

# The U.S. Intelligence Community: Homeland Security Issues in the 116<sup>th</sup> Congress

Updated February 1, 2019 (IN11031)

---

## Related Author

---

- [Michael E. DeVine](#)
- 

Michael E. DeVine, Analyst in Intelligence and National Security ([medevine@crs.loc.gov](mailto:medevine@crs.loc.gov), 7-1126)

---

Intelligence support of homeland security is a primary mission of the entire Intelligence Community (IC). In fulfilling this mission, changes to IC organization and process, since 9/11, have enabled more integrated and effective support than witnessed or envisioned since its inception. The terrorist attacks of 9/11 revealed how barriers between intelligence and law enforcement, which originally had been created to protect civil liberties, had become too rigid, thus preventing efficient, effective coordination against threats. In its final [report](#), the Commission on Terrorist Attacks upon the United States (the *9/11 Commission*) identified how these barriers contributed to degrading U.S. national security. The findings resulted in Congress and the executive branch enacting legislation and providing policies and regulations designed to enhance information sharing across the U.S. government.

The Homeland Security Act of 2002 ([P.L. 107-296](#)) gave the Department of Homeland Security (DHS) responsibility for integrating law enforcement and intelligence information relating to terrorist threats to the homeland. Provisions in the Intelligence Reform and Terrorist Prevention Act (IRTPA) of 2004 ([P.L. 108-458](#)) established the National Counterterrorism Center ([NCTC](#)) as the coordinator at the federal level for terrorism information and assessment and created the position of Director of National Intelligence (DNI) to provide strategic management across the 17 organizational elements of the IC. New legal authorities accompanied these organizational changes. At the federal, state, and local levels, initiatives to improve collaboration across the federal government include the FBI-led Joint Terrorism Task Forces (JTTFs) and, more recently, the DHS National Network of Fusion Centers (NNFC).

Within the IC, the FBI Intelligence Branch ([FBI/IB](#)), and DHS's Office of Intelligence and Analysis ([OIA](#)), and the Coast Guard Intelligence ([CG-2](#)) enterprise, are most closely associated with homeland security. OIA combines information collected by DHS components as part of their operational activities (i.e., those conducted at airports, seaports, and the border) with foreign intelligence from the IC; law enforcement information from federal, state, local, territorial and tribal sources; and private sector data about critical infrastructure and strategic resources. OIA analytical products focus on a wide range of threats to the homeland to include foreign and domestic terrorism, border security, human trafficking, and public health. OIA's customers range from the U.S. President to border patrol agents, Coast Guard personnel, airport screeners, and local first responders. Much of the information sharing is done through the NNFC—with OIA providing personnel, systems, and training.

The Coast Guard Intelligence (CG-2) enterprise is the intelligence component of the United States Coast Guard (USCG). It serves as the primary USCG interface with the IC on intelligence policy, planning, budgeting and oversight matters related to maritime security and border protection. CG-2 has a component Counterintelligence Service, a Cryptologic Group, and an Intelligence Coordination Center to provide analysis and supporting products on maritime border security. CG-2 also receives support from field operational intelligence components including the Atlantic and Pacific Area Intelligence Divisions, Maritime Intelligence Fusion Centers for the Atlantic and Pacific, and intelligence staffs supporting Coast Guard districts and sectors.

FBI/IB includes four component organizations:

- The Directorate of Intelligence has responsibility for all FBI intelligence functions, and includes intelligence elements and personnel at FBI Headquarters in field divisions.
- The Office of Partner Engagement develops and maintains intelligence sharing relationships across the IC, and with state, local, tribal, territorial, and international partners.
- The Office of Private Sector conducts outreach to businesses impacted by threats to vulnerable sectors of the economy such as critical infrastructure, the supply chain, and financial institutions.
- Finally, the Bureau Intelligence Council provides internal to the FBI a forum for senior-level dialogue on integrated assessments of domestic threats.

While the intelligence organizations of FBI and DHS are the only IC elements solely dedicated to intelligence support of homeland security, all IC elements, to varying degrees, have some level of responsibility for the overarching mission of homeland security. For example, in addition to NCTC, the Office of the DNI (ODNI) includes the Cyber Threat Intelligence Integration Center ([CTIIC](#)). It was established in 2015 and is responsible at the federal level for providing *all-source analysis* of intelligence relating to cyber threats to the United States. Much like NCTC for terrorism, CTIIC provides outreach to other intelligence organizations across the federal government and at the state, and local levels to facilitate intelligence sharing and provide an integrated effort for assessing and providing warning of cyber threats to the homeland.

IC organizational developments since 9/11 underscore the importance of adhering to privacy and civil liberties protections that many feared might be compromised by the more integrated approach to intelligence and law enforcement. This is particularly true considering the changing nature of the threat: The focus of intelligence support of homeland security has evolved from state-centric to increasingly focusing on non-state actors, often individuals acting alone or as part of a group not associated with any state. Collecting against these threats, therefore, requires strict adherence to intelligence oversight rules and regulations, and annual training by the IC workforce for the protection of [privacy and civil liberties](#).