Congressional Research Service
Informing the legislative debate since 1914

Intelligence Authorization Legislation for FY2014 and FY2015: Provisions, Status, Intelligence Community Framework

Anne Daugherty Miles
Analyst in Intelligence and National Security Policy

January 14, 2015

Congressional Research Service
7-5700
www.crs.gov
R43793

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Two Intelligence Authorization Acts (IAAs) were passed in 2014. The IAA for Fiscal Year (FY) 2014 (P.L. 113-126) was passed in July and an IAA for FY2015 (P.L. 113-293) was passed in December. This report examines selected provisions in the legislation and provides an intelligence community framework in the **Appendix**.

Summary of Selected Legislative Provisions		
Title	**IAA FY2014 (P.L. 113-126)**	**IAA FY2015 (P.L. 113-293)**
I. Intelligence Activities	Section104 supports the Intelligence Advanced Research Projects Activity.	
III. General Matters	Section 305 codifies provisions already in E.O. 12333 and gives responsibility for designating functional managers (the directors of CIA, NGA, NSA, and DIA) to the President. Section 309 directs the heads of the DNI, CIA, DIA, NSA, NRO, and NGA to undergo full financial audits beginning with FY2014 financial statements. Section 314 directs the DNI to merge the Foreign Counterintelligence Program into the General Defense Intelligence Program. Section 321 requires that the Attorney General provide the congressional intelligence committees a listing of every opinion of the Office of Legal Counsel that has been provided to an element of the IC, whether classified or unclassified.	Section 303 requires a National Intelligence Strategy. Section 309 concerns retention of data on U.S. persons acquired incidentally to an investigation of foreign persons. Section 310 permits individuals to appeal an adverse security clearance action that may be a reprisal for a protected whistleblower disclosure. Section 324 requires a report on DHS's Homeland Security Intelligence Program and National Intelligence Program. Section 327 directs the DNI to provide information about the number of contractors and their functions for each element of the IC as part of the annual authorization process. Section 330 requires a counterterrorism strategy to disrupt, dismantle, and defeat al-Qaeda and its affiliated or associated groups. Several sections concern intelligence-related relationships with Ukraine, the Russian Federation, and North Korea.
IV. Matters Relating to Elements of the Intelligence Community	Four key individuals, the Directors of NSA and NRO and the Inspectors General of each agency, now require presidential appointments.	
V. Security Clearance Reform	Section 501 requires continuous monitoring in association with access to classified information. Section 504 requires the DNI to report to Congress each year, through 2017, on the reciprocal treatment of security clearances.	
VI. Intelligence Community Whistleblower Protections	Section 601 creates a new Section 2303A of Title 5 of the United States Code, modeled on protections for FBI employees.	
Committee Report Language	Contractor Responsibility Watch List	FIX-ITT (Financial Exchange and Intelligence Integration)

Contents

Figures

Tables

Appendixes

Contacts

Introduction

Permanent, continuing, day-to-day oversight of the U.S. intelligence community (IC) by the two congressional intelligence committees will soon mark its 40th anniversary.[1] The IC's missions, responsibilities, capabilities, size, and management have experienced dramatic changes over the past four decades.[2] The congressional oversight committees have played a significant role in shaping these changes and continue to do so, particularly through their annual intelligence authorization bills.

In recent years the IC has initiated a transformation from the agency-centric practices of the past to an "intelligence enterprise"[3] established on a collaborative foundation of shared services, mission-centric operations, and integrated mission management to confront its ever growing list of challenges. The recently released *National Intelligence Strategy 2014* lays out the strategic environment and identifies the scale of what James Clapper, the Director of National Intelligence (DNI), terms the "pervasive and emerging threats":

> While key nation states such as China, Russia, North Korea and Iran will continue to challenge U.S. interests, global power is also becoming more diffuse. New alignments and informal networks, outside of traditional power blocs and national governments, will increasingly have significant impact in global affairs. Competition for scarce resources such as food, water and energy is growing in importance as an intelligence issue as that competition exacerbates instability, and the constant advancements and globalization of technology will bring both benefits and challenges.[4]

The challenge for this and future Congresses is to help shape intelligence priorities while a more integrated IC adjusts to new budget realities. Congress has an important role in the oversight of the agencies responsible for dealing with this altered intelligence environment, and the annual authorization process represents one of the most important opportunities to exercise this role. Intelligence authorization legislation does not guarantee effective interagency intelligence efforts, but proponents of the oversight process maintain that authorization acts are the best lever that Congress has to address the interagency effort.

Background

The "congressional intelligence committees," as defined in 50 U.S.C. §401a (6), consist of the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI). The intelligence committees were created in the 1970s to conduct

[1] The Senate and House intelligence committees were established in 1976 and 1977, respectively.

[2] The Intelligence Community is a federation of 17 separate executive branch agencies that work separately and together to conduct the activities necessary to produce the intelligence required for the conduct of foreign relations and the protection of the national security of the United States. For a list of the components, see the **Appendix**.

[3] A term in vogue since 2010—associated with, and frequently used by, DNI James Clapper in reference to the IC. See Tom Shorrock, "Clapper: Managing the Intelligence Enterprise," *Foreign Policy In Focus*, (June 18, 2010), at http://fpif.org/clapper_managing_the_intelligence_enterprise/. See also Office of the Director of National Intelligence, *National Intelligence Strategy 2014*, p. 16, at http://www.dni.gov/files/documents/2014_NIS_Publication.pdf.

[4] Office of the Director of National Intelligence, "DNI Unveils 2014 National Intelligence Strategy," *ODNI News Release* No. 40-14, September 18, 2014, at http://www.dni.gov/files/documents/2014_NIS_Publication.pdf.

continuous and "vigilant legislative oversight" over the IC to assure (1) "that the appropriate departments and agencies of the United States provide informed and timely intelligence necessary for the executive and legislative branches to make sound decisions affecting the security and vital interests of the Nation," and (2) "that such activities are in conformity with the Constitution and laws of the United States."[5] They operate behind closed doors, for the most part, overseeing the most secret aspects of the U.S. government. The two intelligence committees are the repositories of most intelligence shared with Congress. Their secure office and hearing room spaces are guarded around the clock by Capitol Hill police.[6]

One of the few windows into the activities of the two intelligence committees is their authorization legislation and accompanying committee reports.[7] They produce (but do not always pass) annual legislation that guides the activities of all 17 U.S. intelligence components—providing authorization for critical national security functions. All authorization bills are important resource documents in terms of both money and manpower, and the intelligence bills are particularly important in this regard. (See the **Appendix** for an IC framework that includes a list of IC components.)

Separate and distinct from one another, the authorization and appropriations processes determine budget authority for agencies and programs. The authorization committees establish the necessity, legitimacy, and intent of agencies and programs. In doing so, authorization is an oversight function, communicating general guidance, leadership, and priorities and providing legislation and direction to agencies.

Appropriations committees determine funding levels for policies and programs previously authorized. For the most part, the appropriations process provides specific details within the general guidance and limitations given by authorizations. Cutting funds, adding funds, or attaching provisions to funding are powerful ways to influence policy decisions. The funding associated with intelligence is significant. For FY2014 alone, the aggregate amount (base and supplemental) appropriated to the national and military intelligence programs totaled $67.9 billion.[8]

The complexity and range of activities the intelligence authorizing committees oversee covers a wide range. According to a recent House Intelligence Committee report, current legislation:

> provides authorization for critical national security functions, including: CIA personnel and their activities worldwide; tactical intelligence support to combat units in Afghanistan; NSA's [National Security Agency's] electronic surveillance and cyber defense; global monitoring of foreign militaries, weapons tests, and arms control treaties, including use of

[5] S.Res. 400 §A.

[6] These secure spaces are known as Secure Compartmented Information Facilities (SCIFs).

[7] Other windows into committee operations include occasional open hearings such as the annual threat briefing by the Director of National Intelligence, reports of committee investigations, and so on. See committee websites: http://intelligence.house.gov and http://www.intelligence.senate.gov/.

[8] For FY2014, the aggregate amount (base and supplemental) appropriated to the national and military intelligence programs totaled $67.9 billion. (NIP $50.5 billion, MIP $17.4B billion) See Office of the DNI, "DNI Releases Budget Figure for FY2014 National Intelligence Program," News Release No. 43-14, October 30, 2014, at http://www.dni.gov/index.php/newsroom/press-releases/. See also Department of Defense, "DOD Releases Military Intelligence Program (MIP) Appropriated Top Line Budget for Fiscal Year (FY) 2014," Release No: NR-550-14, October 30, 2014, at http://www.defense.gov/releases/. See also CRS Report R42061, *Intelligence Spending and Appropriations: Issues for Congress*, by Marshall C. Erwin and Amy Belasco.

> satellites and radars; real-time analysis and reporting on political and economic events, such as current events in the Middle East and Eastern Europe; and research and technology to maintain the country's technological edge.[9]

The authorizing legislation passed by the intelligence committees has particular power with the IC agencies because the respective rules that established the intelligence committees provided that, "no funds would be expended by national intelligence agencies unless such funds shall have been previously authorized by a bill or joint resolution passed by the Senate [and House] during the same or preceding fiscal year to carry out such activity for such fiscal year."[10] In 1985, Section 504 of the National Security Act was tightened to require that appropriated funds available to an intelligence agency could be obligated or expended for an intelligence or intelligence-related activity only if "those funds were specifically authorized by the Congress for use for such activities."[11] If and when intelligence authorization bills fail to pass, the IC relies on language in appropriation bills that both authorizes and appropriates funds, until such time as an authorization bill is passed.[12]

In terms of process, each year the House and Senate intelligence committees produce their respective versions of the Intelligence Authorization Act (IAA). Each committee produces an unclassified bill, an unclassified report, and a classified "Schedule of Authorizations" (also known as the "Classified Annex," or simply "the Annex") that provide detailed guidance to the nation's intelligence agencies. The Annex contains a schedule of authorization budget numbers as well as committee guidance and requirements that directly pertain to the classified material and cannot be disclosed publicly.[13] Committee reports state that the Annex "is incorporated by reference in the Act and has the legal status of public law."[14] Both intelligence committees make

---

[9] U.S. Congress, House Permanent Select Committee, *Intelligence Authorization Act for Fiscal Years 2014 and 2015*, report to accompany H.R. 4681, 113th Congress, 2d sess., H.Rept. 113-463, (Washington DC: GPO, 2014), p. 17.

[10] S.Res. 400, §12; H.Res. 658, §11(I). (Both resolutions provided an exception for continuing appropriations bills or resolutions.) The extra power is because most agencies in the executive branch spend appropriated money free of the restrictions imposed by Section 504. There is no statutory reason to prohibit them from spending appropriated funds—especially if authorizing committees failed to pass authorization bills. See CRS Report R42098, *Authorization of Appropriations: Procedural and Legal Issues*, by Jessica Tollestrup and Brian T. Yeh. The IC is careful to spend money only if it both authorized and appropriated. See Dan Elkins, *Managing Intelligence Resources*, 4th Edition, (Dewey, AZ: DWE Press, 2014), p. 7-8.

[11] 50 U.S.C. §414(a)(1). The requirement for "specific authorization" was added to the National Security Act by the *Intelligence Authorization Act for FY1986* (P.L. 99-169), §401(a). The report accompanying the House version of H.R. 2419 (which became P.L. 99-169) stated that "Specifically authorized is defined to mean that the activity and the amounts to be spent for that activity have been identified in a formal budget request to the Congress and that Congress has either authorized those funds to be appropriated and they have been appropriated, or, whether or not the funds have been requested, the Congress has specifically authorized a particular activity, and authorized and appropriated funds for that activity." U.S. Congress, House Permanent Select Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 1986*, Report to accompany H.R. 2419, 99th Congress, 1st sess., H.Rept. 99-106, Part 1, (Washington DC: GPO, May 15, 1985), p. 8. A concern existed at the time that funds had been used by the Reagan Administration for intelligence activities in Central America without appropriate congressional support or even awareness.

[12] See, for example, language in P.L. 110-116: "SEC. 8084. Funds appropriated by this Act, or made available by the transfer of funds in this Act, for intelligence activities are deemed to be specifically authorized by the Congress for purposes of section 504 of the National Security Act of 1947 (50 U.S.C. §414) during fiscal year 2008 until the enactment of the Intelligence Authorization Act for fiscal year 2008."

[13] H.Rept. 113-463, p. 18.

[14] See for example, U.S. Congress, Senate Select Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 2015,* report to accompany S. 2741, 113th Congress, 2nd sess., S.Rept. 113-233, (Washington DC: GPO, July 31, 2014), p. 1. There are many other important provisions included in the Classified Annex that accompanies the intelligence legislation. Those provisions are not included in this report but are available for review by Members of Congress in intelligence committee spaces.

the Annex available for review by Members of their respective chambers, subject to appropriate disclosure restrictions.[15] Following passage of these bills,[16] a conference committee is usually convened to resolve the various differences between the House and Senate versions.

Despite the requirement for both an authorization and matching appropriation, in the years following the 9/11 attacks the intelligence committees have sometimes found it difficult to reconcile philosophical differences over important issues.[17] In some years, IAAs failed to pass one or both chambers before the beginning of the fiscal years they represented, were never passed by one or both chambers, or were vetoed by the President. **Table 1** illustrates this difficulty. The table summarizes the legislation associated with the annual intelligence authorization bill over the past 15 years. IAAs for nine fiscal years (2000-2005, 2012-2013, and 2015) were signed by the President three months into the respective fiscal year. Three intelligence bills were never sent to the President for signature (2006, 2007, and 2009) and two were vetoed (2001 and 2008). The IAA for FY2010 was passed in October 2010, a week after FY2010 was over. The IAAs for FY2011 and FY2014 were passed just a few months prior to the end of their respective fiscal years.

According to media and academic accounts, and statements by Members[18] in committee reports, the reputations of the intelligence committees suffered during the six-year period when no intelligence bills were passed.[19] One year is not really a problem because many activities are authorized on a semi-permanent basis and do not need to be reauthorized each fiscal year. The absence of an authorization bill in a particular fiscal year does not mean that ongoing programs cease to be authorized. Authorization bills may enact far-reaching provisions that are essentially timeless—reporting requirements that recur each year until repealed or suspended by another authorization bill. In this case, however, no intelligence legislation was signed into law for six years (December 2004 to October 2010, see **Table 1**).

During the years when there were no authorization bills, the appropriation committees had the *de facto* ability to both authorize and appropriate. In addition, other authorizing committees with intelligence-related oversight responsibilities began reestablishing their prerogatives in regard to IC activities that fell into their areas of jurisdiction.[20] Beginning in 2009, intelligence committee leaders in both parties dedicated themselves to getting intelligence authorization bills passed on an annual basis. The combined efforts of SSCI Chairwoman Feinstein and HPSCI Chairman Rogers have been particularly effective.[21] **Table 1** illustrates the fact that there has been an

[15] See remarks by Rep. Michael Rogers, *Congressional Record*, vol. 159 (November 21, 2013), p. H7335.

[16] Per S.Res. 400 §3(b)(1), and by convention, the Senate's version of the IAA is sequentially referred to the Senate Armed Services Committee before it is voted on in the Senate.

[17] For details, see CRS Report R40240, *Intelligence Authorization Legislation: Status and Challenges*, by Marshall C. Erwin.

[18] U.S. Congress, House Permanent Select Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 2014*, report to accompany H.R. 3381, 113th Congress, 1st sess., H.Rept. 113-277, (Washington DC: GPO, November 25, 2013), "Committee Statement and Views," on p. 8, "For too many years, intelligence authorization negotiations were the victim of partisan infighting and turf battles."

[19] See for example, Jennifer Sims and Burton Gerber, *Transforming U.S. Intelligence*, (Washington DC: Georgetown University Press, 200C). p. 245.

[20] Other committees with jurisdictional claims to legislative engagement with the IC include the House and Senate Armed Services, Appropriations, Judiciary, Homeland Security, Foreign Affairs/Foreign Relations, and Government Reform/Operations committees.

[21] Senator Feinstein assumed chairmanship of the SSCI in January 2009 and Representative Rogers assumed HPSCI chairmanship in 2011. For an example of their bipartisan/bicameral approach to intelligence oversight, see "Leaders of (continued...)

intelligence bill every year since FY2010, although in several cases there have been considerable lag times between the beginning of the fiscal year and bill passage. They have been successful in getting IAAs passed in both chambers and signed by the President for every fiscal year since 2010. The IAA for FY2015 was signed into law on December 19, 2014.

Later in this report, **Table 2** provides an overview of the intelligence authorization legislation considered in the 113th Congress, with accompanying reports and the dates of major actions. **Table 3** provides a summary of selected provisions from the IAA for FY2015 with comparable provisions in the original H.R. 4681 and S. 2741.

Table 1. Intelligence Authorizations, FY2000-FY2015

Congress	Fiscal Year	House Bill	Senate Bill	FY Began (October)	Presidential Action	Public Law
106	2000	H.R. 1555	S. 1009	1999	12/3/1999	P.L. 106-120
106	2001	H.R. 4392	S. 2507	2000	11/13/2000 Vetoed[a]	—
106	2001	H.R. 5630	H.R. 5630 Senate Passed	2000	12/27/2000	P.L. 106-567
107	2002	H.R. 2883	S. 1428	2001	12/28/2001	P.L. 107-108
107	2003	H.R. 4628	S. 2506	2002	11/27/2002	P.L. 107-306
108	2004	H.R. 2417	S. 1025	2003	12/13/2003	P.L. 108-177
108	2005	H.R. 4548	S. 2386	2004	12/23/2004	P.L. 108-487
109	2006	H.R. 2475	S. 1803 Not Passed	2005	Not Requested	—
109	2007	H.R. 5020 Not Passed	S. 3237 Not Passed	2006	Not Requested	—
110	2007	H.R. 1196	S. 372	2006	Not Requested	—
110	2008	H.R. 2082	S. 1538	2007	3/8/2008 Vetoed[b]	—
110	2009	H.R. 5959	S. 2996 Not Passed	2008	Not Requested	—
111	2010	H.R. 2701	S. 1494	2009	10/7/2010	P.L. 111-259
111	2011	H.R. 5161	S. 3611	—	—	—
112	2011	H.R. 754	S. 719	2010	6/8/2011	P.L. 112-18
112	2012	H.R. 1892	S. 1458	2011	1/3/2012	P.L. 112-97
112	2013	H.R. 5743	S. 3454	2012	1/14/2013	P.L. 112-277
113	2014	H.R. 3381	S. 1681	2013	7/7/2014	P.L. 113-126
113	2015[c]	H.R. 4681	H.R. 4681	2014	12/19/14	P.L. 113-293

Source: CRS

(...continued)

Senate and House Intelligence Committees Praise Passage of 29th Intelligence Authorization Bill," *SSCI Press Release*, December 14th, 2011, at http://www.intelligence.senate.gov/press/record.cfm?id=335622.

Notes:

a. Veto message: *Congressional Record-House*, November 13, 2000, pp H11852-11853. Objectionable provision removed, IAA for FY2001 passed by both chambers in December 2000.

b. Vote on March 11, 2008, to override the veto failed.

c. For details on FY2015 legislation, to include committee report numbers, see **Table 2**.

IAAs for FY2014 and FY2015: Selected Legislative Provisions

The Intelligence Authorization Act (IAA) for Fiscal Year (FY) 2014 (P.L. 113-126) was signed into law on July 7, 2014. An IAA for FY2015 (P.L. 113-293) was signed into law on December 19, 2014.

Understanding what has happened when in terms of actions for the IAAs for FY2014 and FY2015 is difficult because of sequencing issues and bill titles. **Table 2** provides an overview of the intelligence authorization legislation considered in the 113th Congress, with accompanying reports and the dates of major actions. The following timeline may also be helpful:

- October 1, 2013: Fiscal Year 2014 began.
- November 12, 2013: The SSCI reported an IAA for FY2014 (S. 1681) out of committee to the Senate, accompanied a day later by S.Rept. 113-120.
- November 25, 2013: The HPSCI reported an IAA for FY2014 (H.R. 3381) out of committee to the House, accompanied by H.Rept. 113-277.
- May 15, 2014: The HPSCI introduced an IAA for FY2015 (H.R. 4661).
- May 20, 2014: The HPSCI introduced an IAA for both FY2014 *and* FY2015 (H.R. 4681).
- May 27, 2014: The HPSCI reported an IAA for FY2014 *and* FY2015 (H.R. 4681) to the House, accompanied later by H.Rept. 113-463.
- May 30, 2014: The IAA for FY2014 *and* FY2015 (H.R. 4681) was passed by the House and sent to the Senate for consideration.
- June 11 2014: Instead of considering H.R. 4681, the Senate passed the IAA for FY2014 (S. 1681) and sent it to the House.
- June 24, 2014: The House passed the IAA for FY2014 (S. 1681)
- July 7, 2014: The IAA for FY2014 (S. 1681) became **P.L. 113-126**.
- July 31, 2014: The SSCI reported an IAA for 2015 (S. 2741) to the Senate, accompanied by S.Rept. 113-233. It was placed on the Senate Calendar.
- October 1, 2014: Fiscal Year 2015 began.
- December 9, 2014: SSCI discharged H.R. 4681 by Unanimous Consent. The amended version represented the results of an informal HPSCI SSCI compromise and included provisions from the original H.R. 4681 and S. 2741. The Senate amended version of H.R. 4681 passed in the Senate as the "IAA for FY2015."

- December 10, 2014: House agreed to the Senate amended H.R. 4681.
- December 12, 2014: Presented to the President for his signature.
- December 19, 2014: Signed, became **P.L. 113-293**.

Table 2. Intelligence Authorization Legislation, 113th Congress

Congress	Fiscal Year	House Bill	Senate Bill	Fiscal Year Began	Date Signed	Public Law
113	2014	H.R. 3381, H.Rept. 113-277 (Reported to House 11/25/2013) S. 1681 passed in House 06/24/2014	S. 1681 S.Rept. 113-120 (Reported to Senate 11/12/2013; Passed in Senate 06/11/2014)	Oct. 2013	7/7/2014	P.L. 113-126
113	2015	H.R. 4661 (No report, introduced in House as "IAA for FY2015," May 15th, 2014, not reported out of committee) H.R. 4681 (H.Rept. 113-463) Reported to House 05/27/2014 as "IAA for FY2014 and 2015." Passed House 5/30/2014 (Referred to Senate 06/02/2014) SSCI amended version of H.R. 4681 "IAA for FY2015," Passed 12/10/14	S. 2741 (S.Rept. 113-233) (Reported to Senate 07/31/2014) Informal HPSCI/SSCI compromise merged portions of S. 2741 with portions of House-passed H.R. 4681to create Senate amended H.R. 4681"IAA for FY2015" Senate considered Senate amended H.R. 4681(with Joint Explanatory Statement) instead of S. 2741. Senate amended version of H.R. 4681 "IAA for FY2015," Passed in Senate 12/09/14.	Oct. 2014	12/19/14	P.L. 113-293

Source: CRS.

IAA for FY2014 (P.L. 113-126)

Intelligence Advanced Research Projects Activity (IARPA)

Provisions in Section 104 authorize additional appropriations and positions for advanced research and development to remain available through September 2015. The advanced research and development activity refers, in part, to the Intelligence Advanced Research Projects Activity (IARPA), the research and development arm of the Office of the Director of National Intelligence (ODNI). IARPA is the IC's version of the DOD's Defense Research Projects Agency (DARPA). Both IARPA and DARPA invest in high-risk, high-payoff research programs to tackle some of the most difficult challenges of the agencies and disciplines in the defense establishment.[22] According

[22] For more on IARPA, go to http://www.iarpa.gov.

to its Director, IARPA sees itself as "an agency that makes sure no important thing remains undone because it doesn't fit somebody's mission."[23]

According to the Senate report accompanying the legislation, the committee continues to strongly support the mission of the IARPA. It recommends that "IARPA's mission should remain a priority, even during the fiscal environment when research and development investment can come under pressure. Its mission and work should be integral to the IC R&D [Research and Development] strategic plan."[24] The report goes on to say, "Therefore, the Committee strongly supports full preservation of the budget request for IARPA in FY2014 and encourages robust investment by the IC in IARPA in FY2015."[25]

Functional Managers

Section 305 codifies a section[26] of E.O. 12333 that pertains to the DNI and "functional managers," and makes several changes. Several provisions appear to be designed to make the Directors of the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the National Geospatial-Intelligence Agency (NGA) more directly accountable to Congress—especially in regard to their efforts to increase the efficiency, effectiveness, and economy of their government operations—because they bring the SSCI into the appointment process for these individuals and increase their reporting requirements.

E.O. 12333 has been the foundational document in the IC since it was signed by President Reagan in 1981. Section 305 codifies in statute the existing requirement in E.O.12333 to designate functional managers for signals intelligence (SIGINT), human intelligence (HUMINT), and geospatial intelligence (GEOINT), and other intelligence disciplines. At present, the functional managers for SIGINT, HUMINT, GEOINT, and Measurement and Signals Intelligence (MASINT) are the Director of the NSA, the Director of the CIA, the Director of the NGA, and the Director of the Defense Intelligence Agency (DIA), respectively.

Duties of functional managers as described in E.O. 12333 may include:

- developing and implementing strategic guidance, policies, and procedures for activities related to a specific intelligence discipline or set of intelligence activities;
- setting training and tradecraft standards;
- ensuring coordination within and across intelligence disciplines and IC elements and with related non-intelligence activities; and
- advising on the management of resources; policies and procedures; collection capabilities and gaps; processing and dissemination of intelligence; technical architectures; and other issues or activities determined by the Director.[27]

[23] Peter Highnam, IARPA Director, "Opening Remarks," IARPA Day, College Park Marriott & Conference Center, Hyattsville, Maryland, October 30th, 2014.

[24] S.Rept. 113-120, p. 18.

[25] Ibid., p. 21.

[26] E.O. 12333, "U.S. Intelligence Activities," 46 *Federal Register* 59941, (As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)), §1.3(b)(12)

[27] Ibid.

Section 305 also gave responsibility for designating functional managers (that is, the directors of the CIA, NSA, NGA, and DIA) to the President. Under E.O. 12333, the functional managers were designated by the DNI. The section codifies the existing responsibilities of the functional managers to act as the principal adviser to the DNI for their respective intelligence function and in the same capacity for the Secretary of Defense. It also establishes a new requirement for each functional manager to report to Congress annually on the state of their function; this report is scheduled to occur no later than two weeks after the President's budget submission.

The reporting requirements in Section 306 call on each functional manager to identify those programs, projects, and activities that comprise the intelligence discipline for which they are responsible and to report on resource issues and other matters relevant to the state of the function such as "efforts to integrate such function with other intelligence disciplines or to establish consistency in tradecraft and training; and technology developments." This section represents an effort to better integrate and coordinate two "pots" of intelligence money—"national" and "military."[28] (**Table A-2** in the Appendix contains funding sources and illustrates the fact that the Directors of DIA, NGA, NRO, and NSA manage several types of intelligence money.)

Financial Auditability

Section 309 directs the DNI and the Directors of the, CIA, DIA, NSA, National Reconnaissance Office (NRO), and NGA to undergo full financial audits beginning with FY2014 financial statements. Some background is useful on this provision because there is a very long history of presidential and congressional oversight efforts to force the IC into compliance with federal financial accounting standards. IAAs and committee reports have contained a multitude of provisions along these lines since at least FY2002. The Senate report accompanying the IAA for FY2002 called for the financial statements of the NRO, NSA, CIA, DIA, and what is now the NGA to be audited by a statutory Inspector General (IG) or independent public accounting firm by March 1, 2005.[29] In the Senate report accompanying its IAA for FY2010, the SSCI noted the following IC response:

> The bottom line is that more than ten years after the President called for action, and more than four years after the Committee anticipated receiving auditable statements, the five agencies are still unable either to produce auditable financial statements or receive favorable audit opinions on those that are auditable. The current projection for doing so is at least four years away.[30]

The Senate report goes on to urge the IC to get its accounts auditable and to establish an IC-wide business enterprise architecture (BEA) and a consolidated financial statement for the National Intelligence Program:

> Accordingly, the April 2007 plan has now been superseded by the imperative to construct a BEA, which makes the 2012 auditability timeline difficult or impossible to achieve for most agencies. Nonetheless, the Committee strongly supports this BEA work, which, if successful, will provide a stronger foundation for sustainable, financial auditability. Indeed, the

[28] For more on IC budget categories, see **Appendix**.

[29] S.Rept. 107-63.

[30] U.S. Congress, Senate Select Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 2010*, Report to accompany S. 1494, 111th Cong., 1st sess., July 21, 2009, S.Rept. 111-55, pp. 57-58.

> Committee has repeatedly called for a BEA over the last four years. Section 322 of this bill is designed to empower the DNI's fledgling BTO to produce this business systems architecture.
>
> Finally, the Committee believes that both the Congress and the DNI would benefit from the creation of a consolidated National Intelligence Program financial statement. Such a statement would provide valuable macro-level data and, once established, offer insight into financial trends within the Intelligence Community.[31]

Foreign Counterintelligence Program (FCIP) Merged Into General Defense Intelligence Program (GDIP)

Section 314 directs the DNI to merge the Foreign Counterintelligence Program (FCIP) into the (GDIP). The Director of DIA is program manager for both programs. The FCIP designation was an accounting tool to track money used solely for counterintelligence purposes. The GDIP and other IC budget programs are included in the **Appendix**.

Enhanced Oversight Measures

Legal Opinions

Section 321 of the IAA for FY2014 focuses on the opinions of the Office of Legal Counsel (OLC) in the Department of Justice (DOJ) concerning intelligence activities. The provision is designed to increase the committees' ability to understand and question the legal reasoning behind OLC opinions relevant to the committees' oversight functions.[32] This section requires the Attorney General to provide a listing of every opinion of the OLC that has been provided to an element of the IC, whether classified or unclassified. Provisions were made for information associated with covert action "findings"[33] and information subject to "executive privilege." The Senate report explains these provisions in the following manner:

> While the Committee generally is kept apprised of the legal basis for U.S. intelligence activities, as required by Sections 502 and 503 of the National Security Act of 1947, neither the Department nor the IC routinely advises the Committee of the existence of OLC opinions that are relevant to the Committee's oversight functions. This presents an impediment to the

[31] Ibid. Provisions in the IAA for FY2010 amend 50 U.S. Code to include §3100 "Intelligence Community business system transformation."

[32] Intelligence Committee concerns about OLC legal reasoning stem, in part, from opinions related to the CIA Detention and Interrogation Program, particularly the legal reasoning justifying the use of waterboarding as an Enhanced Interrogation Technique. See, for example, John D. Rockefeller, "Release of Declassified Narrative Describing the Department of Justice Office of Legal Counsel's Opinions on the CIA Detention and Interrogation Program," April 22, 2009, at http://www.intelligence.senate.gov/pdfs/olcopinion.pdf.

[33] "Finding" is a term that refers the requirement that a president put in writing when he or she determines that a covert action is "important to national security." The requirement goes back to December 1974, when Congress passed the "Hughes-Ryan Amendment" to the Foreign Assistance Act of 1961, formalizing the regulation of covert actions, primarily in reaction to President Nixon's covert bombings in Cambodia. The Hughes-Ryan Amendment required that any covert action be supported by a Presidential finding that the action was "important to the national security" and that the President report "in a timely fashion, a description and scope of such [actions] to the appropriate committees of the Congress—House and Senate Foreign Relations, House and Senate Armed Services and House and Senate Appropriations." (This grew to eight committees after the House and Senate intelligence committees were established.) See P.L. 93-559, §659 "Limitation on Intelligence Activities," December 30, 1974, enacting 22 U.S.C. §2422. See also William E. Conner, "Congressional Reform of Covert Action Oversight Following the Iran-Contra Affair," *Defense Intelligence Journal* 2 (1993), pp. 35, 41

> Committee's oversight function, as the Committee cannot request access to legal analysis when it is not made aware that such analysis exists. Section 321 would ensure that the Committee is aware of the existence of relevant OLC opinions so that it can obtain access to the legal analysis set forth in these opinions through a process of accommodation with the Executive branch.[34]

Appointments

Title IV of P.L. 113-126 changes the appointment process for four key individuals, the Directors of NSA and NRO and the Inspectors General (IGs) of these two agencies, making all four presidential appointments with the advice and consent of the Senate.[35] This is different from provisions in E.O. 12333. In that document, the "relevant department or bureau head shall provide recommendations and obtain the concurrence of the DNI" for the selection of most of the IC agency directors[36] with certain DOD exceptions.[37]

These appointment process provisions allow the Senate Intelligence Committee to take a more active part in the selection of these four key individuals than it has in the past.[38] The desire for a greater role in the confirmation process for the Director of NSA has been fueled in the past year by the numerous hearings concerning NSA surveillance procedures and privacy protections. Confirmation of the NRO Director has been fueled by concerns associated with acquisition of complex, expensive programs.[39] Attention to the IGs of the NSA and NRO follows a similar rationale.

IGs are an independent oversight tool throughout American government.[40] The Inspector General Act of 1978 (P.L. 95-452) established a government-wide system of IGs, some appointed by the President with the advice and consent of the Senate and others administratively appointed by the heads of their respective federal entities.[41] IGs are authorized to ''conduct and supervise audits and investigations relating to the programs and operations'' of the government and ''to promote economy, efficiency, and effectiveness in the administration of, and ... to prevent and detect fraud and abuse in, such programs and operations."[42] They also perform an important reporting function

[34] S.Rept. 113-120, p. 7.

[35] See also the Senate version of the IAA for FY2010 §432.

[36] E.O. 12333, §1.3 (d) Director of the National Security Agency, the Director of the National Reconnaissance Office, the Director of the National Geospatial-Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State for Intelligence and Research, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury, and the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation.

[37] Ibid., the Under Secretary of Defense for Intelligence (USD(I)); the Director of the Defense Intelligence Agency (DIA); uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps above the rank of Major General or Rear Admiral; the Assistant Commandant of the Coast Guard for Intelligence; and the Assistant Attorney General for National Security.

[38] For a complete list of the positions over which the SSCI has exercised jurisdiction, see CRS Report RL30959, *Presidential Appointee Positions Requiring Senate Confirmation and Committees Handling Nominations*, by Christopher M. Davis and Jerry W. Mansfield.

[39] E.O. 12333, §1.3 (d), pp. 9-10.

[40] See CRS Report R43722, *Offices of Inspectors General and Law Enforcement Authority: In Brief*, by Wendy Ginsberg.

[41] See §8G of the Inspector General Act of 1978, as amended, for those IGs who are administratively appointed, generally for reasons associated with protecting national security.

[42] Ibid., §2(1-3).

by ‘‘keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies relating to the administration of ... programs and operations and the necessity for and progress of corrective action.’’[43]

Traditionally, the issue of IGs in the IC has focused on how independent from an agency director they can and should be. Concerns have been raised over whether an overzealous IG might pose a threat to agency operations.[44] For example, while the CIA has had an IG since 1952, it was only in 1989 that Congress enacted legislation mandating an “independent” IG at CIA, appointed by the President with the advice and consent of the Senate. Before that, CIA IGs were appointed by the Director of the Central Intelligence Agency.[45]

The IAA for FY2014 called for a completely independent ODNI IG appointed by the President, with the advice and consent of the Senate, to report directly to the DNI. To enhance the IG’s independence within the ODNI, the IG may be removed only by the President, who must communicate the reasons for the removal to the congressional intelligence committees.[46] The IGs of the CIA and Departments of Defense, Energy, Homeland Security, Justice, State, and the Treasury are appointed by the President with the advice and consent of the Senate.[47] The IAA for FY2014 extended this list to include the IGs at the NSA and NRO.

S.Res. 470[48] was passed by the Senate on July 7, 2014 (in conjunction with the IAA for FY2014), to amend the committee’s charter legislation[49] and implement these new appointment provisions. The procedures in the Senate resolution point out the SSCI’s shared jurisdiction with other IC oversight committees:

> 1) Assistant Attorney General for National Security: referred to the Judiciary Committee and, if and when reported, to the SSCI. This person heads the National Security Branch, a Federal Bureau of Investigation (FBI) component of the IC.
>
> 2) NSA Director, NSA/IG, NRO Director and NRO/IG:
>
> a) If military and on active duty—referred to the SASC and, if and when reported, to the SSCI.
>
> b) If civilian—referred to the SSCI and, if and when reported, to the SASC.

Notice that in each case, only the primary committee with jurisdiction has the right of refusal. The nomination proceeds forward, via the mechanism of sequential referral, only if the primary committee reports it out of committee. If the secondary committee fails to report the nomination after a specified time, the nomination is automatically discharged and placed

[43] Ibid.

[44] See Britt Snider, “Creating a Statutory IG at the CIA,” *Studies in Intelligence*, vol. 44, no 5, (August 3, 2011), p. 1, https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol44no5/html/v44i5a02p.htm.

[45] Ibid. See also 50 U.S.C. §403(q) and CIA Act of 1949 §17. The Director of the CIA was also the Director of Central Intelligence at this time. For more, see **Appendix**.

[46] S.Rept. 111-55, p. 32.

[47] Ibid, p. 40.

[48] U.S. Congress, Senate Select Committee on Intelligence, *S.Res. 470 - A resolution amending Senate Resolution 400 (94th Congress) to clarify the responsibility of committees of the Senate in the provision of the advice and consent of the Senate to nominations to positions in the intelligence community*, 113th Congress, 2nd sess. (Washington DC: GPO, July 7, 2014).

[49] S.Res. 400.

on the Senate's Executive Calendar. In its report, the SSCI notes that it believes Senate confirmation of these four positions will improve oversight and accountability and, ultimately, the effectiveness of the agencies in question.

Insider Threats

Title V of P.L. 113-126 contains a number of provisions designed to improve security. Several address the "insider threat problem" and speak to recommendations made by a presidential group established to review intelligence and communications technologies. The insider threat problem refers to efforts by individuals who work within the IC to purposefully leak classified data and sabotage networks. The problem assumed critical proportions in 2013, when Edward Snowden, a contractor working inside NSA, released thousands of classified documents to the British newspaper *The Guardian*. The Snowden leaks came on the heels of Army Private Manning's 2010 release of thousands of classified documents to WikiLeaks.

> In a short period of time, stealing secrets has gone from the laborious task of copying papers taken surreptitiously from filing cabinets to the current age in which files can be electronically copied onto thumb drives. Manning was said to have disguised his efforts by downloading secrets onto compact discs made to look like pop music recordings.[50]

A presidential group headed by Richard Clarke issued a final report known by many as the Clarke Report.[51] Section 501, for example, reflects the Clarke Report's recommendation (#38) to establish a personnel continuous monitoring program for those with classified information access. The HPSCI report language says "the IC might have caught Snowden sooner if it had continuously evaluated the backgrounds of employees and contractors and if IC elements had more effectively shared potentially derogatory information about employees and contractors with each other."[52] According to the HPSCI, continuous evaluation "allows the IC to take advantage of lawfully available and public information to detect warning signals that the current system of 5 year periodic investigation misses."[53]

The insider threat problem is discussed in some detail in the SSCI Report. It notes that "initiatives have been underway for years to deal with such contingencies, most recently the President's National Insider Threat Policy, signed in November 2012. However, the Committee is concerned that this policy has not been fully implemented across the IC. The Committee supports substantially enhancing and expediting efforts to deter the insider threat."[54]

Intelligence Community Information Technology Enterprise (IC ITE)

In relation to protections against insider threats, the Senate report makes reference to the IC's information technology (IT) modernization effort—the IC Information Technology Enterprise (IC

[50] Noah Bierman and Bryan Bender, "Leaks show U.S. intelligence vulnerability," *The Boston Globe*, June 11, 2013.

[51] Richard A. Clarke et al, *Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, (The White House: December 12, 2013), at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. See recommendations #37-#44. Clarke served on the National Security Council Staff from 1992-2003in a number of positions to include Special Assistant to the President for Global Affairs, Special Advisor to the President for Cyberspace, and National Coordinator for Security and Counter-terrorism.

[52] H.Rept. 113-463, p. 18.

[53] Ibid.

[54] S.Rept. 113-120, p. 17.

ITE, pronounced "eyesight")—and says that it "must provide the infrastructure to detect insider threats earlier and more effectively. Robust counterintelligence data and analytic tools to monitor, analyze and audit personnel behavior will be critical to this endeavor."[55] By way of explanation, the goal of IC ITE is a secure and trusted IT environment. IC ITE services focus on providing a common IC desktop, secure online collaboration tools, and secure common cloud architectures. If all goes as planned, IC ITE will help the IC to pool IT resources, cut costs, increase data storage capabilities, increase mission agility and efficiency, and increase the ability to protect all levels of data.[56]

Security Clearance Reciprocity

In terms of the clearance process, provisions address the time and money associated with the security investigation and adjudication process, and reciprocity of clearances between agencies. Security clearance reciprocity refers to ongoing efforts to have "all security clearance background investigations and determinations completed by an authorized investigative agency or authorized adjudication agency ... accepted by all agencies."[57] Reports by the Government Accountability Office (GAO) and ODNI offer analysis which suggests that agencies may be reluctant to accept the background investigations or security clearance determinations made by other agencies.[58]

The Senate report accompanying S. 1681 provides background information to clarify some of the provisions associated with reciprocity—citing several problems associated with "out-of-scope" determinations.[59] Out-of-scope refers to the fact that an individual's background investigation for one IC agency may not adhere to the requirements of another IC agency for a variety of possible reasons. For example, an out-of-scope determination may depend on factors associated with the depth and breadth of the background investigation or the lack of a particular type of polygraph examination. It may also be based on timing issues such as the time elapsed since the individual's initial investigation (or periodic update), a gap in his or her agency employment, or date of his or her last polygraph examination. If agency requirements do not match on any or all criteria, there may be an out-of-scope determination made by security personnel that overrides the reciprocity requirement.[60]

The Senate report points out that some agencies are inconsistent when it comes to applying out-of-scope determinations—waiving inconsistencies for its own employees but not for employees of other agencies. It also points out what may be inefficiencies and unnecessary costs associated with the adjudication process.

---

[55] Ibid.

[56] Chief Information Officer, Office of the DNI, "IC IT Enterprise Fact Sheet," p. 1, at http://www.dni.gov/files/documents/IC%20ITE%20Fact%20Sheet.pdf.

[57] Mandated in P.L. 108-458, §3001(d) the *Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004*.

[58] See, for example, U.S. Congress, House Permanent Select Committee on Intelligence, *Security Clearance Reform—Upgrading the Gateway to the National Security Community,* 110th Congress, 2nd sess., H.Rept. 110-916, Washington, DC: GPO, November 20, 2008); Testimony of Charles B. Sowell, Deputy Assistant Director for Special Security, Office of the Director of National Intelligence, for U.S. Congress, Senate Homeland Security and Government Affairs, *Security Clearance Changes*, hearings, 112th Congress, 2nd sess., June 21, 2012; and U.S. Government Accountability Office, *Personnel Security Clearance, Progress Has Been Made to Improve Timeliness but Continued Oversight Is Needed to Sustain Momentum*, GAO-11-65, November 2010, p. 27.

[59] S.Rept. 113-120, p. 11.

[60] CRS Report R43216, *Security Clearance Process: Answers to Frequently Asked Questions*, by Michelle D. Christensen and Frederick M. Kaiser. See also CRS Report RL31988, *Polygraph Use by the Department of Energy: Issues for Congress*, by Alfred Cumming (archived).

> The Committee understands that some agencies have denied security clearance reciprocity for some IC personnel where an eligibility determination is out-of-scope, even when the agency employs personnel whose eligibility determinations also are out of scope. In addition, the Committee understands that some agencies have delayed employment of personnel who have been determined to be eligible for access to classified information while the agency adjudicates their suitability for employment. The Committee believes that both of these practices inappropriately impede the movement of cleared personnel between agencies, often at significant cost to the government.[61]

Section 501 requires the DNI, subject to the direction of the President, to ensure that the background of each employee or officer and contractor of the IC is monitored continuously to determine their eligibility for access to classified information; and secondly, to require IC elements to share potentially derogatory security information concerning any employee that may impact the eligibility of such individuals for a security clearance.

Section 504 requires the DNI to report to Congress each year, through 2017, on the reciprocal treatment of security clearances, including (1) the periods of time required by authorized adjudicative agencies for accepting background investigations and determinations completed by an authorized investigative entity or adjudicative agency; and (2) the total number of cases in which a background investigation or determination completed by an authorized investigative entity or adjudicative agency is, or is not, accepted by another agency.

Whistleblower Protections

Intelligence whistleblowers are generally IC employees or contractors who want to focus attention on possible agency wrongdoings. Such individuals can face retaliation from their employers for their disclosures, and the fear of such retaliation may deter whistleblowing. The IC Whistleblower Protection Act (ICWPA) of 1998 provides a process by which employees, or contractor employees, of the DIA, NGA, NRO, and the NSA can report matters of "urgent concern" to the intelligence committees of Congress.[62] The act was augmented by Presidential Policy Directive 19, signed by President Obama in 2012, which required IC agencies to provide employees with protections from retaliation.

This issue is a particular concern for the IC because it does not want individuals leaking classified information under the guise of "whistleblowing." On the other hand, whistleblowing is an important element of the oversight function, in that it helps overseers to identify "urgent concerns," defined as follows:[63]

- A serious or flagrant problem, abuse, violation of law or Executive Order, or deficiency relating to the funding, administration, or operations of an intelligence activity involving classified information, but does not include differences of opinion concerning public policy matters;
- A false statement to Congress, or a willful withholding from Congress, on an issue of material fact relating to the funding, administration, or operation of an intelligence activity; and/or

[61] S.Rept. 113-120, p. 11.

[62] See IC Inspector General website, at http://www.dni.gov/index.php/about-this-site/no-fear-act/whistleblower-protection-laws.

[63] "ICWPA Complaints," DOD IG website, at http://www.dodig.mil/programs/whistleblower/icwpa.html.

- An action, including a personnel action described in Section 2302(a)(2)(A) of Title 5, constituting reprisal or threat of reprisal prohibited under Section 7(c) of the Inspector General Act of 1978, as amended, in response to an employee reporting an urgent concern.

When NSA contractor Edward Snowden was asked why he did not go to the government first, he cited the severe retaliation that previous IC whistleblowers experienced when they worked through institutional channels without specific rights.[64]

Title VI of P.L. 113-126 provides additional protections for IC whistleblowers against reprisals. Section 602 includes due process protections, including the right (1) to an independent and impartial fact-finder; (2) for notice and the opportunity to be heard, including the opportunity to present relevant evidence, including witness testimony; (3) to be represented by counsel; (4) to receive a decision based on the record developed; and (5) to receive a decision within 180 days, unless the employee and the agency agree to an extension, or the impartial fact-finder determines in writing that a greater time period is needed in the interest of fairness or national security. An employee is permitted to appeal the agency's decision within 60 days of receiving it. Detailed procedures for each stage of the process are included in the bill. Some whistleblower advocates would like to see additional protections available to IC contractors as well.[65]

Section 604 states that the legislation affords no protections for certain terminations of employment, if, for example, the Director or agency head determines the termination to be in the interest of the United States, determines that the procedures prescribed in other provisions of law that authorize the termination of the employee's employment cannot be invoked in a manner consistent with national security, and notifies Congress within five days of the termination. Additional information on Title VI provisions is available in CRS Report R43765, *Intelligence Whistleblower Protections: In Brief*, by Rodney M. Perry.

Contractor Responsibility Watch List

There are several additional provisions in the SSCI Report that refer to activities not specifically mentioned in the unclassified bill but nonetheless include directive language.[66] For example, the SSCI Report includes a management-focused provision designed to enhance the procurement process with a "Contractor Responsibility Watch List."[67] The committee wants the IC to have a better sense of whether prospective vendors are debarred, suspended, or listed on the federal government's System for Awards Management (SAM), a Web-based system maintained by the General Services Administration (GSA). The report cites the following concerns.[68]

[64] Suzanna Andrews, et al., "The Snowden Saga: A Shadowland of Secrets and Light," *Vanity Fair*, (May 2014): pp. 4-5, at http://www.vanityfair.com/politics/2014/05/edward-snowden-politics-interview#.

[65] See for example, Charles S. Cook, "Intel Contractors' Whistleblower Rights are a work in Progress, *Government Executive*," August 30, 2013, at http://www.govexec.com/oversight/2013/08/intel-contractors-whistleblower-rights-are-work-progress/69026/.

[66] While not in the legislation, as report language accompanying the bill, the Committee will expect the IC to comply. Reports are written by staff and are directed to Members and staff outside the Committee to help everyone understand committee actions and intentions. Congressional intent is clear and though nonbinding, most executive branch officials agree that ignoring such provisions can be perilous.

[67] S.Rept. 113-120, p. 16.

[68] Ibid.

> [T]he IC does not have an IC-wide mechanism for identifying and tracking exploitative, unscrupulous, suspended or debarred contractors to ensure the Community deals only with vendors who are responsible in fulfilling their legal and contractual obligations. It is through the sharing of such information that the IC can make informed decisions, ensure the Community conducts business only with responsible contractors, prevent suspended and debarred contractors from initiating or repeating business throughout the IC, and avoid misuse or loss of potentially billions of dollars of taxpayer money.

The IAA for FY2015 (P.L. 113-293)

In the normal legislative process, after one house passes a bill and the other then passes it with amendments, the House and Senate need to resolve the differences between their positions and agree to exactly the same language. A formal conference committee may not be necessary if the two chambers can reach an agreement through informal negotiations—as was the case with the IAA for FY2015.[69] The IAA for FY2015 essentially combined those provisions offered in the original House and Senate bills that both chambers could agree to. Several provisions in the original H.R. 4681 no longer appear in the amended version of H.R. 4681 passed in December.[70] For example, Title IV, proposing a General Counsel to the NSA IG, is no longer included. Other provisions, such as Section 305 on "functional managers," were incorporated into the IAA for FY2014 passed in July 2014.

In the absence of a conference committee, there was no formal conference committee report to accompany the amended version of H.R. 4681. Instead, a short "Joint Explanatory Statement" was read into the *Congressional Record* on December 9, 2014.[71] In a number of cases, the formal HPSCI and SSCI committee reports (H.Rept. 113-463 and S.Rept. 113-233) accompanying the committee's originally proposed legislation offer fuller descriptions of the provisions in the amended H.R. 4681 than those contained in the joint statement. Unfortunately, section numbers for similar provisions vary across these reports, and determining what is new or different in the IAA for 2015 can be difficult.

Table 3 lists selected provisions in the IAA for FY2015 (P.L. 113-293) and provides corresponding provisions in the original House and Senate versions, if present. For example, Section 309 of the IAA for FY2015, on data retention, is Section 306 in S. 2741. Section 307 on management and oversight of financial intelligence, is Section 304 in S. 2741. Section 303 requiring a National Intelligence Strategy is new, but reads much like the provision for a Quadrennial Intelligence Strategic Review in S. 2741. Section 310 is new but is simply a technical correction to existing statutory language (see Whistle Blower Protections section below). Section 323 requiring an annual report on violations of law or EO has corresponding provisions in both the original H.R. 4681 (Section 321) and S. 2741 (Section 313).

[69] See CRS Report 96-708, *Conference Committee and Related Procedures: An Introduction*, by Elizabeth Rybicki.

[70] Some provisions may have been moved into the Classified Annex of the intelligence authorization legislation.

[71] "Joint Explanatory Statement to Accompany the Intelligence Authorization Act for Fiscal Year 2015," Senate Debate, *Congressional Record*, daily edition, vol. 160, part 149 (December 9, 2014), pp. S6464-S6465.

Table 3. Selected Provisions in the IAA for FY2015 (P.L. 113-293) with Corresponding Provisions in House and Senate Proposed Legislation

H.R. 4681[a]	S. 2741	IAA for FY2015 (P.L. 113-293)
	303: Quadrennial Intelligence Strategic Review	303. National Intelligence Strategy
307		304. Software Licensing
310		305. Reporting of employment activities by former intelligence officers and employees
315		306. Inclusion of Predominantly Black Institutions in Intelligence Officer Training Program
	304	307. Management and oversight of financial intelligence.
	305	308. Analysis of private sector policies and procedures for countering insider threats.
	306	309. Procedures for the retention of incidentally acquired communications.
		310. Clarification of limitation of review to retaliatory security clearance or access determinations.
	307	311. Feasibility study on consolidating classified databases of cyber threat indicators and malware samples.
	308	312. Sense of Congress on cybersecurity threat and cybercrime cooperation with Ukraine.
	309	313. Replacement of locally employed staff serving at United States diplomatic facilities in the Russian Federation.
	310	314. Inclusion of Sensitive Compartmented Information Facilities in United States diplomatic facilities in the Russian Federation and adjacent countries
	311	321. Report on declassification process.
	312	322. Report on intelligence community efficient spending targets.
321	313	323. Annual report on violations of law or executive order.
	314	324. Annual report on intelligence activities of the Department of Homeland Security.
	316	325. Report on political prison camps in North Korea.
327		326. Assessment of security of domestic oil refineries and related rail transportation infrastructure.
330		327. Enhanced contractor level assessments for the intelligence community.
331		328. Assessment of the efficacy of memoranda of understanding to facilitate intelligence-sharing.
329		329. Report on foreign man-made electromagnetic pulse weapons.
333		330. Report on United States counterterrorism strategy to disrupt, dismantle, and defeat al-Qaeda and its affiliated or associated groups.
324		331. Feasibility study on retraining veterans in cybersecurity.

Source: CRS

Notes:

a. To read original text, see the version referred to the Senate.

National Intelligence Strategy (NIS)

Section 303 requires the DNI to develop a NIS every four years beginning in 2017.[72] It requires each strategy, in a manner consistent with other relevant U.S. agencies' strategic plans and national-level plans, to (1) address national and military intelligence, including counterintelligence; (2) identify current and future major national security missions of the intelligence community, including factors that may affect performance during the following 10-year period; (3) assess threats from foreign intelligence and security services, as well as insider threats; (4) outline organizational roles and missions; and (5) identify sources of strategic, institutional, programmatic, fiscal, and technological risk.

This requirement codifies an existing practice. The ODNI has been producing a NIS since 2005 largely in reaction to provisions included in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), referred to as the Intelligence Reform Act or IRTPA. The IRTPA did not specifically mandate one overarching NIS, but did require strategic plans for many intelligence-related activities such as counterterrorism and partnerships with foreign countries. The 2005 NIS[73] implemented while Ambassador John Negroponte was DNI was updated in 2009 under DNI Dennis Blair and again in 2014 by DNI James Clapper.[74]

Data on U.S. Persons

Section 309 prescribes how long data on U.S. persons can be retained if it is acquired incidentally (that is, inadvertently obtained) as part of investigations of foreign persons—and therefore, obtained with*out* a court order and with*out* consent.

Privacy advocates raised objections to Section 309 shortly before bill passage in the House arguing the provision expands the government's authority to collect the communications of U.S. persons.[75] The intelligence committees defended the provisions, countering that Section 309 does the opposite—it "protects privacy rights.… Although the executive branch already follows procedures along these lines, Section 309 would enshrine the requirement in law."[76]

---

[72] This new provision resembles the requirement originally in S. 2741 for a *Quadrennial Intelligence Strategic Review* similar in content to the DOD's Quadrennial Defense Review (QDR). The DOD QDR is a long-term review of DOD strategy and priorities. For further details, see the DOD's QDR webpage at http://www.defense.gov/home/features/2014/0314_sdr/qdr.aspx.

[73] Office of the Director of National Intelligence, *National Intelligence Strategy: Transformation through Integration and Innovation*, October 2005, at http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/NISOctober2005.pdf.

[74] Office of the Director of National Intelligence, *National Intelligence Strategy,* August 2009, http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2009_NIS.pdf; and *National Intelligence Strategy 2014*, at http://www.dni.gov/files/documents/2014_NIS_Publication.pdf.

[75] See, for example, Representative Justin Amash, "Block New Spying on U.S. Citizens: Vote 'No' on H.R. 4681," *Dear Colleague*, December 10, 2014, at https://www.facebook.com/repjustinamash/posts/812569822115759. See also Electronic Frontier Foundation, "EFF Statement on the 2015 Intelligence Authorization Bill," December 15, 2014, at https://www.eff.org/deeplinks/2014/12/eff-statement-2015-intelligence-authorization-bill.

[76] U.S. Congress, House Permanent Select Committee on Intelligence, "Fact Sheet," at http://intelligence.house.gov/press-release/fact-sheet-hr-4681-fiscal-year-2015-intelligence-authorization-act. For SSCI defense of Section 309 see Mario Trojillo, "Intel figures downplay spy provision," *The Hill*, December 15, 2014, at http://thehill.com/policy/(continued...)

Section 309 requires all IC elements to adopt Attorney General-approved procedures to prohibit retention for a period in excess of five years of nonpublic telephone or electronic communications to or from a U.S. person that are acquired without a court order and without the consent of a person who is a party to the communication (including communications in electronic storage), with some national security-related exceptions.[77]

The section also requires the head of an IC element approving retention in excess of five years to certify to Congress (1) the reasons extended retention is necessary to protect U.S. national security, (2) the duration of the retention, the particular information to be retained, (3) the measures being taken to protect the privacy interests of U.S. persons or persons located inside the United States.

Whistle Blower Protections and Security Clearances

Section 310 is a technical provision that adds to the Whistle Blower protections discussed earlier in this report as part of the IAA for FY2014. It amends legislation[78] pertaining to policies and procedures associated with security clearance actions taken against individuals alleging reprisal for having made a protected disclosure.

If a determination is made to suspend or revoke a security clearance (or access to classified information), this provision allows employees to retain their government employment status while the challenge is pending. The provision extends protections, to the extent practicable, to individuals alleging reprisal for having made a protected disclosure (provided the individual does not disclose classified information or other information contrary to law) to appeal any action affecting an employee's access to classified information.

The Homeland Security Intelligence Program

Section 324 requires the Department of Homeland Security (DHS) Under Secretary for Intelligence and Analysis (USDHS/I&A) to provide the congressional intelligence committees with a report on each intelligence activity of each intelligence component of the Department that includes, among other things, the amount of funding requested, the number of full-time employees, and the number of full-time contractor employees. In addition, Section 324 requires the Secretary of Homeland Security to submit to the congressional intelligence committees a report that examines the feasibility and advisability of consolidating the planning, programming, and resourcing of such activities within the Homeland Security Intelligence Program (HSIP).

According to the Joint Explanatory Statement accompanying the IAA for FY2015

> The HSIP [Homeland Security Intelligence Program] budget was established to fund those intelligence activities that principally support missions of the DHS separately from those of the NIP [National Intelligence Program]. To date, however, this mechanism has only been

(...continued)

technology/227164-intelligence-community-plays-down-worries-on-bill.

[77] Exceptions include communications that (1) suggest evidence of a crime, (2) are enciphered and appear to have a secret meaning, (3) have foreign intelligence or counterintelligence value, (4) involve only non-U.S. persons, and (5) suggest an imminent threat to human life.

[78] 50 U.S.C. §3341(b)(7), Section 3001(b)(7) of the Intelligence Reform and Terrorism Prevention Act of 2004.

> used to supplement the budget for the office of Intelligence and Analysis. It has not been used to fund the activities of the non-IC components in the DHS that conduct intelligence-related activities. As a result, there is no comprehensive reporting to Congress regarding the overall resources and personnel required in support of the Department's intelligence activities.[79]

This section is significant from an oversight perspective because it addresses shared jurisdiction between the Intelligence and Homeland Security Committees. By way of explanation, DHS/I&A is an element of the IC and is funded with National Intelligence Program (NIP) dollars.[80] However, DHS has other intelligence activities that are funded entirely with DHS money. Theoretically, those activities support the DHS mission, as opposed to an IC-wide mission (intelligence for the use of Customs only, for example). This DHS-only intelligence money is called the Homeland Security Intelligence Program (HSIP). Because it is not part of the NIP, it does not belong to the DNI; it belongs instead to the Secretary of Homeland Security. The Department of Homeland Security is overseen by the Homeland Security Committees. This is a case of shared jurisdiction over intelligence-related activities. For more on IC budget programs, see the IC budget section in the **Appendix**.

Regional Issues

Section 312 illustrates the way in which certain issues such as cybersecurity and cybercrime transcend traditional boundaries between law enforcement and intelligence, and between congressional committees—in this case intelligence and judiciary. Its provisions express the sense of Congress that the President, working with the government of Ukraine should:

- initiate U.S.-Ukraine bilateral talks on cybersecurity threat and cybercrime cooperation, with additional multilateral talks that include other law enforcement partners such as Europol and Interpol;
- work to obtain a commitment from Ukraine to end cybercrime directed at persons outside Ukraine and to work with the United States and other allies to deter and convict known cybercriminals;
- establish a capacity-building program with Ukraine, which could include joint intelligence efforts, U.S. law enforcement agents being sent to Ukraine to aid investigations, and agreements to connect U.S. and Ukrainian law enforcement agencies through communications networks and hotlines; and
- establish and maintain a scorecard with metrics to measure Ukraine's responses to U.S. requests for intelligence or law enforcement assistance.

Two sections refer to diplomatic facilities in the Russian Federation. Section 313 is directed at the Department of State and requires the Secretary to ensure that every supervisory position at a U.S. diplomatic facility in the Russian Federation is occupied by a U.S. citizen who is subject to and has passed a thorough background check. It also directs the Secretary to submit to Congress a plan to further reduce the reliance on locally employed staff in such facilities. Section 314 requires restricted access space to be included in each U.S. diplomatic facility that is constructed

[79] "Joint Explanatory Statement to Accompany the Intelligence Authorization Act for Fiscal Year 2015," Senate Debate, *Congressional Record*, daily edition, vol. 160, part 149 (December 9, 2014), p. S6465.

[80] The USDHS/I&A is confirmed by the SSCI. See CRS Report RL30959, *Presidential Appointee Positions Requiring Senate Confirmation and Committees Handling Nominations*, by Christopher M. Davis and Jerry W. Mansfield, p. 38.

in, or undergoes a construction upgrade in, the Russian Federation, any country that shares a land border with the Russian Federation, or any country that is a former member of the Soviet Union.[81]

Section 325 directs the DNI to report to the congressional intelligence committees, the Senate Foreign Relations Committee and the House Foreign Affairs Committee, regarding political prison camps in North Korea. It requires such report to describe U.S. actions to support implementation of the recommendations of the U.N. Commission of Inquiry on Human Rights in the Democratic People's Republic of Korea, including the eventual establishment of a tribunal to hold individuals accountable for abuses. It also requires as much information as possible on topics such as prisoner populations, treatment and living conditions.

Contractor Level Assessments

Improved planning for, and management of contractors has been a recurring theme in IC legislation, particularly since September 11, 2001. The IAA for FY2015 is no exception. Section 327 amends the National Security Act to require *annual* personnel level assessments for the IC that include a separate estimate of the number of intelligence collectors and analysts contracted by each element of the IC and a description of the functions performed by such contractors.

The request echoes a similar requirement for information made five years ago—in Section 339 of the IAA for FY2010 (P.L. 111-259). Section 339 required the DNI to submit a single report (by February 2011) describing a number of contractor related issues across the IC to include hiring, training and retention; clearances; conversion of contractors to U.S. government employees; accountability mechanisms; number of contracts; and costs. Section 339 requirements included contractors associated with intelligence collection, analysis, and covert actions (including rendition, detention and interrogation activities).

The dramatic growth in IC contracting activities following the September 11, 2001 attacks on the United States has primarily been associated with the need for "surge" capacity. According to Ronald Sanders, Associate DNI when he wrote the following in 2007,

> [O]ur agencies simply did not have enough people to do the job. In the months after Sept. 11, 2001, contract personnel emerged as our "reserves," allowing us to surge to meet unprecedented mission demands. Why not just hire more civilians? We have, but it takes years to train and develop intelligence analysts and case officers. In the interim, contract personnel have filled the gap, in many cases with decades of priceless experience. [82]

Congressional overseers have long recognized that contractors provide a wide range of services for the IC (just as they do for the military) from transportation, construction, and support services, to intelligence collection, analysis and private security. Contractors provide a surge capability, quickly delivering critical support capabilities tailored to specific intelligence needs. Because contractors can be hired when a particular need arises and released when their services are no

[81] This requirement can be waived (due to national security interests) by the Secretary of State if s/he requests a waiver in writing to appropriate congressional committees prior to exercising the waiver.

[82] See Ronald P. Sanders, "The Value of Private Spies," Letter to the Editor, *Washington Post*, July 18, 2007, at http://www.washingtonpost.com/wp-dyn/content/article/2007/07/17/AR2007071701679.html. Ron Sanders was then-Associate Director of National Intelligence.

longer needed, contractors can be less expensive in the long run than maintaining a permanent in-house capability.[83]

Unfortunately, critics argue that contractors can also compromise the credibility and effectiveness of the IC and undermine operations.[84] Concerns over government reliance on contractors often focus on cost, accountability and workforce issues.[85] Most recently, the *SSCI Study of the CIA's Detention and Interrogation Program* has renewed debate over which activities performed by contractors are "inherently governmental."[86] According to the SSCI Study's Finding 13, "The psychologists carried out inherently governmental functions, such as acting as liaison between the CIA and foreign intelligence services, assessing the effectiveness of the interrogation program, and participating in the interrogation of detainees held in foreign government custody."[87]

Memoranda of Understanding May Improve Intelligence Sharing

Section 328 requires the USDHS/I&A to provide appropriate congressional committees with an assessment of the usefulness of a memoranda of understanding signed between federal, state, local, tribal, and territorial agencies to improve intelligence-sharing within and separate from the Joint Terrorism Task Force (JTTF). JTTFs are operated by the Federal Bureau of Investigation (FBI) and are based in 104 cities nationwide. Although they have been in existence since 1980[88] 71 have been created since 9/11. Their primarily purpose is to co-locate counterterrorism-related resources to enhance coordination and collaboration. According to the FBI, they consist of "small cells of highly trained, locally based, passionately committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies."[89] The FBI describes a JTTF's duties as follows: "chase down leads, gather evidence, make arrests, provide security for special events, conduct training, collect and share intelligence, and respond to threats and incidents at a moment's notice."[90]

---

[83] See CRS Report R43074, *Department of Defense's Use of Contractors to Support Military Operations: Background, Analysis, and Issues for Congress*, by Moshe Schwartz.

[84] See Simon Chesterman, "We Can't Spy … If We Can't Buy!: The Privatization of Intelligence and the Limits of Outsourcing 'Inherently' Governmental Functions," *European Journal of International Law*, vol. 19, no. 5 (2008): 1055-1074, at http://ejil.oxfordjournals.org/content/19/5/1055.full.pdf+html.

[85] See for example, U.S. Congress, Senate, Committee on Homeland Security and Government Affairs, Testimony by Timothy J. DiNapoli, Director of Acquisition and Sourcing Management for the Government Accountability Office, "Additional Actions Needed to Improve Reporting on and Planning for the Use of Contract Personnel," February 13, 2014, p. 3, at http://www.gao.gov/assets/670/660945.pdf; Vinh Nguyen, "Current Trends in Intelligence Outsourcing Affect Work Force Stability," *Signal OnLine*, December 2007, at http://www.afcea.org/content/?q=node/1440; and Brian Fung, "U.S. intelligence agencies can't justify why they use so many contractors," *Washington Post*, February 14, 2014, at http://www.washingtonpost.com/blogs/the-switch/wp/2014/02/14/u-s-intelligence-agencies-cant-justify-why-they-use-so-many-contractors/.

[86] U.S. Congress, Senate Select Committee on Intelligence, "Findings and Conclusions," *Committee Study of the Central Intelligence Agency's Detention and Interrogation Program*, 113th Congress, 2nd sess., December 3, 2014, p. 11 of 19, at http://www.intelligence.senate.gov/study2014/sscistudy1.pdf. Office of Management and Budget Circular A-76 defines an inherently governmental activity is "an activity that is so intimately related to the public interest as to mandate performance by government personnel." See CRS Report R42325, *Definitions of "Inherently Governmental Function" in Federal Procurement Law and Guidance*, by Kate M. Manuel.

[87] Ibid.

[88] The first was established in New York City according to the JTTF webpage at http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jttfs.

[89] Ibid.

[90] Ibid.

Section 328 was prompted by April 2013 bombing of the Boston Marathon.[91] A 2014 Report collectively issued by four IGs (the IGs for the DNI, CIA, DOJ and DHS) found that the FBI, CIA, DHS, and National Counterterrorism Center (NCTC) generally shared information, and followed procedures appropriately but improvements could be made. The report recommended (1) the FBI and DHS clarify JTTF alert procedures, and (2) the FBI consider establishing a procedure for sharing threat information with state and local partners more proactively and uniformly.[92] According to the intelligence committees' *Joint Explanatory Statement*, Section 328 "should help identify any obstacles to intelligence sharing between agencies, particularly any obstacles that might have impeded intelligence sharing in the wake of the April 2013 bombing of the Boston Marathon, and find improvements to existing intelligence sharing relationships."[93]

Counterterrorism Strategy

Section 330 directs the DNI to submit an unclassified comprehensive report[94] on the U.S. counterterrorism (CT) strategy to disrupt, dismantle, and defeat al-Qaeda and its affiliated or associated groups to the appropriate committees in Congress. The committee envisions an interagency approach, coordinated by the DNI, including the views of the Secretaries of State, Treasury, and Defense, the Attorney General, and the head of any other appropriate department or agency of the United States Government. Required elements of the report include an assessment of the strengthening or weakening of the groups in question from January 1, 2010 to the present.

The CT report required by Section 330 should complement a report required in the FY2008 Supplemental Appropriations Act (P.L. 110-252, §9304) that required a comprehensive global strategy to defeat al Qaeda and its affiliates—jointly submitted by the Secretaries of Defense, State and Homeland Security, in coordination with the Chairman of the Joint Chiefs of Staff and the DNI. The strategy submitted to Congress in 2008 was classified.[95]

FIX-ITT (Financial Exchange and Intelligence Integration)

The SSCI report accompanying the FY2015 legislation directs the DNI to provide performance assessments for a new initiative called "FIX-ITT" (Financial Exchange and Intelligence Integration). The committee "applauds" improvements made by the National Intelligence Manager for Threat Finance and Transnational Organized Crime in response to language in the

[91] On April 15, 2013, two pressure cooker bombs placed near the finish line of the Boston Marathon detonated within seconds of each other, killing three and injuring more than two hundred people. Law enforcement officials identified brothers Tamerlan and Dzhokhar Tsarnaev as primary suspects in the bombings. The Boston JTTF conducted an assessment of Tamerlan Tsarnaev to determine whether he posed a threat to national security and closed the assessment three months later having found no link or "nexus" to terrorism.

[92] "Unclassified Summary of Information Handling and Sharing Prior to the April 15, 2013 Boston Marathon Bombings, Prepared by the Inspectors General of the: Intelligence Community, Central Intelligence Agency, Department of Justice, and the Department of Homeland Security," 10 April 2014, at http://www.dni.gov/index.php/newsroom/reports-and-publications/204-reports-publications-2014/1042-unclassified-summary-of-information-handling-and-sharing-prior-to-the-april-15,-2013-boston-marathon-bombings.

[93] "Joint Explanatory Statement to Accompany the Intelligence Authorization Act for Fiscal Year 2015," Senate Debate, *Congressional Record*, daily edition, vol. 160, part 149 (December 9, 2014), p. S6465.

[94] The report is due within 180 days of the bill's passage on December 19, 2014 and may include a classified annex.

[95] Section 330 was a floor amendment offered by Representative Lloyd "Ted" Poe. The report it requires focuses on the relationships between "core" al Qaeda fighters and al Qaeda affiliates, as well the relationship between al Qaeda and the Islamic State. See Remarks by Rep. Ted Poe, "Amendment No. 7 to the Intelligence Authorization Act for Fiscal Years 2014 and 2015," *Congressional Record*, daily edition, vol. 160 (May 30, 2014), pp. H5051-H5052.

FY2014 legislation.[96] FIX-ITT is an ODNI integrating effort to bring all financial intelligence-related activities spread across various IC agencies together to better understand, map, and disrupt terrorist organizations, narco-trafficking networks, proliferation networks, organized crime, and other threats.[97]

[96] S.Rept. 113-120, p. 7.

[97] Ibid.

Appendix. Intelligence Community: In Brief

The congressional intelligence committees oversee the activities of the 17 components that currently comprise the U.S. Intelligence Community (IC). This confederation of agencies is led and managed on a daily basis by the Director of National Intelligence (DNI), with the assistance of the leadership team within the Office of the DNI (ODNI) to include the Director of Defense Intelligence (DDI).[98] The core mission of ODNI is to lead the IC in intelligence integration—synchronizing collection, analysis, and counterintelligence so that they are fused—effectively operating as one team.[99]

The task of leading the IC is particularly challenging because the IC is spread across six separate Cabinet departments and one independent agency within the executive branch. In fact, most intelligence offices/agencies have a dual mission: (1) support to national-level intelligence related activities managed by the DNI and (2) support to operational-level intelligence related activities managed by their parent department.

An overview of the IC components, leadership structure, and the overarching budget aggregations known as the National Intelligence Program (NIP) and the Military Intelligence Program (MIP) provides some of the basic terminology necessary to understanding intelligence legislation.

Components

The IC, as defined in 50 U.S. Code §401a (4), consists of the following components:

- The Office of the Director of National Intelligence.
- The Central Intelligence Agency.
- The National Security Agency.
- The Defense Intelligence Agency.
- The National Geospatial-Intelligence Agency.
- The National Reconnaissance Office.
- Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs.
- The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Federal Bureau of Investigation, and the Department of Energy.
- The Bureau of Intelligence and Research of the Department of State.
- The Office of Intelligence and Analysis of the Department of the Treasury.

[98] The Under Secretary of Defense for Intelligence or USD(I)) is called the Director of Defense Intelligence (DDI) when he wears his ODNI "hat."

[99] Office of the Director of National Intelligence, *U.S. National Intelligence: An Overview 2013*, pp 1-2, at http://www.dni.gov.

- The elements of the Department of Homeland Security concerned with the analysis of intelligence information, including the Office of Intelligence of the Coast Guard.
- Such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the IC.

Leadership Structure: the DNI and USD(I)

The Director of National Intelligence

The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), referred to as the Intelligence Reform Act or IRTPA, is widely considered to be the most significant legislation affecting the IC since the National Security Act of 1947. Most notably, the IRTPA established the position of DNI with more extensive authorities to coordinate the nation's intelligence effort than those formerly possessed by Directors of Central Intelligence (DCI).[100] The 9/11 Commission concluded that a central lesson that Congress and the executive branch drew from the 9/11 attacks was that there had been inadequate interagency coordination partially as a result of separate statutory missions and administrative barriers.[101] A number of reform measures were passed—a great many of which were designed to more closely and effectively coordinate the acquisition and dissemination of available intelligence. In terms of enhancing DNI's authorities over other IC leaders, the IRTPA focused particularly on personnel, tasking, acquisition, and budget.

The IRTPA divided the DCI's three major responsibilities between two new positions—the Director of the CIA (DCIA) and DNI—making the new DNI both community manager and principal advisor to the President (and leaving leadership of the CIA to its director). The DNI speaks for U.S. intelligence agencies, he briefs the President, has authority to develop the budget for the national intelligence effort and manage appropriations made by Congress, and, to some extent, can transfer personnel and funds from one agency to another. The ODNI, a staff of some 1,600 officials along with additional contract personnel, works to carry out the DNI's responsibilities. The President appoints the DNI with the advice and consent of the Senate.

The Office of the DNI

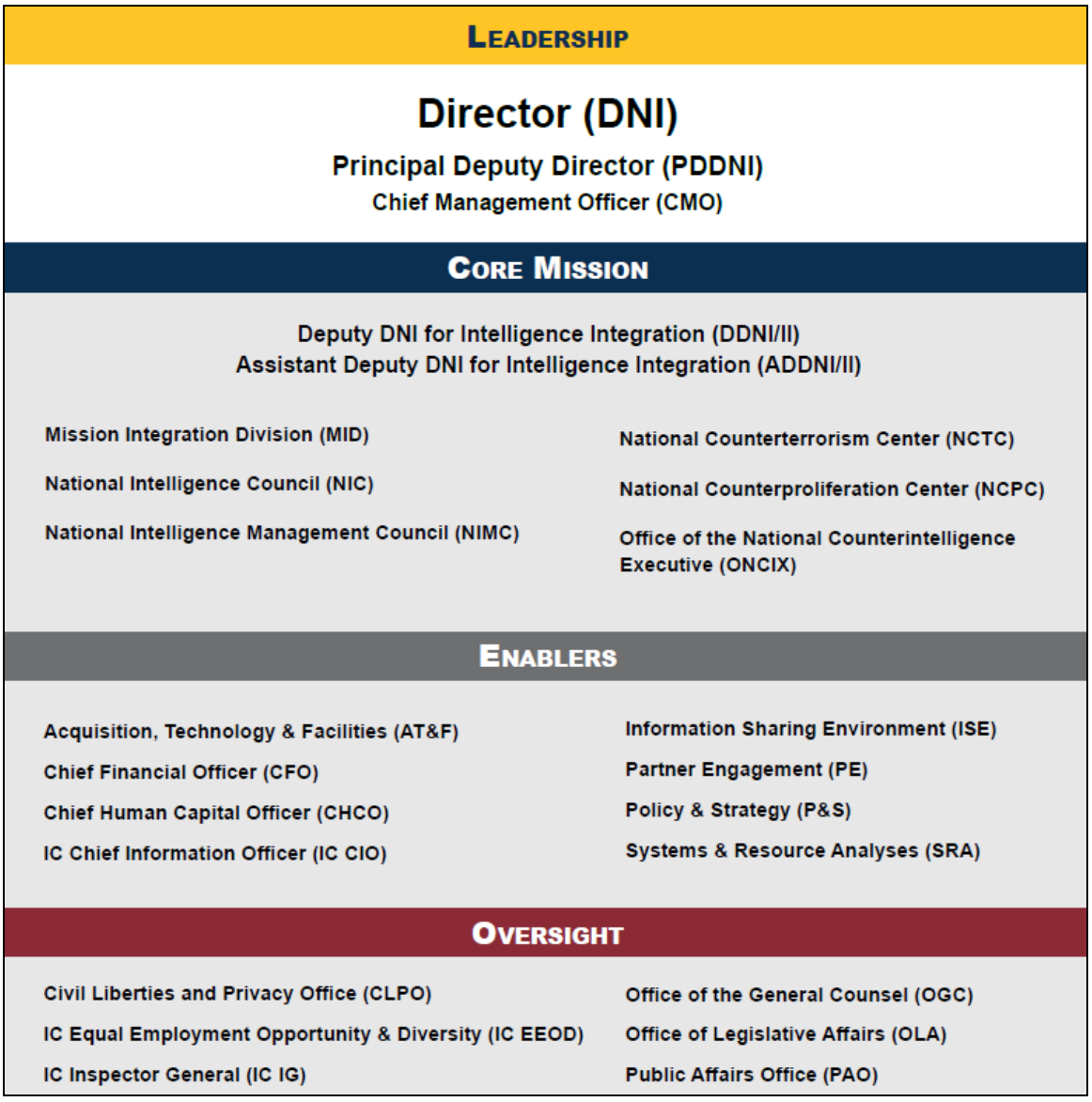
The ODNI carries out what it calls its "core" integration responsibilities with the help of several statutory components within the ODNI to include the National Counterterrorism Center (NCTC), the National Counterproliferation Center (NCPC), the National Counterintelligence Executive (NCIX), and the National Intelligence Council (NIC). **Figure A-1** illustrates the composition of the ODNI to include its core activities, "enabler," and "oversight" offices. Enabler offices focus on IC-wide concerns such as acquisition, budget, human capital, policy and strategy, and systems

[100] See Richard Best, "Leadership of the U.S. Intelligence Community: From DCI to DNI," *International Journal of Intelligence and Counterintelligence*, vol. 27, No. 2, (March, 2014): pp. 253-333, at http://www.tandfonline.com/.

[101] National Commission on Terrorist Attacks Upon the United States, Final Report, *The 9/11 Commission Report* (Washington D.C.: Government Printing Office, 2004), pp. 407-411; U.S. Congress, Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence, *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, 107th Congress, 2nd sess., S.Rept. 107-351/H.Rept. 107-792, December 2002, pp. 33-117; U.S. Commission on the Intelligence Capabilities of the U.S. Regarding Weapons of Mass Destruction, *Report to the President of the United States*, March 31, 2005, pp. 311-350.

and resource analysis. Oversight offices such as the General Counsel, Inspector General, and the Civil Liberties and Privacy Protection Office focus on IC-wide activities such as compliance with U.S. law, investigating allegations of fraud, waste, and abuse, and other issues.[102]

Figure A-1. Office of the Director of National Intelligence



Source: "Organization," at http://www.dni.gov.

The Under Secretary of Defense (Intelligence)/Director of Defense Intelligence

For reasons similar to those associated with the creation of the DNI, but by means of a different statute,[103] the position of Under Secretary of Defense (Intelligence) (USD(I)) was established in

[102] "Organization," under "About," ODNI webpage, at http://www.dni.gov.

[103] National Defense Authorization Act for FY2003 (P.L. 107-314,§901).

2003. The law divided the duties associated with the former Assistant Secretary of Defense for Command, Control, Communications and Intelligence, or ASD/C3I, into two positions—one position responsible for managing the intelligence portfolio, and one position responsible for supervising information systems across the DOD. The statute and DOD directives[104] gave the USD(I) significant authorities for the direction and control of intelligence agencies within the DOD.

In May 2007, the Secretary of Defense and DNI formally agreed in a Memorandum of Agreement (MOA) that the position would be "dual-hatted"—the incumbent acting as both the USD(I) within the Office of the Secretary of Defense (OSD) and Director of Defense Intelligence (DDI) within the ODNI in order to improve the integration of national and military intelligence.[105] According to the MOA, when acting as DDI, the incumbent reports directly to the DNI and serves as his principal advisor regarding defense intelligence matters. James Clapper, DDI at the time, said that the creation of the DDI position was a way to better "strengthen the relationship between the DNI and the DOD … (and) to facilitate staff interaction and promote synchronization."[106] The MOA did not alter the statutory responsibilities or authorities of either the Secretary of Defense or the DNI.

The Intelligence Budget

Many authorities and responsibilities associated with the DNI and USD(I) make reference to the national and military intelligence programs—known commonly as "the NIP and MIP." The terms NIP and MIP are fairly new, the former created by the IRTPA of 2004 §1074, and the latter created by DOD Directive in 2005.[107] Prior to the IRTPA, the NIP was known as the National Foreign Intelligence Program (NFIP). The MIP represents the merger of two programs formerly known as the Tactical Intelligence and Related Activities (TIARA) Program and the Joint Military Intelligence Program (JMIP).[108]

The DNI is most closely associated with the NIP and the USD(I) (in his role as DDI) is most closely associated with the MIP. Together, they oversee a number of interagency activities designed to facilitate the "seamless integration" of NIP and MIP intelligence efforts. Mutually beneficial programs, for example, may receive both NIP and MIP resources.[109] The NIP is associated with national-level intelligence. Some NIP programs fall within the DOD, some do not. Dr. Mark Lowenthal, former HPSCI Staff Director, describes the NIP as "programs that

[104] The primary directive is Department of Defense Directive 5132.01, "Under Secretary of Defense for Intelligence (USD(I))," November 23, 2005, pp. 2-7, posted on http://fas.org/irp/doddir/dod/d5143_01.pdf.

[105] Michael McConnell, DNI and Robert Gates, Secretary of Defense, "Memorandum of Agreement," May 2007, See DOD News Release No 637-07, May 24, 2007, "Under Secretary of Defense for Intelligence to be Dual-Hatted as Director of Defense Intelligence.," at http://www.defense.gov/Releases/Release.aspx?ReleaseID=10918.

[106] Ibid.

[107] Deputy Secretary of Defense Memorandum, "Establishment of the Military Intelligence Program," September 1, 2005. See also DOD Directive 5205.12, "Military Intelligence Program," November 14, 2008 (certified current through November 14, 2015), at http://www.dtic.mil/whs/directives/corres/pdf/520512_2008_certifiedcurrent.pdf. (DODD 5205.12).

[108] Elkins, p. 4-12.

[109] For information on specifics associated with NIP and MIP spending over time, see CRS Report R42061, *Intelligence Spending and Appropriations: Issues for Congress*, by Marshall C. Erwin and Amy Belasco.

either transcend the bounds of any one agency or are nondefense in nature."[110] 50 U.S.C. Section 401a (6) defines the term "National Intelligence Program" as

> [A]ll programs, projects, and activities of the IC, as well as any other programs of the IC designated jointly by the Director of National Intelligence and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.

Both defense and nondefense NIP funds are determined and controlled by the DNI, from budget development through execution. The NIP is often perceived as more complicated than the MIP because it is an aggregation of 14 programs that span the entire IC. NIP programs are capabilities based. Cryptology, for example, is a capability that spans several IC components. Each program within the NIP is headed by a Program Manager. These Program Managers exercise daily direct control over their NIP resources. The DNI acts as an intermediary in the budget process, between these managers, on the one side, and the President and Congress on the other.[111]

In contrast, "the MIP" is only those defense dollars associated with the operational and tactical-level activities of the military services. It all "belongs" to the Secretary of Defense.[112] It refers to service specific and DOD wide intelligence assets that are seen as "organic" to military units (e.g., deployable SIGINT personnel and equipment or tactical reconnaissance aircraft).[113] According to the MIP charter directive[114]

> The MIP consists of programs, projects, or activities that support the Secretary of Defense's intelligence, counterintelligence, and related intelligence responsibilities. This includes those intelligence and counterintelligence programs, projects, or activities that provide capabilities to meet warfighters' operational and tactical requirements more effectively. The term excludes capabilities associated with a weapons system whose primary mission is not intelligence.

The MIP label is a tool that allows the USD(I) to collectively manage all the dispersed funds associated with military intelligence support to the DOD "warfighters." As its Program Executive, the USD(I) as DDI

> [L]eads all Department of Defense actions involving the MIP, including issuing guidance, coordinating its development and execution, and chairing groups to address programmatic issues; and monitors the broader Battle Space Awareness Portfolio to achieve balance and synergies from its panoply of intelligence, surveillance and reconnaissance, command and control complementary capabilities.[115]

MIP Component Managers are "the individual(s) assigned by either this Directive, the Secretary of a Military Department, or the Commander, USSOCOM ... responsible for managing MIP

[110] Mark Lowenthal, *Intelligence: From Secrets to Policy*, 5th Edition, (Washington DC: Sage CQ Press, 2012), p. 52.

[111] Elkins, p. 4-5.

[112] See Robert Mirabello, "Budget and Resource Management," *Intelligencer: Journal of U.S. Intelligence Studies*, vol. 20, No. 2, (Fall/Winter 2013), p. 68, at http://www.afio.com/publications/MIRABELLO%20Pages%20from%20INTEL_FALLWINTER2013_Vol20_No2.pdf

[113] Elkins, p. 4-11.

[114] DOD Directive 5205.12 (3) (a).

[115] Mirabello, p. 68.

resources within his or her respective MIP Component in accordance with USD(I) guidance and policy."[116] The MIP components include the Office of the Secretary of Defense, Military Departments, U.S. Special Operations Command (USSOCOM), DIA, NGA, NRO, and the NSA/CSS.[117]

Table A-1 identifies four defense NIP programs: the Consolidated Cryptologic Program (CCP); General Defense Intelligence Program (GDIP); National Geospatial-Intelligence Program (NGP); and the National Reconnaissance Program (NRP). Intelligence authorization legislation passed in July 2014 merged the Foreign Counterintelligence Program (FCIP) into the GDIP program.[118]

Table A-1 identifies eight nondefense NIP programs: the Central Intelligence Agency Program (CIAP); the CIA's Retirement and Disability System[119] (CIARDS); the Office of the DNI[120] (CMA); and the intelligence entities within the departments of Energy, Homeland Security, Justice, State, and the Treasury.

Table A-1 identifies 10 MIP programs: the DIA MIP, NGA MIP, NRO MIP, NSA/CSS MIP, OSD MIP, USSOCOM MIP and service-specific MIP (Air Force MIP, Army MIP, Navy MIP, and Marine Corps MIP). Of the 9 Combatant Commands (COCOMs) only USSOCOM has its own budget.[121] The other COCOMs submit their budget requests through the military departments.

Table A-2 illustrates that six IC components have both MIP and NIP funding sources. The directors of DIA, NGA, NRO, and NSA are "dual-hatted" as Program Managers for their NIP funds and Component Managers for their MIP funds. Exactly what goes into what budgetary pot is not precise. Those decisions are guided by what is known as the NIP MIP "Rules of the Road."[122]

[116] DOD Directive 5205.12 (3) (c).

[117] DOD Directive 5205.12 (3) (b).

[118] P.L. 113-126, §314.

[119] CIARDS is a small fund that provides pension benefits to a selected group of the CIA's workforce—particularly those whose identities must be protected. Section 202 of the IAA for FY2014 amends the Central Intelligence Agency Retirement Act to expand the definition of "qualifying service" for purposes of designating CIA employees to participate in a retirement system based on a period of service abroad that is hazardous to life or health, or that is determined to be specialized because of security requirements, to include the service of CIA employees on detail to another agency. Without this provision, such qualifying service had to be performed within the CIA. (The provision made such qualifying detail service applicable to retired or deceased CIA officers.)

[120] The CMA, also referred to as the Intelligence Community Management Account or ICMA, is an account name that refers back to the IC Community Management Staff (CMS). The CMS supported the Director of Central Intelligence in his role as community manager. When the position of DNI was established, much of the old CMS became the new ODNI.

[121] Elkins, p. 6-6. For more on COCOMs, see CRS Report R42077, *The Unified Command Plan and Combatant Commands: Background and Issues for Congress*, by Andrew Feickert.

[122] Michael Vickers, "Defense Intelligence Resources," PowerPoint Presentation to Armed Forces Communications and Electronics Association (AFCEA), March 13, 2014, Slide 37.

Table A-1. National and Military Intelligence Programs (NIP and MIP)

National Intelligence Program	
Defense NIP:	
Consolidated Cryptologic Program (CCP)	Funds the signals intelligence (SIGINT) mission throughout the IC.
General Defense Intelligence Program (GDIP)	Funds wide range of national-level operations and intelligence infrastructure throughout the IC. The Foreign Counterintelligence Program (FCIP) merged with GDIP in IAA for FY2014.
National Geospatial-Intelligence Program (NGP)	Funds national-level geospatial-intelligence related activities throughout the IC.
National Reconnaissance Program (NRP)	Funds national-level satellite reconnaissance activities of the National Reconnaissance Office.
Nondefense NIP:	
Central Intelligence Agency Program (CIAP)	Funds complete range of CIA activities.
CIA Retirement and Disability Program (CIARDs)	Funds pension benefits to a selected group of the CIA's workforce—particularly those whose identities must be protected.
Community Management Account (CMA)	Funds the Office of the DNI.
NIP Programs associated with Departments of Energy, Homeland Security, Justice (within FBI and DEA), State and the Treasury	Funds intelligence integration/analysis offices in each department in support of the DNI and IC mission.
Military Intelligence Program	
DIA MIP	Tactical and joint general military intelligence and counter-intel activities of DIA, military services and Combat Commands not covered by GDIP.
NGA MIP	Tactical military geospatial intelligence related activities of the NGA, military services and Combat Commands not funded by the NGP.
NRO MIP	Tactical military air and space reconnaissance related activities of the NRO not funded by the NRP.
NSA/CSS MIP	Tactical military SIGINT related activities of the NSA and CSS not funded by the CCP.
OSD MIP	Office of the Secretary of Defense managed, defense-wide intelligence programs not covered by the GDIP or DIA MIP.
U.S. Special Operations Command (USSOCOM) MIP	Tactical military intelligence related activities and asset designed to support USSOCOM missions not funded by the NIP.
Service Specific MIP: **USAF, USA, USN, USMC**	Intelligence and related activities and assets of services "organic" to military combat units, or parts of joint/defense wide intelligence activities or programs in which they participate. These activities are generally within the scope of the Title 10 mission of the military departments to organize, train, and equip forces for combat application.

Source: Dan Elkins, *Managing Intelligence Resources,* 4th Edition, (Dewey, AZ: DWE Press, 2014): Chapter 4 pp 1-16.

Table A-2. Intelligence Community Components: NIP and MIP Funding Sources

Component	MIP Sources	NIP Sources
CIA		CIAP
COCOMs (Except SOCOM)	DIA MIP	GDIP, NGP, CCP
DIA	DIA MIP	GDIP
DOE, DOJ, DOS, Treasury		Department Specific NIP
NGA	NGA MIP	NGP
NRO	NRO MIP	NRP
NSA	NSA MIP	CCP
ODNI		CMA
USDI	OSD MIP	
USSOCOM	USSOCOM MIP	GDIP, NGP, CCP

Source: Dan Elkins, *Managing Intelligence Resources*, 4th Edition, (Dewey, AZ: DWE Press, 2014): Chapter 4 pp 1-16.

Author Contact Information

Anne Daugherty Miles
Analyst in Intelligence and National Security Policy
amiles@crs.loc.gov, 7-7739