehicles, and examine the materials, labor, engineering, styling, manufacturing, and sales distribution network of the auto industry. Such a course would be of great interest to those who want a career working in the automotive industry —but it would be less useful to those whose primary responsibility is to actually purchase cars and trucks for their company.

Alternatively, these students are better served by a course that focuses on motor vehicles as products. One could begin by identifying and categorizing the different customer sets and their distinct transportation needs, such as retail delivery, long-haul commercial transport, commuting, and recreation. After analyzing such needs of specific customer sets, this study would focus on the most appropriate product lines for each customer, such as trucks versus SUVs versus automobiles, not to mention product subsets such as subcompact, compact, full size, and luxury. This course would be useful to customers of, as well as marketers in, the automotive industry.

Homeland security intelligence courses structured in an analogous fashion put the focus on the customer and his/her mission—the homeland security practitioner who receives and uses the intelligence product to achieve a specific goal.

[9] John M. Persyn and Cheryl J. Polson "Understanding Homeland Security Education Graduate Program Core Content Priorities: A Mixed Methods Research-based Approach," 8th Annual Homeland Defense and Security Education Summit, Colorado Springs, CO., October 9-10, 2014.

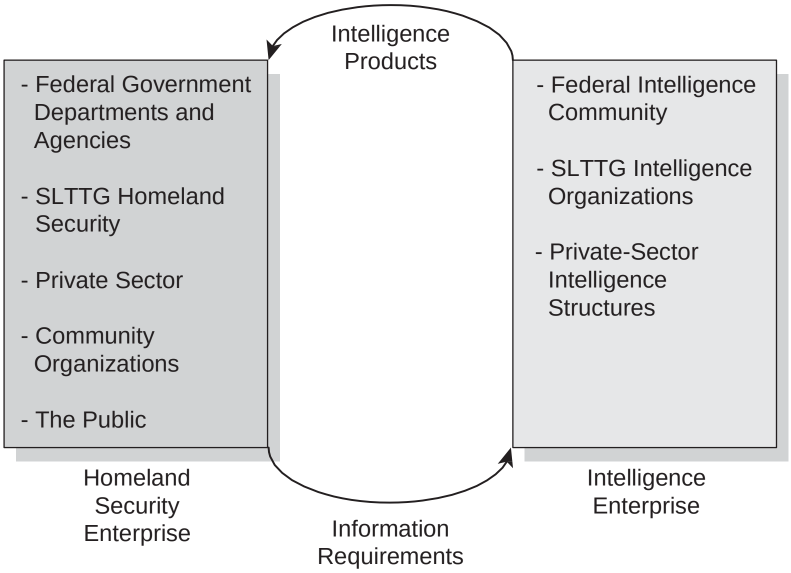
[10] Based on the number of academic and research institutions in the University and Agency Partnership Initiative, Center for Homeland Defense and Security, Naval Postgraduate School, Monterey, CA. https://www.chds.us/?special/info&pgm=Partner

[11] See Mark Lowenthal, *Intelligence: From Secrets to Policy,* 6th ed. (Thousand Oaks, CA: CQ Press/SAGE, 2014).

A Homeland Security Intelligence Course Approach[12]

To set the stage, a homeland security intelligence course normally would begin with an overview of the broad range of players in the homeland security and intelligence enterprises.[13]

Figure 1 Homeland Security Enterprise: Information Requirements


Intelligence Products
- Federal Government Departments and Agencies
- SLTTG Homeland Security
- Private Sector
- Community Organizations
- The Public
Homeland Security Enterprise
- Federal Intelligence Community
- SLTTG Intelligence Organizations
- Private-Sector Intelligence Structures
Intelligence Enterprise
Information Requirements

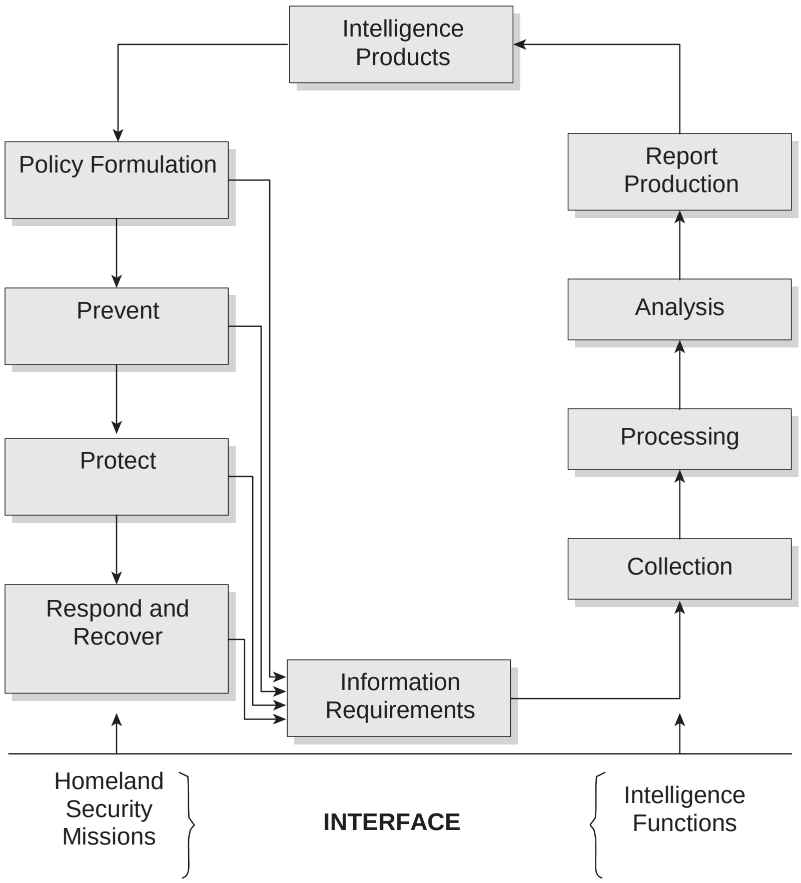
Next, after describing the intelligence cycle, the traditional "customer" box is expanded to show the full range of homeland security missions or functions as shown below.[14]

[12] This section and the course structure follow the structure of my textbook. See Steiner (2015).

[13] Steiner 2015, 3. SLTTG is State, Local, Tribal, and Territorial Governments.

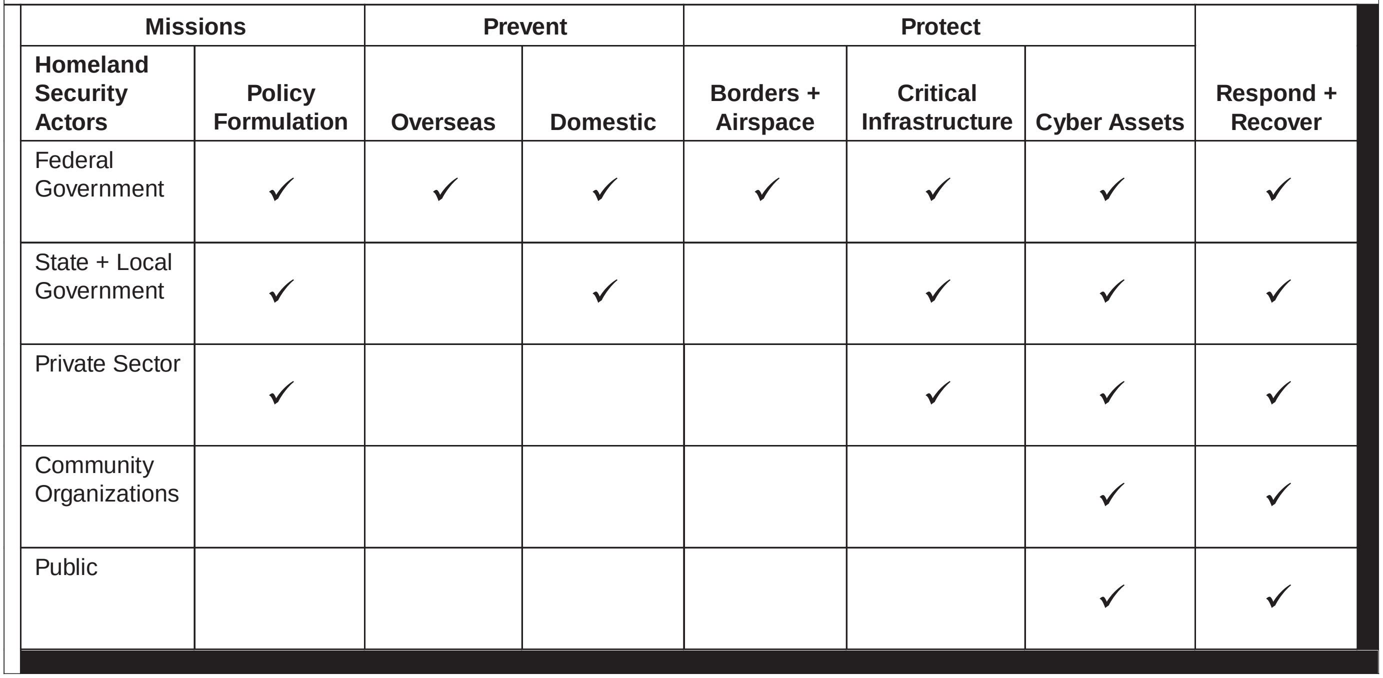
[14] Steiner 2015, 10.

Figure 2 Intelligence Support to Homeland Security: Missions



Once this foundation is in place, the course could delve into each specific homeland security mission, identifying and discussing the major actors, and looking at how intelligence supports them. Individual lectures should cover the range of programs. Two lectures might be required for the "prevent" mission—one for intelligence support to counterterrorism programs overseas and one focused on support to domestic efforts. Three lectures could address intelligence support to our diverse "protect" programs—first, programs protecting US borders and airspace; second, activities protecting critical infrastructure and key resources; and, finally, a whole-of-the-nation effort to protect the cyber infrastructure and information. On the other hand, intelligence support to our "respond" and "recover" missions could be covered in one lecture, with the bulk of the discussion devoted to emergency response, treating the recovery efforts as the final step in response.[15]

Figure 3 Securing the Homeland: Major Roles and Responsibilities



Missions		Prevent		Protect			
Homeland Security Actors	Policy Formulation	Overseas	Domestic	Borders + Airspace	Critical Infrastructure	Cyber Assets	Respond + Recover
Federal Government	✓	✓	✓	✓	✓	✓	✓
State + Local Government	✓		✓		✓	✓	✓
Private Sector	✓				✓	✓	✓
Community Organizations						✓	✓
Public						✓	✓

Using this paradigm, most professionals can identify their specific jobs as included in at least one of these missions, but only a handful will be familiar with the intelligence dimension of other homeland security missions. Unclassified and/or declassified intelligence products can help students look at the full range of intelligence needed and used by the entire homeland security enterprise.

For example, in dealing with our overseas "prevent" programs, three declassified intelligence reports can be parsed by the students. The first, a CIA intelligence report[16] assesses the threat posed by terrorist/insurgent groups in Peru in the early 1990s and can be used strategically to help decide if the United States should take action to disrupt, dismantle, and/or destroy the threat; whether such action should use diplomacy, covert action, or military force; and whether the US should act unilaterally or with the Peruvian government. Next, going down the military track, the Army intelligence handbook on Peru[17] can be used by defense and military planners to construct an operational plan. Finally, a tactical intelligence product[18] from the 470th Military Intelligence Brigade can be used that reports on a sighting of a band of insurgents, with specifics on how many and where, and which direction they were heading. This is the near–real-time intelligence that our troops on the ground need to attack the enemy.

When addressing a domestic emergency the response to the Boston Marathon bombing in 2013 is a useful example. In this example, students can see how specialized training and

[16] Directorate of Intelligence, Central Intelligence Agency, *Tupac Amaru Revolutionary Movement: Growing Threat to US Interests in Peru*, March 28, 1991, http://www.foia.cia.gov/sites/default/files/document_conversions/89801/DOC_0000393913.pdf.

[17] *Army Country Profil: Peru* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB64/peru32.pdf.

[18] The full (declassified) tactical report, produced by the U.S. Army's 470th Military Intelligence Brigade, is available at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB64/peru31.pdf .

exercises for first responders and hospital emergency room personnel familiarized them with an attack involving an improvised explosive device (IED). Their preparedness actions included creating the procedures and acquiring the capabilities that enabled them to deal effectively with the aftermath of the attack. That specialized training and those exercises, of course, were designed using extensive intelligence on terrorist tactics, practices, and procedures involving IEDs around the world, and, in fact, the attack itself was very similar to one of the intelligence-intensive national planning scenarios (#12)[19] developed as part of the preparedness cycle. Other lectures could provide more examples of strategic, operational, and tactical intelligence and how they are used.

By the end of such a course, students should have a strong appreciation for the categories of intelligence needed by the broad range of homeland security practitioners. Hopefully, they would be better prepared not only to receive intelligence products, but also to demand intelligence support tailored to their needs. In fact, perhaps the single most important theme in this education/training is that intelligence must be tailored to the needs of each specific client in the diverse homeland security customer set. Implicit in this theme is the assertion that in meeting this imperative, the intelligence product will be significantly different depending on the mission of the customer.

For example, consider the characteristics of the intelligence product produced for the Governor of New York to help him and his staff in the risk analysis and management process leading to appropriate funding levels in the New York State budget for cybersecurity as opposed to funding for counterterrorism. Now think about the intelligence product required by the federal immigration officer at a port of entry trying to spot an Al Qaida operative attempting to enter the US. Clearly, these two customers (one strategic, one tactical), whose positions require them to address very different dimensions of homeland security (resource allocation, border protection), demand and deserve very different intelligence products.

Readings for Instructors

There are only a few texts, listed below, that address the relationship between homeland security and intelligence. Most homeland security texts fail to address the intelligence relationship and many intelligence texts do not address specifically the homeland security mission.

Hulnick, Arthur S. *Keeping Us Safe: Secret Intelligence and Homeland Security*. Westport Connecticut: Praeger, 2004. Boston University professor and former CIA officer Hulnick was the first to take a targeted look at intelligence and homeland security. Eleven of his 12 chapters are on intelligence support to the *preventers*. His text is now dated and there have been significant organizational changes since. There is very little discussion of the role of state and local elements of the homeland security establishment, much less their intelligence requirements.

Logan, Keith (Editor). *Homeland Security and Intelligence.* Santa Barbara, California: Praeger, 2010. This book of readings has some chapters which are quite good but others poorly conceptualized and written. It has little to offer on the role of state and local government as intelligence producers and consumers.

[19] U.S. Department of Homeland Security, *National Planning Scenarios*, March 2006, https://publicintelligence.net/national-planning-scenarios-version-21-3-2006-final-draft/ , 12-1.

O'Sullivan, Terry M. (Editor). *Department of Homeland Security Intelligence Enterprise: Overview and Issues*. Hauppauge, NY: Nova Publisher, 2011. This book uses publically available US government documents. The first two chapters come from a GAO study "The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress." The remainder of the book contains transcripts from congressional hearings. The sole focus is on intelligence produced and consumed by the Department of Homeland Security.

Steiner, James. *Homeland Security Intelligence*. Thousand Oaks, CA: CQ Press/SAGE, 2015. Much of this article is derived from this text.

Taylor, Robert and Charles Swanson. *Terrorism, Intelligence, and Homeland Security*. New York: Prentice Hall, 2015. Although this book has "intelligence" in the title, it is a criminal justice textbook and is limited to the law enforcement customer.

Author

James Steiner is Public Service Professor (Intelligence Studies) and Program Coordinator, Homeland Security, Cyber Security, and Emergency Management at Rockefeller College, SUNY Albany. He is a retired senior CIA officer and has taught intelligence analysis at the FBI Academy. He has served as a senior consultant to both the Undersecretary for Intelligence at DHS and the New York State Homeland Security Advisor.