Congressional Research Service
Informing the legislative debate since 1914

Intelligence Community Programs, Management, and Enduring Issues

Anne Daugherty Miles
Analyst in Intelligence and National Security Policy

November 8, 2016

Congressional Research Service
7-5700
www.crs.gov
R44681

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Congress's and the American public's ability to oversee and understand how intelligence dollars are spent is limited by the secrecy that surrounds the intelligence budget process. Yet, total spending on the Intelligence Community (IC) programs discussed in this report equates to approximately $70 billion dollars—roughly 10% of national defense spending. This report is designed to shed light on the IC budget—in terms of its programs, management, and enduring issues—using unclassified materials available in the public domain.

This report focuses those IC programs, grouped, for the most part, under two labels: (1) the National Intelligence Program (NIP), and (2) the Military Intelligence Program (MIP). Nevertheless, the combined NIP and MIP budgets do not encompass the total of U.S. intelligence-related spending. Intelligence-related programs that are not part of the IC include, for example, the large Office of Intelligence within the Department of Homeland Security's (DHS's) Immigration and Customs Enforcement (ICE) division. The ICE Office of Intelligence is not included in the IC because, theoretically, ICE activities primarily support the DHS mission to protect the homeland.

This report explains the management structure for the NIP and MIP to include their two separate budget processes and the roles of the Director of National Intelligence and the Under Secretary of Defense (Intelligence). The concluding section of this report considers the ability of the U.S. government to make the best use of its intelligence-related resources when: (1) total intelligence spending is impossible to calculate; (2) its management and oversight is completely decentralized; and (3) IC funding alone is largely divided into two categories (NIP and MIP)– managed within the executive branch separately, justified to Congress separately, and overseen by separate congressional committees.

The Appendices are designed, in a number of cases, to provide quick reference tables summarizing the more detailed information available in the body of the report.

- **Appendix A** provides a summary of intelligence disciplines.
- **Appendix B** provides very brief explanations of NIP and MIP subordinate programs.
- **Appendix C** examines two unique and relatively obscure NIP programs, the Central Intelligence Agency's Retirement and Disability System and the IC's Community Management Account.
- **Appendix D** briefly describes a program called the Homeland Security Intelligence Program (HSIP).
- **Appendix E** provides a summary table of management *hats*. (Senior executives are often referred to as dual-hatted, triple-hatted, and so on, when they are charged with a number of different roles and responsibilities and associated titles.)
- **Appendix F** provides a summary table comparing the IPPBE and PPBE budget systems.
- **Appendix G** provides a figure illustrating the ways in which the IPPBE and PPBE are integrated.
- **Appendix H** provides a list of IC-related acronyms, many of which are commonly used in this report.

For more on IC spending trends, see CRS Report R44381, *Intelligence Spending: In Brief*, by Anne Daugherty Miles.

Contents

Figures

Tables

Appendixes

Contacts

Introduction

Intelligence Community (IC) spending reveals much about the IC's structure, capabilities, missions, and customers.[1] Program budgets provide resources (money and manpower) considered necessary to accomplish IC goals, directives, duties and responsibilities defined by the U.S. Code and Executive Order (E.O.) 12333.[2] They fund *intelligence and intelligence-related activities* such as the collection, analysis and dissemination of information about any entity whose activities may pose a threat to the internal security of the United States, and "covert or clandestine activities affecting the relations of the United States with a foreign government, political group, party, military force, movement, or other association."[3]

IC program budgets fund the organizations charged with providing information of value to decision makers in the national security policy process. Such decision makers are thought of as *customers*—the President, National Security Council (NSC), heads of departments and agencies of the executive branch, the Chairman of the Joint Chiefs of Staff, senior military commanders, Members of Congress, and others as the Director of National Intelligence (DNI) determines appropriate. The IC tends to group its customers into two categories: (1) national/ strategic-level and (2) military/tactical-level.

Based on the distinction between national and operational/tactical, IC spending is usually understood as the combination of (1) the National Intelligence Program (NIP), which covers the programs, projects, and activities of the intelligence community oriented towards the strategic needs of decision makers, and (2) the Military Intelligence Program (MIP), which funds defense intelligence activity intended to support tactical military operations and priorities. In Fiscal Year (FY) 2016, the aggregate amount (base and supplemental) appropriated to these two programs totaled $70.7 billion (NIP $53B, MIP $17.7).[4]

National/strategic- and military/tactical-intelligence differ primarily in where they fall along a continuum stretching from support to the highest levels of the policy making process at one end to conduct of troop-level military operations at the other end. They may also vary in terms of scope and detail.[5] National-level *strategic intelligence* is associated with grand-scale (big picture)

[1] See **Table 2** and **Figure 1** of this report for the current composition and structure of the IC.

[2] IC-related provisions can be found throughout the U.S. Code, but most particularly in Titles 5, 6, 10, 22, 42 and 50. U.S. Code provides the legal foundation for E.O. 12333, *United States Intelligence Activities*—issued on December 4, 1981 and amended by E.O. 13284 (2003), E.O. 13355 (2004) and E.O. 13470 (2008).

[3] For a complete definition, see U.S. Congress, Rules of the House of Representatives, 114th Cong., 1st sess., January 6, 2015, Rule X (11) (j) (1). The definition is included in the Rule pertaining to the Permanent Select Committee on Intelligence. The definition was first adopted in by the House in its "Resolution to amend the Rules of the House of Representatives and establish a Permanent Select Committee on Intelligence," H.Res. 658, 95th Cong., 1st sess., *Congressional Record—House*, July 14, 1977, pp. 22932-22934. A similar definition is included in Senate Resolution 400 §14 establishing the Senate Select Committee on Intelligence.

[4] See Office of the DNI, "DNI Releases Budget Figure for 2016 National Intelligence Program," *news release* no. 20-16, October 28, 2016, at https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1443-dni-releases-budget-figure-for-2016-national-intelligence-program; and Department of Defense, "Department of Defense Releases Budget Figure for 2016 Military Intelligence Program (MIP)," Release No: NR-386-16, at http://www.defense.gov/News/News-Releases/News-Release-View/Article/990166/department-of-defense-releases-budget-figure-for-2016-military-intelligence-pro.

[5] For example, strategic-level intelligence might lead to an objective such as defeating the enemy in Afghanistan. Operations-level intelligence might focus on the information necessary to seize a certain city in Afghanistan, and tactical-level intelligence might focus on the information necessary to seize a bridge leading into the city.

policy objectives.[6] *Operational intelligence* narrows its focus to foreign military or military-related situations or activities within theaters or operational areas.[7] *Tactical intelligence* is very detailed intelligence required for planning and conducting military operations at the troop level.[8] To help clarify these three levels of intelligence, **Table 1** provides an overview of the intelligence associated with what the Department of Defense (DOD) refers to as *levels of war*.[9]

Table 1. Levels of Intelligence

Strategic

Senior Military and Civilian Leaders; Combatant Commanders

- *Assist in developing national strategy and policy.*
- *Monitor the international or global situation.*
- *Assist in developing military plans.*
- *Assist in determining major weapon systems and force structure requirements.*
- *Support the conduct of strategic operations.*

Operational

Combatant and Subordinate Joint Force Commanders and Component Commanders

- *Focus on military capabilities and intentions of enemies and adversaries.*
- *Analyze the operational environment.*
- *Identify adversary centers of gravity and critical vulnerabilities.*
- *Monitor events in the joint force commander's area of interest.*
- *Support the planning and conduct of joint campaigns.*

Tactical

Commanders

- *Support planning and the execution of battles, engagements, and other joint force activities.*
- *Provide commanders with information on imminent threats to their forces and changes in the operational environment.*
- *Provide commanders with obstacle intelligence.*

Source: Joint Publication 2-0, *Joint Intelligence*, Figure I-7, p. I-24.

[6] "Strategic Intelligence" can be defined as any "intelligence that is required for the formulation of strategy, policy, and military plans and operations" by decisionmakers at the theater-, national-, and international-levels. Office of CI, Defense and HUMINT Center, *Counterintelligence Glossary*, Defense Intelligence Agency, May 2, 2011, at https://www.ncsc.gov/publications/ci_references/docs/CI_Glossary.pdf. See also Joint Publication 2-0, *Joint Intelligence*, October 22, 2013, p. I-23.

[7] "Operational intelligence" can be defined as "intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or operational areas." Office of CI, Defense and HUMINT Center, *Counterintelligence Glossary*, Defense Intelligence Agency, May 2, 2011. See also Joint Publication 2-0, *Joint Intelligence*, October 22, 2013, pp. I-24 to I-25.

[8] "Tactical Intelligence" can be defined as "information about the enemy that is designed to help locate the enemy and decide which tactics, units, and weapons will most likely contribute to victory in an assigned area." Office of CI, Defense and HUMINT Center, *Counterintelligence Glossary*, DIA, May 2, 2011. See also Joint Publication 2-0, *Joint Intelligence*, October 22, 2013, p. I-25.

[9] See for example, Joint Publication 3-0, *Joint Operations*, August 11, 2011, p. I-12. The DOD's Joint Publication series, particularly those on Joint Intelligence (2-0 and 2-01) are useful references for information on the entire IC—not just DOD intelligence-related activities. DOD doctrine has the added advantage of being easily available online at http://dtic.mil/doctrine/new_pubs/jointpub_operations.htm. The IC has no comparable documents available in the public domain.

Organizations such as the Central Intelligence Agency (CIA) integrate intelligence from all sources into *national intelligence* in support of the policy process while organizations such as the Defense Intelligence Agency (DIA) are more focused on integrating service-specific intelligence into *defense intelligence* for the warfighter.[10] Furthermore, joint intelligence elements exist within the DOD to provide a common, coordinated picture for military commanders by fusing national and theater intelligence information into *all-source* assessments and estimates.

Background on the National and Military Intelligence Programs

Origins of an intelligence budget, separate and distinct from the defense budget, date back to the Nixon Administration.[11] Early efforts to consolidate intelligence-related funds were energized by calls to improve oversight and accountability of the IC.[12] Three programs formed the basis for what we now call the National Intelligence Program (NIP) and Military Intelligence Program (MIP): the National Foreign Intelligence Program, Tactical Intelligence and Related Activities Program, and the Joint Military Intelligence Program.[13]

National Foreign Intelligence Program (NFIP)

The NFIP was a consolidation of the CIA budget with portions of the defense budget associated with national-level intelligence activities such as cryptologic and reconnaissance programs.[14] The NFIP was originally managed by the Director of Central Intelligence (DCI), in consultation with the Secretary of Defense, and overseen by the NSC.[15] The term *NIP* was created by the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 (P.L. 108-458 §1074). The IRTPA deleted *Foreign* from NFIP and also created the position of DNI. The DNI position will be discussed in greater detail later in the report.

Tactical Intelligence and Related Activities (TIARA)

Funding for military specific tactical-level or operational intelligence activities was not included in the NFIP. It was referred to as TIARA and was managed separately by the Secretary of Defense. TIARA referred to the intelligence activities *of a single service* that were considered "organic" (meaning "to belong to") military units.

[10] Defense intelligence can be defined as intelligence "relating to capabilities, intentions, and activities of foreign powers, organizations, or persons, including any foreign military or military-related situation or activity which is significant to Defense policy-making or the planning and conduct of military operations and activities." See "defense intelligence" in Office of CI, Defense and HUMINT Center, *Counterintelligence Glossary*, Defense Intelligence Agency, May 2, 2011.

[11] It was known at that time as the *Consolidated Intelligence Budget*. See Tyrus Fain, *The Intelligence Community: History, Organization, and Issues*, Public Document Series, (New York: R.R. Bowker, 1977), pp. 202-203.

[12] Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), p. 4-3.There were a number of reforms, some directed at reforms of the entire congressional budget process and other directed at improved oversight of the IC.

[13] NIP and MIP rhyme with the words like "hip" or "dip."

[14] See E.O. 11905 (1976), E.O 12036 (1978), E.O. 12333 (1981).

[15] Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), p. 4-3.

Joint Military Intelligence Program (JMIP)

In 1994, a new budget category, known as the JMIP, was created by the Secretary of Defense for joint, defense-wide intelligence programs.[16] DOD Directive 5205.9 describes the intended purpose of the JMIP this way:

> The JMIP shall improve the effectiveness of DoD intelligence activities when those activities involve resources from more than one DoD Component; when users of the intelligence data are from more than one DoD Component; and/or when centralized planning, management, coordination, or oversight will contribute to the effectiveness of the effort.[17]

The term *MIP* originated in 2005 when Acting Deputy Secretary of Defense Gordon England signed a DOD memorandum merging TIARA and JMIP.[18] DOD Directive 5205.12 established policies and assigned responsibilities, to include the Under Secretary of Defense (Intelligence)'s (USD(I)'s) role as program executive of the MIP, acting on behalf of the Secretary of Defense.[19]

NIP and MIP *Rules of the Road*

The line between NIP and MIP can be difficult to draw. Many intelligence-related activities serve both national-level and tactical-level purposes. For example, the same intelligence about the location of a building and its occupants might be used to inform strategic-level discussions about a terrorist group's intentions or plans as well as to develop the tactics to blow it up or capture the inhabitants at the operational/tactical-level. NIP and MIP labels are also not definitive. A program under the NIP one year may be categorized MIP the next. Much depends on who is managing the process and how the program is justified. NIP and MIP labels depend on answers to the following kinds of questions:

- What is the program designed to do?
- What need does it satisfy?
- Who will derive the greatest benefit?
- Is the customer national- or tactical-level?
- What label makes the most sense from a logic standpoint?
- Who needs to do what to get the mission accomplished?
- How urgent is the need?

---

[16] Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), p. 4-13. JMIP was created via a Secretary of Defense Memorandum, "Joint Military Intelligence Program (JMIP)," May 14, 1994.

[17] DOD Directive 5205.9 "Joint Military Intelligence Program (JMIP)," April 7, 1995, at http://biotech.law.lsu.edu/blaw/dodd/corres/html2/d52059x.htm. According to the directive, the JMIP was initially comprised of the following programs: the Defense Cryptologic Program; Defense Imagery Program; Defense Mapping, Charting, and Geodesy Program; Defense General Intelligence and Applications Program; Defense Airborne Reconnaissance Program; Defense Intelligence Counterdrug Program; DIA's Tactical Program; Defense Space Reconnaissance Program; and Defense Intelligence Special Technology Program.

[18] Janet McDonnell, "The Office of the Under Secretary of Defense for Intelligence: The First 10 Years," *Studies in Intelligence*, vol. 58, no. 1 (Extracts, March 2014): 9-16, p. 13. McDonnell cites the memorandum creating the MIP as follows: Acting Deputy Secretary of Defense Gordon England, Memorandum to the Secretaries of Military Departments et al., Subj: Establishment of the Military Intelligence Program, September 1, 2005.

[19] DOD Directive 5205.12, "Military Intelligence Program," November 14, 2008 (online version certified current through November 14, 2015), at http://www.dtic.mil/whs/directives/corres/pdf/520512_2008_certifiedcurrent.pdf.

In the end, NIP and MIP designations are simply ways to manage resources. Anything that is not NIP funded is typically MIP funded. The IC currently uses what it colloquially calls the NIP MIP *Rules of the Road* to loosely define what falls into either the NIP or MIP.[20]

According to these *Rules of the Road*, an IC program, project, or activity is primarily NIP if it:

- supports more than one department or agency;
- provides a service of common concern for the IC;
- supports Secure Compartmented Information Communications (SCI) across the IC;
- supports a capability at intelligence agencies and subordinate centers; and
- supports Information Technology (IT) equipment at Combatant Commands.

An IC program, project, or activity is primarily MIP if it:

- supports military operations;
- addresses a unique DOD requirement; and
- supports a capability at Combatant Command headquarters and below.

Caveats to these rules include the following:

- NIP and MIP may add funds to sustain, enhance or increase the capacity and/or capability of the other's systems;
- NIP capabilities may be temporarily provided to Operating Forces; and
- NIP and MIP can share program cost based on a DNI and Secretary of Defense determination that the activity is mutually beneficial.[21]

Topline Numbers Only

While many details associated with funding for IC programs are classified, much can be learned from publicly available documents. The information in this report is based entirely on unclassified, publicly available sources.[22] Disclosure of details associated with the intelligence budget has been debated for many years, with proponents of more disclosure arguing for more accountability.[23] Meanwhile, IC leadership argues that disclosure could cause damage to national security.[24]

At present, only the NIP and MIP aggregate budget numbers are publicly available. The appropriations for FY2017 were $53 billion and $17.7 billion respectively.[25] Together, the $70.7B

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

[21] To see a chart depicting NIP and MIP funding, see Figure F-1 in Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, January 5, 2012, p. F-2.

[22] The most comprehensive source is Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), available by contacting DWE Press at dwelkins2@cs.com.

[23] See for example, Cynthia Lummis and Peter Welch, "Intelligence Budget Should Not Be Secret," *CNN*, April 21, 2014, at http://www.cnn.com/2014/04/21/opinion/lummis-welch-intelligence-budget/.

[24] See for example, "Declaration of George Tenet," *Aftergood v. CIA*, U.S. District Court for the District of Columbia, Civ. No. 98-2107, April, 1999, at http://fas.org/sgp/foia/tenet499.html.

[25] See Office of the DNI, "DNI Releases Budget Figure for 2016 National Intelligence Program," *news release* no. 20-16, October 28, 2016, at https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1443-dni-releases-budget-figure-for-2016-national-intelligence-program; and Department of Defense, "Department of Defense (continued...)

IC budget is approximately 11% of the national defense budget.[26] CRS Report R44381, *Intelligence Spending: In Brief*, by Anne Daugherty Miles, contains tables comparing NIP and MIP spending to national defense spending from FY2007 to FY2017.[27]

There is some confusion over whether the NIP or MIP (or both) comprise what is popularly known as the *black budget*.[28] The term *black budget* has no official status in policy or regulation. In using the term, most observers are making a generic reference to all programs (including intelligence programs) for which funding figures are classified at some level. Likewise, there is no authoritative, unclassified, aggregate budget total for the *black budget*—whether one counts all or a portion of the NIP, MIP or non-intelligence DOD classified program budgets.

(...continued)

Releases Budget Figure for 2016 Military Intelligence Program (MIP)," Release No: NR-386-16, at http://www.defense.gov/News/News-Releases/News-Release-View/Article/990166/department-of-defense-releases-budget-figure-for-2016-military-intelligence-pro.

[26] 11% is based on a national defense budget of $619B. See Office of Management and Budget, *Historical Tables*, Table 5.1, "Budget Authority by Function and Subfunction: 1976-2020," Function 50 "National Defense," for FY2017.

[27] For more on the national defense budget see CRS Report R44454, *Defense: FY2017 Budget Request, Authorization, and Appropriations*, by Pat Towell and Lynn M. Williams.

[28] See for example, Dana Priest, et al, "The Black Budget," *Washington Post*, August 29, 2013.

The Intelligence Community (IC): Definition and Disciplines

Table 2. Statutory U.S. Intelligence Community Elements (2016)

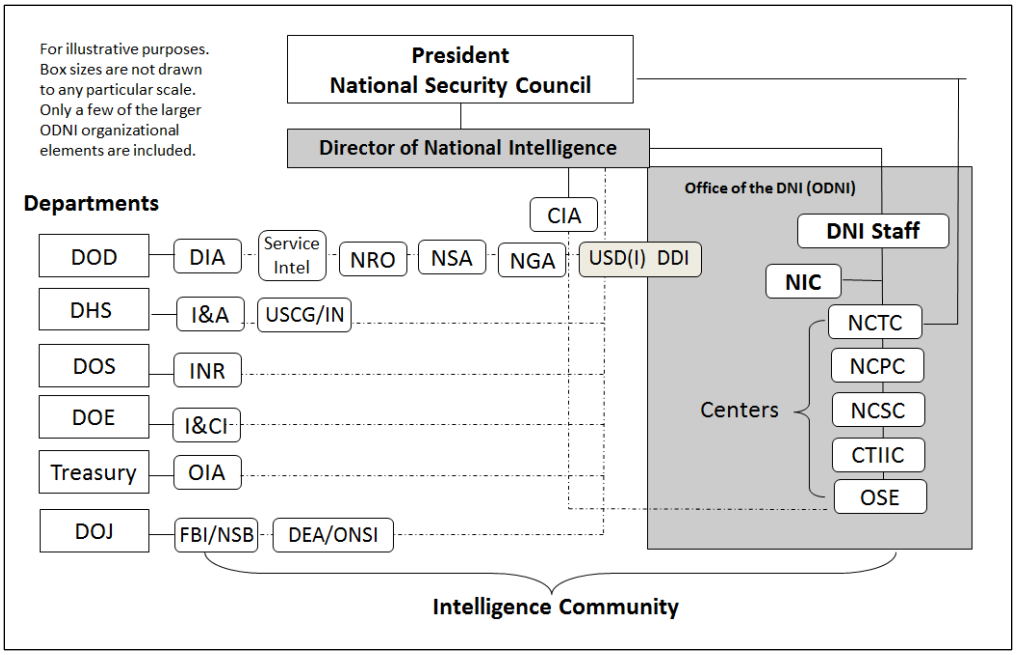
8 Department of Defense (DOD) Elements:
1. Defense Intelligence Agency (DIA)
2. National Geospatial-Intelligence Agency (NGA)
3. National Reconnaissance Office (NRO)
4. National Security Agency (NSA)
Intelligence elements of the military services:
5. U.S. Air Force Intelligence (USAF/IN)
6. U.S. Army Intelligence (USA/IN)
7. U.S. Marine Corps Intelligence (USMC/IN)
8. U.S. Navy Intelligence (USN/IN)
9 Non-DOD Elements:
1. Office of the Director of National Intelligence (ODNI)
2. Central Intelligence Agency (CIA)
Department of Energy (DOE) intelligence element:
3. Office of Intelligence and Counter-Intelligence (I&CI)
Department to Homeland Security (DHS) intelligence elements:
4. Office of Intelligence and Analysis (OIA)
5. U.S. Coast Guard Intelligence (USCG/IN)
Department of Justice (DOJ) intelligence elements:
6. Drug Enforcement Agency's Office of National Security Intelligence (DEA/ONSI)
7. Federal Bureau of Investigation's National Security Branch (FBI/NSB)
Department of State (DOS) intelligence element:
8. Bureau of Intelligence and Research (INR)
Department of Treasury (Treasury) intelligence element:
9. Office of Intelligence and Analysis (OIA)

Source: 50 U.S.C. §3003

While intelligence-related organizations span the federal, state and local governments, this report focuses only on programs associated with the agencies considered part of the IC. The IC is a confederation of 17 disparate organizations that all carry out some intelligence function related to national security.[29] The National Security Act of 1947 (P.L. 80-253) created the framework for the IC. U.S. Code, primarily Titles 10 and 50 in combination, regulate its activities and funding and provide the legal foundation for E.O. 12333.

[29] As early as 1956, Dillon Anderson, then-Special Assistant to the President for National Security Affairs (1955-1956) referred to the "Intelligence Community" in his article "The President and National Security," in *The Atlantic Monthly* (January 1956): 42-46, p. 44. There are also several references to an "intelligence community" in the *Executive Sessions of the Senate Foreign Relations Committee*, Volume VIII, 84th Cong, 2nd sess., 1956 (WDC: GPO, 1978).

Figure 1. U.S. Intelligence Community Structure (2016)



Source: CRS

Notes: For IC element acronyms see Figure 1. Within the ODNI: NIC—National Intelligence Council, NCTC—National Counterterrorism Center, NCPC—National Counterproliferation Center, NCSC—National Counterintelligence and Security Center, CTIIC—Cyber Threat Intelligence Integration Center, OSE—Open Source Enterprise. For more on the ODNI see **Appendix C**.

The current roles and responsibilities of the DNI are based on provisions in the IRTPA of 2004 (P.L. 108-458).[30] The IRTPA charges the DNI with three main roles: (1) head of the IC, (2) principal intelligence advisor to the President, and (3) director of the NIP. **Figure 1** illustrates that with the exception of the CIA and Office of the DNI (ODNI), IC components are housed in one of six separate departments headed by cabinet secretaries. Most IC elements have a dual mission: (1) support to *national-level* intelligence activities, and (2) support to *operational-level* intelligence activities associated with its host department.

Each intelligence agency is associated with one *or more* intelligence collection disciplines. Several NIP programs focus as much on funding a specific intelligence disciplines (such as signals intelligence) as they do on funding specific agencies. Collection disciplines are often referred to by IC professionals and commentators as *INTs* because the acronyms for each source end with *INT*. The five main INTs include:

1. Human Intelligence (HUMINT),
2. Open Source Intelligence (OSINT),
3. Signals Intelligence (SIGINT),[31]
4. Geospatial Intelligence (GEOINT),[32] and

[30] The IRTPA also created the Office of the DNI (ODNI). P.L. 108-458, Title I, "Reform of the Intelligence Community," Subtitle A, "Establishment of Director of National Intelligence," §1011(a), "Reorganization and Improvement of Management of Intelligence Community." Prior to the IRTPA, the DCI served as both IC manager and Director of the CIA (DCIA). The IRTPA prohibited anyone from serving simultaneously as DNI and DCIA.

[31] An INT such as Communications Intelligence (COMINT) is considered a subset of SIGINT.

5. Measurement and Signature Intelligence (MASINT).

Table A-1 (Appendix A) describes the major INTs and their subset INTs, and provides examples of each.

Each IC agency brings its own special expertise to what is commonly referred to as the *Intelligence Enterprise*. For example,[33]

- CIA is the largest producer of all-source, national security intelligence primarily for the President, Congress, and senior policy-makers in the NSC. It manages clandestine HUMINT collection, covert operations, and OSINT across the IC.
- DIA collects, produces and disseminates a full range of basic, current, warning, and estimative intelligence that supports geographic commanders and operational forces, the Military Departments, and national policymakers. It also manages MASINT for the IC.[34]
- NGA acquires imagery, geospatial information, and other products to produce and disseminate GEOINT in all forms to policy makers, military commanders and to first responders, and to mariners and pilots for safety of navigation.[35]
- NRO builds and operates a fleet of satellites and ground stations whose main purpose is collecting SIGINT and GEOINT.[36]
- NSA specializes in cryptology, collecting SIGINT, and information assurance (secure data) activities, to include cyber-related operations.[37]

(...continued)

[32] Imagery Intelligence (IMINT) is a subset of GEOINT.

[33] The descriptions are not comprehensive; rather are representative of the general missions of each entity. For more a more complete description of the mission of each IC element, see Executive Order 12333, "United States Intelligence Activities," December 4, 1981 (as amended by EOs 13284, 13355 and 13470). See also, Intelligence Community Information Sharing Executive, *U.S. National Intelligence—An Overview 2013*, at https://www.dni.gov/index.php/newsroom/reports-and-publications/193-reports-publications-2013/835-u-s-national-intelligence-an-overview-2013-sponsored-by-the-intelligence-community-information-sharing-executive. See also Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, January 5, 2012.

[34] The DIA was formed in 1961 to provide a national focus for Air Force, Army, Navy, and Marine Corps intelligence and to reduce redundancy. Prior to DIA's creation, each armed service collected, analyzed and disseminated its own intelligence and provided separate estimates to the Secretary of Defense.

[35] When originally created, NGA was named the National Imagery and Mapping Agency (NIMA) and represented the consolidation of eight agencies or programs associated with either mapping or imagery. For more on the creation of NIMA, see Anne Daugherty Miles, *The Creation of the National Imagery and Mapping Agency: Congress's Role as Overseer*, Occasional Paper Number Nine (Washington, DC: Joint Military Intelligence College, 2002), at http://ni-u.edu/ni_press/pdf/The_Creation_of_the_National_imagery_and_Mapping_Agency.pdf. The NDAA for FY 2004 (P.L. 108-136 §921) changed the name of the NIMA to NGA. The name change was intended to introduce the term "geospatial intelligence" to better describe the unified activities of NGA related to the "analysis and visual representation of characteristics of the earth and activity on its surface." See S.Rept. 108-466 accompanying the NDAA for FY 2004, S. 1050, 108th Cong., 1st sess., p. 349.

[36] The NRO's existence was classified from 1961 until 1992. The official "Declassification of the Fact of Existence of the National Reconnaissance Office" took place on September 18, 1992, in a "Memorandum for Correspondents" released by the Office of the Secretary of Defense. See Jeffrey Richelson, "Out of the Black: The Declassification of the NRO," *National Security Archive Electronic Briefing Book No. 257*, September 18, 2008, at http://nsarchive.gwu.edu/NSAEBB/NSAEBB257/.

[37] Cryptology is the science (and art) concerning the principles, means and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form. See Jan Goldman, *Words of Intelligence: A Dictionary* (Lanham, MD: Scarecrow Press, 2006).

- Military service elements collect much of the intelligence associated with the *INTs* discussed above, and provide the service-specific expertise necessary for support to military operations.
- Non-DOD department elements such as DHS/OIA, DEA/ONSI, State/INR and DOE/I&CI contribute energy, homeland security, law enforcement, drug, diplomatic, and financial intelligence (primarily HUMINT and OSINT) necessary for all-source intelligence analysis and warning. [38]

National Intelligence Program (NIP)[39]

Both 50 U.S.C. §3003(6) and E.O. 12333 define the NIP as *including* "all programs, projects, and activities of the Intelligence Community, as well as any other programs of the Intelligence Community designated jointly by the Director [DNI] and the head of a United States department or agency or by the President," but *excluding*, "programs, projects, and activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by U.S. Armed Forces."

In reality, the NIP budget is an aggregation of a number of subordinate programs that are often subdivided into defense NIP and nondefense NIP because they are managed separately. These subordinate programs fund the activities of the IC elements. They often assist the DNI in his or her efforts to integrate the IC because a number of the subordinate programs are explicitly designed to coordinate intelligence agencies, budget requirements and mission execution across agencies. Electronic communications and connectivity between intelligence agencies (and their customers) is a good example of the integrating function associated with many NIP-related funds because the secure email network connects all IC employees to one another.[40]

NIP programs compete for resources within the IC, not within the larger department budgets. According to one account, this can be a "tremendous advantage to all the departmental intelligence organizations" because NIP resources are protected from use by other organizations within their respective agencies.[41] This special protection is informally known as the NIP *fence*.[42] The existence of this special protection is a long-standing practice. According to a House Permanent Select Committee Staff Study, the NIP fence was already a "well established tradition" in 1981:

> DoD internal guidance (Carlucci memorandum of April 17, 1981) stated the policy that NFIP 'resources are "fenced" and they are not to be increased, decreased, or transferred at any point in the fiscal cycle unless such action has been officially coordinated with the DCI.' This policy is deemed to continue and has never been seriously challenged. Thus,

[38] For more on the agencies within the IC, see ODNI, *U.S. National Intelligence: An Overview 2011*, at https://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf.

[39] **Table B-1** (**Appendix B**) summarizes the NIP and MIP programs discussed in detail in the next two sections.

[40] Kristin Quinn, "Journey to Integration," *Trajectory Magazine*, U.S. Geospatial Intelligence Foundation, Issue 3, 2013, at http://trajectorymagazine.com/web-exclusives/item/1553-journey-to-integration.html. Quinn quotes Robert Cardillo, then-Deputy DNI for Intelligence Integration (DDII) and currently Director of NGA: "Information technology is a great example of the opportunity for reducing, opening, eliminating, connecting physically the community.… I spend most of my days removing inhibitors and setting conditions to enable it to happen."

[41] Gerald Hopple and Bruce Watson, *The Military Intelligence Community* (Boulder, Co: Westview Press, 1986), p. 18.

[42] For a more detailed discussion of the NIP *fence*, particularly as it affects defense NIP programs, see Dan Elkins, *Managing Intelligence Resources*, (Dewey, AZ: DWE Press, 2014), pp. 4-16 to 4-17.

> the concept of the NFIP as a fenced program is well-established and accepted in the Executive Branch.[43]

In contrast, MIP funds are said to be *protected* but not fenced. The MIP's protected status is discussed more fully below in the "Military Intelligence Program (MIP)" section. The resources (manpower and dollars) associated with the NIP's subordinate programs are managed by *Program Managers*.[44] Program Managers are discussed later in the "Program and Component Managers" section.

Defense NIP

Defense NIP is focused on strategic-level intelligence for military-related activities.[45] Defense NIP programs are primarily associated with four IC agencies—NSA, DIA, NGA and NRO—and their respective capabilities—cryptologic, defense, geospatial, and reconnaissance intelligence. These four capabilities form the basis for five defense NIP subordinate programs known as the Consolidated Crytologic Program (CCP), General Defense Intelligence Program (GDIP), National Geospatial-Intelligence Program (NGP), National Reconnaissance Program (NRP), and the Specialized Reconnaissance Program (SRP). Together, these programs comprise roughly 60% of the total NIP budget.[46]

Consolidated Cryptologic Program (CCP)

The CCP is managed by the Director of the NSA, who simultaneously acts as Commander, U.S. Cyber Command (USCYBERCOM) and Chief, Central Security Service (CHCSS).[47] Funding for the SIGINT mission and information assurance (IA) activities across the IC are provided through the CCP. NSA's SIGINT mission is specifically limited by law to gathering information about international terrorists and foreign powers, organizations, or persons in response to formal requirements levied by IC customers with a *need to know*. SIGINT collection activities are widespread among IC elements. For example, the U.S. Coast Guard has a SIGINT collection entity as do each of the military services.

In its IA role, NSA protects U.S. intelligence and national security communications and data storage systems for a number of government agencies, including the State Department, DOD, the CIA, and the FBI. This role includes development of secure data and voice transmission links on satellite systems such as the Defense Satellite Communications System.[48] Members of the defense cryptologic community receive additional funds from the Information Systems Security Program (ISSP) for information assurance activities.[49]

---

[43] U.S. Congress, House, Permanent Select Committee, *IC21: The Intelligence Community in the 21st Century*, 104th Cong., 2nd sess. (Washington D.C.: GPO, 1996), p. 77, at https://www.hsdl.org/?view&did=439040.

[44] For more, see "Program and Component Managers" section below, and **Table E-1**, Appendix E.

[45] Office of CI, Defense and HUMINT Center, *Counterintelligence Glossary*, Defense Intelligence Agency, May 2, 2011.

[46] Jeffrey Richelson, *The U.S. Intelligence Community*, 7th ed. (Boulder, CO: Westview Press, 2016), p. 506.

[47] The CSS was established in 1972 to promote partnership between the NSA and the armed services' cryptologic entities, known as the Service Cryptologic Components (SCCs). The CSS represents a unified DOD cryptologic effort focusing on cryptologic support for military-related activities. See also, DOD Directive 5100.20, "National Security Agency/Central Security Service (NSA/CSS)," January 26, 2010.

[48] Jeffrey Richelson, *The U.S. Intelligence Community*, 7th ed. (Boulder, CO: Westview Press, 2016), p. 34. According to Richelson, the NSA also develops the codes used by the President to release nuclear weapons.

[49] For more on ISSP, see Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), p. 4-6.

General Defense Intelligence Program (GDIP)[50]

The GDIP is a catch-all program managed by the Director of DIA that supports the wide range of national-level defense intelligence activities that do not fall within the other more specific CCP, NGP, NRP and SRP budgets. It includes the collection, analysis, production and dissemination of the intelligence associated with DIA organizations[51] and Service intelligence centers.[52]

GDIP-funded collection activities include:

- defense HUMINT, particularly through the Defense Attaché System;
- MASINT against geographic targets, foreign forces, and foreign weapon systems;
- medical intelligence—intelligence that focuses on "worldwide health threats and issues, foreign medical capabilities, infectious disease, environmental health risks, developments in biotechnology and biomedical subjects of national and military importance, and support to force protection;"[53]
- IC-wide infrastructure--it operates the Joint Worldwide Intelligence Communications System (JWICS) for the DOD, for example;[54] and
- support to OSD, the JCS, and the Combatant Commands (COCOMs). For example, it supports the intelligence division (J-2) within the Chairman's Joint Staff.[55]

The DIA Director has a Defense Intelligence Resource Program Office (DIRMO) to manage all the separate GDIP inputs from DIA, the military services, and U.S. Special Operations Command (USSOCOM, or SOCOM).[56]

Foreign Counterintelligence Program (FCIP)

The FCIP no longer exists as a separate program. The IAA for FY2014 (P.L. 113-126 §314) directed the DNI to merge the FCIP into the GDIP. The DIA Director served as Program Manager for both programs. The FCIP designation was an accounting tool to track money used solely for counterintelligence purposes.[57] CI can be tracked within the GDIP, but lacking the visibility it had as a separate program, it may have less protection now, when weighed against other priorities.

---

[50] P.L. 113-126, §314 (the IAA for FY2014) merged FCIP into the GDIP program.

[51] DIA organizations include the DIA headquarters, the Missile and Space Intelligence Center (MSIC), National Center for Medical Intelligence (NCMI), and the Joint Intelligence Task Force for Combatting Terrorism (JITF-CT). See Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, January 5, 2012, p. F-3.

[52] Services centers include the National Ground Intelligence Center (NGIC), National Air and Space Intelligence Center (NASIC), the Office of Naval Intelligence (ONI) and the Marine Corps Intelligence Activity (MCIA).

[53] Jeffrey T. Richelson, *The US intelligence Community*, 7th ed. (Boulder, CO: Westview Press, 2016), pp. 69 and 72. See also DOD Instruction 6420.01, *National Center for Medical Intelligence (NCMI)*, March 20, 2009 as amended September 2, 2014.

[54] JWICS is the IC's global communications network for those operating at the top secret level. It provides DOD and IC users with "a mature, reliable, and flexible SCI communications architecture. For a detailed description of JWICS, see Joint Publication 2-0, *Joint Intelligence*, October 22, 2013, p. V-2.

[55] For more on COCOMs and the J-2, see the section later in this report on "Special Operations Command (SOCOM) MIP".

[56] The Navy submission includes some funding for those U.S. Coast Guard intelligence-activities that fall within the GDIP. For more on the GDIP and DIRMO, see Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), p. 6-9.

[57] According to Joint Publication 2-0, *Joint Intelligence*, October 22, 2013, pp. I-19 & I-20, "CI is information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, (continued...)

National Geospatial-Intelligence Program (NGP)

The NGP is managed by the Director of NGA. It funds national-level GEOINT-related activities throughout the IC. GEOINT products range from three-dimensional maps and charts, to computerized databases. NGA predominately relies on overhead reconnaissance platforms to provide the raw imagery it needs to produce finished intelligence products.

The Globe is an example of an NGP investment that consolidates legacy search tools into "a single enterprise search and discovery system" designed to deliver "authoritative GEOINT into the hands of our customers."[58] Such products enable analysts to monitor foreign nuclear weapons programs and track ongoing military activities on a worldwide basis.

NGA Director Robert Cardillo's testimony before the House Armed Services Committee provides a good example of the NGP's funding for products like commercial imagery. Cardillo stated:

> This budget request supports U.S. government acquisition of commercial imagery. This imagery enhances U.S. geospatial readiness and responsiveness, and complements national technical means collection for current high-interest areas and rarely imaged areas. This investment in commercial imagery funds a large percentage of our foundation GEOINT data and supports air and sea navigation and humanitarian assistance. In addition, because commercial imagery is unclassified, it meets the growing demands for shareable GEOINT data and products across the government, with allies and nongovernmental partners.[59]

National Reconnaissance Program (NRP)

The NRP is managed by the NRO Director.[60] The NRP was established in 1961 by the Secretary of Defense to coordinate the development and operation of all U.S. reconnaissance programs, covert and overt, as well as aerial and space-based overflight operations of the Air Force and the CIA.[61] In the spring of 1962, the Navy reconnaissance satellite program, which gathered the signals emitted by foreign radars, was also added to the NRP.[62]

The NRP is hardware-focused as opposed to analysis-focused. Government personnel working for the NRO are primarily on detail from the Air Force, CIA, NSA and Navy.[63] The NRP funds

---

(...continued)

sabotage or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities." See also, DOD Directive 5240.02, "Counterintelligence," March 17, 2015.

[58] Globe Fact Sheet, "The Globe: Your Online Connection to the World in Context," at nga.mil.

[59] Testimony of NGA Director Robert Cardillo, "Statement for the Record," in U.S. Congress, House Armed Services Committee, Subcommittee on Strategic Forces, *Fiscal Year 2016 National Security Space Hearing*, 114th Cong., 1st sess., March 25, 2015, at http://docs.house.gov/meetings/AS/AS29/20150325/103106/HHRG-114-AS29-Wstate-CardilloR-20150325.pdf.

[60] The NRO Director also dual-hatted as the Under Secretary of the Air Force from 1961 until 2005. The dual-hatted arrangement allowed each NRO Director—until 2005, when the position of DNRO became an open, singular one—to operate overtly (openly) as an Air Force executive in the Pentagon while running the covert (secret, until 1992) NRO organization. The dual-hatted arrangement stopped after the creation of the DNI position in the IRTPA of 2004.

[61] The NRO was established on September 6, 1961, with a letter from Deputy Secretary of Defense Roswell Gilpatric to DCI Allen W. Dulles. See Clayton D. Laurie, *Congress and the National Reconnaissance Office*, June 2001, p.10, at http://www.nro.gov/history/csnr/programs/docs/prog-hist-04.pdf.

[62] Jeffrey Richelson, *Out of the Black: The Declassification of the NRO*, National Security Archive Electronic Briefing Book No. 257, posted September 18, 2008, at http://nsarchive.gwu.edu/NSAEBB/NSAEBB257/.

[63] Jeffrey Richelson, *The Intelligence Community*, 7th ed. (Boulder, Co: Westview Press, 2016), p. 41.

the NRO and the NRO's efforts to develop, build, launch, and operate satellites associated with *multi-INT* collection—meaning that they collect a variety of signals from foreign instrumentation (FISINT), communications (COMINT), electronics (ELINT), and various forms of measurements and signatures (MASINT).[64] With the benefit of these forms of intelligence, the NRP provides the IC with capability to provide intelligence on topics like imminent military aggression, early warning of foreign missile launches, battle damage assessments, tracking high-value individuals, and monitoring treaty agreements and peacekeeping operations. The NRP also provides the IC with the capability to make NRO satellite information available to first responders and disaster relief operations.[65]

Specialized Reconnaissance Program (SRP)

The SRP is referenced in intelligence policy documents but little is publicly known about the program.[66] According to Elkins, it funds both the procurement of special intelligence gathering devices (to include research and development) and specialized reconnaissance collection activities, in response to tasking procedures established by the DNI.[67]

Nondefense NIP

Nondefense NIP programs are associated with the IC elements located outside the DOD (CIA and the intelligence elements of DOE, DHS, DOJ, State, and Treasury). Nondefense NIP spending funds their associated capabilities: human, all-source, energy, homeland security, law enforcement, drug, diplomatic, and financial intelligence for strategic-level intelligence purposes. Like the defense NIP programs, nondefense NIP programs are traditionally *fenced* from their respective department's budget. They compete for resources within the IC, not within their parent organization. Together, they comprise about 40% of the total NIP budget.[68]

Central Intelligence Agency Program (CIAP)

The CIAP is managed by the Deputy Director CIA and is the largest NIP nondefense program.[69] The CIAP funds the activities of the entire agency, as the CIA is an independent entity and falls under no federal department. The CIA was originally established for the purpose of providing all-source intelligence analysis to senior policymakers.[70] However, covert and clandestine operations

[64] FISINT, COMINT, ELINT and MASINT are defined in **Table A-1**. It was not until December 1, 1995, that the DCI approved declassification of "the fact of" SIGINT collection to include COMINT, ELINT and FIS. See James P. Cavanaugh, Chief Office of Policy, "Declassification of the Fact of Overhead SIGINT -- Information Memorandum," N5P/010/96, April 10, 1997. See Bruce Berkowitz, *NRO at 50 Years: A Brief History*, Center of the Study of National Reconnaissance, NRO, September 2011, p. 26, at http://www.nro.gov/history/csnr/programs/NRO_Brief_History.pdf.

[65] Bruce Berkowitz, *NRO at 50 Years: A Brief History*, Center of the Study of National Reconnaissance, NRO, September 2011, p. 29: "After Hurricane Katrina struck the southeastern United States in August 2005, for example, the Federal Emergency Management Agency and the Army Corps of Engineers used NRO imagery to assess flooded areas and identify the location of hazards."

[66] The SRP is listed as a NIP Program in IC Directive 104, "National Intelligence Program (NIP) Budget Formulation and Justification, Execution, and Performance Evaluation," April 30, 2013, at http://www.dni.gov/files/documents/ICD/ICD%20104.pdf.

[67] Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), p. 4-10.

[68] Jeffrey Richelson, *The U.S. Intelligence Community*, 7th ed. (Boulder, CO: Westview Press, 2016), p. 506.

[69] Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, January 5, 2012, p. F-3.

[70] National Security Act of 1947 (P.L. 80-253).

became and continue to be the agency's most notable activity. CIAP funded CIA activities include:

- HUMINT;
- technical intelligence collection;
- covert and clandestine activities;[71]
- OSINT;
- counterintelligence (CI) outside the United States; and
- research and development, and acquisition of technical collection systems.[72]

CIA's Reserve for Contingencies

Intelligence Authorization Acts—and related appropriations measures—include funding for the CIA's *Reserve for Contingencies*, a budgetary account originally established in 1952 to provide funding for unanticipated intelligence activities, including covert actions.[73] The DCIA must notify congressional intelligence committees when he or she intends to transfer funds from the Reserve for Contingencies to undertake a covert action.[74] Although the DCIA has latitude to spend these funds in a number of ways, and effective oversight is difficult at best, they may not be legally spent on any activity for which funding was denied by Congress.[75]

CIA Retirement and Disability System (CIARDS)

CIARDS is a pension (entitlement) program for certain CIA employees, and as such, is a form of mandatory spending.[76] CIA employees are covered under different retirement systems, depending

[71] Covert action is defined in 50 U.S.C. §3093(e) as "an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include (1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities; (2) traditional diplomatic or military activities or routine support to such activities; (3) traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or (4) activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad." Covert action can include a wide range of clandestine efforts—from subsidizing foreign journals and political parties to participation in what are essentially military operations. A covert operation differs from a clandestine operation in the emphasis that is placed on concealment of the identity of those conducting the operation (i.e., covert) rather than on concealment of the operation (i.e., clandestine). For example, with luck, no one will ever know a clandestine operation occurred (e.g., concealing a listening device). In a covert operation (e.g., blowing up a bridge) the operation is observable, but the identity of those who conducted the operation is disguised. See Jan Goldman, *Words of Intelligence: A Dictionary* (Lanham, MD: Scarecrow Press, 2006). The Directorate of Operations, formerly known as the National Clandestine Service, focuses on the clandestine collection of HUMINT and conducting covert action. For more on the original authorization for the CIA to conduct covert operations, see National Security Directive 10/2, June 18, 1948.

[72] Dan Elkins, *Managing Intelligence Resources*, (Dewey, AZ: DWE Press, 2014), pp. 4-5 to 4-6.

[73] Britt Snider, *The Agency and the Hill: CIA's Relationship with Congress, 1946-2004*, (Washington D.C.: Center for the Study of Intelligence, 2008), p. 164. Pursuant to 50 U.S.C. §3024(d), the DNI also has a "Reserve for Contingencies" with similar restrictions. According to Snider, p. 162, the request in 1952 was tied to covert action in Korea and elsewhere.

[74] 50 U.S.C. 3094(a). Transfers from budgetary accounts other than the Reserve for Contingencies require more extensive congressional notification.

[75] 50 U.S.C. 3094(b).

[76] For more on entitlement programs, see CRS Report RS20129, *Entitlements and Appropriated Entitlements in the* (continued...)

on date of hire and type of duties performed. Most CIA employees are covered by either the Civil Service Retirement System (CSRS) or the Federal Employees Retirement System (FERS). All retirement benefits for CIA employees (CSRS, FERS or CIARDS) are administered by CIA, to protect employee personnel information.[77] For more on CIARDS, see **Appendix C**.

Intelligence Community Management Account (ICMA or CMA)

The ICMA (or CMA) is so titled because it was established in 1992 to support a Community Management Staff (CMS) created by then-DCI Robert Gates to coordinate cross-program activities, improve budget oversight, and strengthen community management. When the IRTPA abolished the position of DCI, it created the new position of DNI assisted by an ODNI. The ODNI absorbed the functions of the old CMS and gained new ones. Although the CMS was abolished, the CMA continued and is referred to as either the ICMA or CMA. For more on the ICMA, see **Appendix C**.

NIP Program within the Department of Energy (DOE NIP)

DOE's Office of Intelligence and Counterintelligence (DOE/IN) represents the DOE in the IC. Its director manages the DOE NIP program. DOE/IN is reportedly valued within the IC for its analysis of "all things nuclear, energy, science and technology and cyber."[78] It provides "timely, technically based intelligence analyses of foreign nuclear/terrorist activities, and the disposition and security of nuclear materials worldwide."[79] Furthermore, DOE/IN provides analyses of major advancements in technology related to global energy security issues.[80] Its counterintelligence efforts are focused on protecting its personnel, technologies, facilities, and intellectual property from foreign collection efforts (particularly cyber threats).[81]

DOE/IN has a "reimbursable Intelligence Work (IW) Program" designed to tap into the DOE's nationwide complex of laboratories—each lab focused on highly advanced, high-risk research in areas such as computers, meteorology, space science, molecular biology, environmental science, and alternative energy sources.[82] In this way, DOE's national laboratories perform work for non-DOE sponsors, such as the DOD and IC.[83] According to a DOE report, "The total volume of IW and the customer base is classified, but it is quite a bit larger than IN's appropriated budget, and it

(...continued)

Federal Budget Process, by Bill Heniff Jr.

[77] The Office of Personnel Management (OPM) administers CSRS and FERS benefits for non-CIA employees.

[78] Department of Energy, *2012 Corporate Overview*, Section 6, p. 33, at http://energy.gov/sites/prod/files/DOE_Corporate_Overview-2012.pdf.

[79] Department of Energy, *2012 Corporate Overview*, Section 6, p. 33.

[80] Department of Energy, *2012 Corporate Overview*, Section 6, p. 33.

[81] Department of Energy, *2012 Corporate Overview*, Section 1, p. 8. For more on DOE/IN, particularly its actions in response to certain security lapses, see U.S. Congress, Senate Committee on Intelligence, *Department of Energy Counterintelligence, Intelligence, and Nuclear Security Reorganization*, 106th Cong., 1st sess., S. Hrg. 106-592, June 9, 1999 (Washington D.C.: GPO, 2000), at http://www.intelligence.senate.gov/sites/default/files/hearings/106592.pdf.

[82] Some of the most well-known labs include Lawrence Livermore, Los Alamos, Sandia and Oak Ridge. For more on the national labs, see "About the National Labs," at http://energy.gov/about-national-labs.

[83] See National Academy of Public Administration, "Positioning DOE's Labs for the Future: A Review of DOE's Management and Oversight of the National Laboratories," *A Report for the U.S. Congress and Department of Energy*, January 2013, p.7, at http://www.napawash.org/wp-content/uploads/2013/01/DOE-FINAL-REPORT-1-2-13.pdf.

represents a very sizable portion of the total reimbursable work performed in the Department's laboratory complex."[84]

NIP Programs within the Department of Homeland Security (DHS/OIA and USCG/IN)

There are only two NIP funded intelligence elements in the DHS, despite the fact that a number of DHS operational components have robust intelligence organizations to support their respective missions (e.g., U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, U.S. Citizenship and Immigration Services, the Transportation Security Administration, U.S. Coast Guard, and the U.S. Secret Service.)[85] The NIP funds the DHS Office of Intelligence and Analysis (DHS/OIA) and some of the U.S. Coast Guard's (USCG's) national-level intelligence-related activities. DHS NIP primarily funds people and activities associated with intelligence analysis as opposed to other types of intelligence-related activities like collection.

DHS Office of Intelligence and Analysis (DHS/OIA)

The NIP Homeland Security program funds the DHS/OIA and is managed by the Under Secretary of DHS for Intelligence and Analysis (DHS/I&A). OIA combines the unique information collected by DHS components as part of their operational activities (e.g., at airports, seaports, and the border) with foreign intelligence from the IC; law enforcement information from federal, state, local, and tribal sources; private sector data about critical infrastructure and key resources; and information from domestic open sources to develop homeland security intelligence.[86] OIA analytical products focus on a wide range of homeland security threats to include: foreign and domestic terrorism, border security, human trafficking, and public health.[87] OIA's customers range from the U.S. President to border patrol agents, Coast Guard seamen, airport screeners, and local first responders.

When the DHS/OIA was incorporated into the IC, it was funded through the NIP. In time, the DNI and DHS leadership argued that because OIA supported both an IC-wide mission and a department-specific mission, it needed both NIP funds to support DNI requirements, and separately controlled Homeland Security Intelligence Program (HSIP) funds to support DHS requirements. In response, the congressional intelligence committees established the HSIP within DHS/OIA to separately manage those intelligence activities that serve predominantly DHS missions. The HSIP is discussed more fully in **Appendix D**.

U.S. Coast Guard Intelligence (USCG/IN)

The USCG's NIP program is managed by the Assistant Commandant for Intelligence and Criminal Investigations (CG-2). The CG-2 is responsible for both the National Intelligence Element and the Law Enforcement Intelligence Program. Coast Guard Intelligence efforts are

[84] Department of Energy, *2012 Corporate Overview*, p. 33.

[85] DHS was founded in 2002 in the wake of September 11, 2001 (9/11) (P.L. 107-296), combining activities that previously had been scattered across a number of agencies and initiating new intelligence and other programs aimed at preventing terrorism through the exploitation of domestic intelligence.

[86] For more on domestic intelligence see Greg Treverton, "Reorganizing U.S. Domestic Intelligence: Assessing the Options," *Monograph*, RAND Corporation, 2008, at http://www.rand.org/pubs/monographs/MG767.html

[87] DHS, "Office of Intelligence and Analysis," at https://www.dhs.gov/office-intelligence-and-analysis.

focused primarily on countering illegal smuggling of weapons, drugs, and migrants; port status and/or safety; counterterrorism; coastal and harbor defense operations; and marine safety and/or environmental protection.[88]

USCG/IN was made a formal member of the IC pursuant to the Intelligence Authorization Act (IAA) for FY2002 (P.L. 107-108, §105). USCG/IN was included as a formal member for a number of reasons but most particularly because it brought new capabilities into the IC.[89] The USCG has diverse missions and unique authorities associated with its dual role as both an armed service and the nation's primary maritime law enforcement agency. A HPSCI report to accompany the IAA for FY2002 quoted the Commandant of the Coast Guard as indicating that the definition of national security

> has widened to include many of the things for which the Coast Guard has been responsible for years. The so-called asymmetric array of threats are now added to the classical inventory of nation-state engagement, potentially leading to armed conflict. It certainly now includes counter-terrorism, counter-narcotics, illegal alien smuggling and worrying about our Exclusive Economic Zone.[90]

USCG intelligence activities are distributed among a number of components to include: the USCG investigative service, CI service, cryptologic group,[91] cyber program, Intelligence Coordination Center (ICC), and several intelligence staffs aligned with regional and field activities.[92] The ICC is the Coast Guard's national-level intelligence analysis and production center.[93] It serves as the liaison between the USCG and other national-level IC and law enforcement entities. The ICC produces intelligence that supports the Coast Guard's maritime intelligence requirements, disseminates intelligence to relevant national and military decision makers, and manages USCG intelligence requirements and the collection management process.

NIP Programs within the Department of Justice (FBI/NSB and DEA/ONSI)

Federal Bureau of Investigation National Security Branch (FBI/NSB)

The FBI is an intelligence and law enforcement agency. Joint Publication 2-01 describes the FBI's role in the IC this way:

> It is responsible for understanding threats to our national security and penetrating national and transnational networks that have a desire and capacity to harm the US. The FBI coordinates these efforts with its IC and law enforcement partners. It focuses on terrorist

[88] For a primer on the IC and USCG/IN, see U.S. Coast Guard, *Intelligence*, May 2010, at https://www.uscg.mil/doctrine/CGPub/CG_Pub_2_0.pdf. See also Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, January 5, 2012, pp. A-9 and A-10.

[89] The attacks on September 11, 2001 were a major catalyst for including the USCG/IN. See Kevin Wirth, *The U.S. Coast Guard Intelligence Program Enters the Intelligence Community*, Occasional Paper, National Defense Intelligence College, May 2007, at http://www.dtic.mil/dtic/tr/fulltext/u2/a476640.pdf.

[90] U.S. Congress, House Permanent Select Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 2002*, 107th Cong., 1st sess., H.Rept. 107-219 to accompany H.R. 2883, September 26, 2001 (Washington, D.C.: GPO, 2001), p. 24.

[91] USCG, *Commandant Instruction 3820.5, Coast Guard Implementation of Presidential Policy Directive/PPD-28-Policies and Procedures*, at http://www.uscg.mil/directives/ci/3000-3999/CI_3820_5.pdf.

[92] U.S. Coast Guard, *Intelligence*, May 2010, pp. 19-22. See also Sally Brice O'Hara, Vice Commandant, "Coast Guard Intelligence—As Unique as the Coast Guard Itself," *Defense Media Network*, January 6, 2012.

[93] The ICC is co-located with the Office of Naval Intelligence at the National Maritime Intelligence Center in Suitland, Maryland.

> organizations, foreign intelligence services, WMD [Weapons of Mass Destruction] proliferators, and criminal enterprises. As the principal investigative arm of DOJ, the FBI is primarily responsible for CI and counterterrorism operations conducted in the United States. CI operations contemplated by any other organizations in the United States must be coordinated with the FBI. Any overseas CI operation conducted by the FBI must be coordinated with the CIA.[94]

The FBI was one of the organizations targeted for reform after the attacks of September 11, 2001. Investigations highlighted a number of obstacles to information sharing among the nation's intelligence and law enforcement communities. In the decade following 9/11, a number of laws and executive orders included provisions designed to improve the FBI's counterterrorism efforts.[95] For example, the IRTPA of 2004 (P.L. 108-458) directed the FBI Director "to develop and maintain a specialized and integrated national intelligence workforce consisting of agents, analysts, linguists, and surveillance specialists who are recruited, trained, and rewarded in a manner which ensures the existence within the Federal Bureau of Investigation of an institutional culture with substantial expertise in, and commitment to, the intelligence mission of the Bureau."[96]

The FBI's NIP program is headed by the Intelligence Branch Executive Assistant Director. It funds the FBI's National Security Branch (NSB). Within the NSB, the CI Division's efforts focus on preventing theft of sensitive information and advanced technologies.[97] The Directorate of Intelligence maintains field offices throughout the United States, each with its own intelligence staff.[98] The Counterterrorism Division oversees over 100 interagency groups comprised of federal, state, and local government intelligence and law enforcement entities known as Joint Terrorism Task Forces. The WMD Division helps coordinate intelligence-related efforts designed to prevent the use of chemical, biological, radiological, and nuclear weapons. Among its many functions, the Terrorist Screening Center maintains the U.S. government's consolidated watch list of known or suspected terrorists.

Drug Enforcement Administration's Office of National Security Intelligence (DEA/ONSI)

The DEA's NIP program is headed by DEA's Assistant Administrator and Chief of Intelligence. It funds the intelligence activities of DEA/ONSI—the IC's most recent formally added entity.[99]

---

[94] Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, January 5, 2012, p. A-9.

[95] See for example USA PATRIOT Act (2001) (P.L. 107-56) ; USA PATRIOT Reauthorization and Improvement Act of 2005 (P.L. 109-177), and E.O. 12333, as amended by E.O.s 13284 (2003), 13355 (2004) and 13470 (2008).

[96] P.L. 108-458 §2001(c).

[97] FBI, *Intelligence National Strategy*, November 4, 2011, at https://www.fbi.gov/news/stories/2011/november/counterintelligence_110411. See also E.O. 12333 §1.3 (b) (20) (A) which directs the intelligence elements of the FBI to: (1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions; (2) Conduct counterintelligence activities; and (3) Conduct foreign intelligence and counterintelligence liaison relationships with intelligence, security, and law enforcement services of foreign governments or international organizations.

[98] Unlike other IC entities, the FBI is authorized to conduct HUMINT operations within the U.S. as part of its law enforcement duties. FBI/DI uses this authority to conduct source operations and interrogations of known or suspected terrorists, criminals, or facilitators on U.S. soil. See testimony of FBI Director Robert S. Mueller III, U.S. Congress, House Permanent Select Committee on Intelligence, *The State of Intelligence Reform 10 Years after 9/11*, hearings, 112th Cong., 1st sess., October 6, 2011, at https://www.fbi.gov/news/testimony/the-state-of-intelligence-reform-10-years-after-911.

[99] DEA/ONSI was designated as the 16th member of the IC in in February 2006 by then-DNI John Negroponte and Attorney General Alberto Gonzales. See Office of the DNI, "Drug Enforcement Administration Element Becomes 16th (continued...)

While the office is a part of the Office of Strategic Intelligence within the DEA's Intelligence Division, only DEA/ONSI is designated as a member of IC.[100] ONSI employs intelligence analysts in 21 U.S. field divisions and over 80 offices overseas located in more than 60 countries. It seeks to reduce the supply and international flow of narcotics, combat terrorism, and protect U.S. national security interests.[101]

E.O. 12333 directs the DEA and the intelligence elements within the Departments of Energy, Homeland Security, State, and Treasury, to: "collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and CI to support national and departmental missions; and … conduct and participate in analytic or information exchanges with foreign partners and international organizations."[102]

NIP Program within the Department of State (State INR)

The Assistant Secretary of State for Intelligence and Research directs the department's Bureau of Intelligence and Research (INR), serves as the Secretary of State's principal adviser on intelligence matters, and coordinates and supervises all intelligence-related activities in the Department.[103] State Department NIP primarily funds people and activities associated with intelligence analysis. According to the State Department's Foreign Affairs Manual (FAM), the Assistant Secretary's responsibilities include the following:[104]

- directing the Department's all-source and independent research and analysis;
- ensuring INR participation in community intelligence analyses;
- ensuring that U.S. intelligence activities support U.S. foreign policy priorities are consistent with Chief of Mission authority, laws, and Executive Orders and do not undermine the foreign policy interests of the United States;
- coordinating and representing the State Department's requirements for intelligence collection and analysis to the IC;
- ensuring efficient receipt, processing, and dissemination of intelligence;
- facilitating State Department requests for declassification, release, or exceptional use of information derived from State Department intelligence sources;
- determining whether a State Department employee may have access to certain classified materials; and
- serving as the primary reporting channel to the President's Intelligence Advisory Board (PIAB) and the Intelligence Oversight Board (IOB).[105]

(...continued)

Intelligence Community Member," February 17, 2006, at http://www.dni.gov/files/documents/Newsroom/Press%20Releases/2006%20Press%20Releases/20060217_release_content.htm.

[100] This is similar to how the Department of the Treasury's Office of Intelligence and Analysis, itself subordinate to the Treasury's Office of Terrorism and Financial Intelligence, exists as Treasury's representative to the IC.

[101] "Member Agencies," at http://www.intelligence.gov/mission/member-agencies.html.

[102] E.O. 12333 (as amended) §1.7 (i).

[103] State Department, *U.S. Department of State Foreign Affairs Manual Volume 1, 1 FAM 430 Bureau of Intelligence and Research (INR)*, November 19, 2015, at https://fam.state.gov/fam/01fam/01fam0430.html.

[104] These types of responsibilities are equally applicable to the responsibilities of the heads of IC elements in Departments like Treasury and Energy.

[105] State Department, *U.S. Department of State Foreign Affairs Manual Volume 1, 1 FAM 430 Bureau of Intelligence and Research (INR)*, November 19, 2015. For more on the PIAB and IOB, see "About the PIAB and IOB" on the (continued...)

INR has a number of offices that produce all-source analysis on issues as diverse as economic security, terrorist group financing, strategic arms control, political-military issues, and cyber for the Secretary of State and other key policymakers.[106] INR Watch is the State Department's 24-hour, seven-day-a-week center for monitoring, evaluating, alerting, and reporting time-sensitive intelligence to department and INR principals and serves as liaison to other IC operations centers.[107] INR does not engage in clandestine collection operations.[108]

NIP Program within the Department of Treasury (Treasury OIA)

The Assistant Secretary of Treasury for Intelligence and Analysis (AS/OIA) manages the NIP program for financial intelligence.[109] The IC element within the Department of Treasury is the Office of Intelligence and Analysis (OIA). The Treasury NIP primarily funds people and activities associated with intelligence analysis. OIA provides intelligence support to both the IC as a whole and the Treasury Department's regulatory and enforcement authorities.

As the DNI's focal person for threat finance, the AS/OIA has responsibility for ensuring all IC finance intelligence elements collaborate and integrate their respective operations across focus areas such as terrorist financing, weapons proliferation, drug trafficking, and other areas. OIA also provides all-source intelligence relevant to warfighters at the tactical-level. The office established joint intelligence, military, and law enforcement cells in Iraq and Afghanistan to help identify and interdict funding streams to terrorist and insurgent networks. These cells allow OIA to interact with other IC entities and military forces to produce time-sensitive and actionable intelligence valuable to the day-to-day war effort.

Both the AS/OIA and the Assistant Secretary for Terrorism Financing (AS/TF) report to the Under Secretary of Treasury for Terrorism and Financial Intelligence (OTFI). OTFI's stated mission is to assemble "the department's intelligence and enforcement functions with the twin aims of safeguarding the financial system against illicit use and combating rogue nations, terrorist facilitators, weapons of mass destruction (WMD) proliferators, money launderers, drug kingpins, and other national security threats."[110]

The Senate Intelligence Committee report accompanying the IAA for FY2015 (P.L. 113-293) directs the DNI to provide performance assessments for an initiative called FIX-ITT (Financial Exchange and Intelligence Integration).[111] FIX-ITT is an ODNI integrating effort to bring all

(...continued)

White House website at https://www.whitehouse.gov/administration/eop/piab.

[106] State Department, *U.S. Department of State Foreign Affairs Manual Volume 1, 1 FAM 430 Bureau of Intelligence and Research (INR)*, November 19, 2015.

[107] Ibid.

[108] INR does not have agents in the field. INR engages with Embassy staff who share HUMINT gathered locally and overtly by virtue of their presence in foreign countries.

[109] Congress created OIA in the Intelligence Authorization Act for FY2004 (P.L. 108-177, Section 105). The head of Treasury intelligence also serves as National Intelligence Manager (NIM) for Threat Finance and Transnational Organized Crime. NIMs serve as the principal substantive advisors on intelligence related to designated countries, regions, topics, or functional areas. NIMs provide a single voice to policymakers to orient and guide collection and analytic activities to satisfy customers' information needs. For more on NIMs, see "Intelligence Integration, Who We Are," at odni.gov.

[110] Department of the Treasury, "Terrorism and Financial Intelligence," at http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorism-and-Financial-Intelligence.aspx

[111] U.S. Congress, Senate Select Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 2015*, 113th Cong., 2nd sess., S.Rept. 113-233 to accompany S. 2741, July 31, 2014, (Washington, D.C.: GPO, 2014), p. 7.

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.[112]

Military Intelligence Program (MIP)

In contrast to the NIP, the MIP *belongs* to the Secretary of Defense.[113] A program is primarily MIP if it funds an activity that addresses a unique DOD requirement. Each MIP program consists of a "wide range of diverse, disparate joint and tactical intelligence" assets and activities that all reside in the budget of a single DOD component.[114] According to the MIP charter directive:

> 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.[115]

Intelligence budget expert Robert Mirabello explains the MIP as providing "the 'take it with you' intelligence organic to the deployable units in all services at all echelons of command."[116] MIP programs are not capability based. They support anything from language training to biometrics to any number of surveillance tools. Examples include the Army's intelligence support to detainee operations; the Navy's ballistic missile data collection radar system known as Cobra Judy Replacement; the Air Force's Global Hawk unmanned aircraft system; and DIA's intelligence support to the Combatant Commands.

Unlike the defense NIP programs, MIP programs compete for resources within the larger DOD budget. The MIP label does not confer any special status on a program or activity.[117] MIP funds are not *fenced*, but they are monitored closely, and cannot be reprogrammed without the approval of the USD(I).[118] While MIP-labelled resources are *protected* by the USD(I) from use by other organizations within the DOD, they are still subject to DOD budget constraints.[119] In other words, MIP-funded people and programs can be subject to DOD-wide requirements in ways that NIP-funded people and programs are not. For example, when the DOD furloughed thousands of civilian employees for 11 days in 2013 (for reasons related to congressionally mandated

[112] Ibid.

[113] See Robert Mirabello, "Budget and Resource Management," *Intelligencer: Journal of U.S. Intelligence Studies*, vol. 20, no. 2 (Fall/Winter 2013), p. 68.

[114] Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), p. 4-12.

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

[116] Robert Mirabello, "Budget and Resource Management," *Intelligencer: Journal of U.S. Intelligence Studies*, vol. 20, no. 2 (Fall/Winter 2013), p. 67. See also Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), p. 4-11.

[117] Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), p. 4-13.

[118] The role and responsibilities of the USD(I) are discussed in the "Under Secretary of Defense for Intelligence (USD(I))/Director of Defense Intelligence (DDI)" section later in this report.

[119] Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), pp. 4-18 to 4-19. See also S. Rept. 102-117, 102nd Cong., 1st sess. (Washington D.C: GPO, July 24, 1991), p. 5: "Tactical intelligence systems—which, unlike national intelligence programs, must compete for funding directly with weapons systems…"

automatic budget cuts) NIP-funded civilian personnel were exempted but MIP-funded civilian personnel were not.[120]

Table B-1 identifies and briefly describes a number of MIP programs. Funding associated with each MIP program supports tactical-level intelligence activities associated with that entity's overall mission. Each MIP program is managed separately by a *Component Manager*. See "Program and Component Managers" section below. They are also listed in Table E-1, Appendix E.

Defense-Wide MIP

DIA, NGA, NRO and NSA MIP

The Directors of DIA, NGA, NRO, and NSA manage NIP and MIP funds. Those agency activities that support tactical-level operations not funded by the GDIP, NGP, NRP, or CCP, respectively, are supported in many cases with MIP funds.[121] According to Joint Publication 2-01:

- DIA MIP consists of DIA's intelligence activities focused on support to the COCOMs. The COCOM Joint Intelligence Operations Centers (JIOCs)[122] and the DOD counterintelligence and HUMINT center resources are included here. The Component Manager is the Director DIA.
- NGA MIP funds defense-wide GEOINT activities, including communication, and production system improvements, as well as the defense imagery activities of NGA. Also funded are selected defense airborne and space reconnaissance activities managed by NGA. The Component Manager is the Director, NGA.
- NSA MIP consists of cryptologic and SIGINT support to the DOD. The Component Manager is the Director, NSA.
- NRO MIP augments the NRO NIP resources addressing specific DOD requirements. The Component Manager is the Director, NRO.[123]

In 2015, Betty Sapp, current Director of the NRO, testified publicly about NRO's support to the warfighter, particularly its "ability to fuse multi-intelligence data to support warfighter intelligence needs:"

> I would like to start by highlighting the real bottom line for the NRO – our support to the warfighter. The NRO has become a key global military operations enabler and many capabilities are integral to the conflict in Afghanistan and other theaters. In addition to traditional NRO ISR systems and support, we provide a wide array of focused

[120] See for example, Associated Press, "Pentagon set to furlough 680,000 civilian employees," *Daily News*, May 14, 2013, at http://www.nydailynews.com/news/politics/pentagon-set-furlough-680-000-civilian-employees-article-1.1343794.

[121] There are other non-intelligence funding sources beyond the NIP and MIP. For example, according to Elkins, the DOD may provide personnel-related resources such as family housing, or provide funding from its Information Systems Security Program for certain information technology related activities. Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), p. 4-6.

[122] JIOCs integrate all DOD intelligence functions and disciplines, and facilitate access to all sources of intelligence—external defense and national intelligence organizations, multinational/partner nations, nongovernmental organizations, other government department and agencies, and law enforcement. They are the focal point for the COCOM's intelligence planning, collection management, analysis, and production effort. For more see, Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, January 5, 2012, p. xii.

[123] Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, January 5, 2012, p. F-8.

> capabilities to help solve specific, critical ISR needs for deployed personnel around the world.
>
> These services, products, and tools directly contribute to the highest priority missions, to include: countering Improvised Explosive Devices (IEDs); identifying and tracking High-Value Targets; and improving battlespace awareness.
>
> To ensure users are able to take advantage of NRO capabilities, we developed the Field Representative program that puts NRO subject matter experts, both military and civilian, at the combatant commands and in the theater battlespace. These men and women serve as technical liaison officers to units, and support specific NRO programs and capabilities focused on the warfighter.
>
> A real strength of the NRO is our ability to fuse multi-intelligence data to support warfighter intelligence needs. We have helped the warfighter visualize large volumes of data temporally and spatially, establishing patterns of life, identifying the unusual within a multitude of fused data sets, and integrating full motion video data with automated multi-intelligence tipping, cueing, and alerting capabilities.
>
> Our cutting-edge solutions combine GEOINT and SIGINT, and span the space, air, and ground operational domains to provide the warfighter a comprehensive common operational picture, enhancing the ability to find, fix, and finish targets.[124]

Office of the Secretary of Defense (OSD) MIP

OSD MIP funds are managed by the USD(I) and used "to exercise planning, policy, and strategic oversight of all DOD intelligence, CI, and security policy, plans and program. OSD MIP provides funds for counternarcotics intelligence support managed by the Deputy Assistant Secretary of Defense for Counternarcotics and Global Threats."[125] It also supports special technology programs with DOD-wide applications that are not funded elsewhere. For example, it funds the following:

- Advanced Sensors Application Program—a program researching and developing sensors for a variety of service-specific intelligence needs;
- Foreign Materiel Acquisition and Exploitation Program—a program to acquire, analyze and counter foreign materials that could potentially be used in harmful ways (e.g., chemicals, weapons systems, computer software, microbes); and
- Horizontal Fusion Program—a program to connect soldiers in the field with commanders and with battlefield information—helping them to "fuse" information available from a number of physically dispersed data sources.[126]

Special Operations Command (SOCOM) MIP

As a rule, Combatant Commands (COCOMs), such as the U.S. Pacific Command or the U.S. Central Command, have no military forces or equipment assigned directly to them. Instead, they

[124] Testimony of NRO Director Betty Sapp, "Statement for the Record," in U.S. Congress, House Armed Services Committee, Subcommittee on Strategic Forces, *Fiscal Year 2016 National Security Space Hearing*, 114th Cong., 1st sess., March 25, 2015, at http://docs.house.gov/meetings/AS/AS29/20150325/103106/HHRG-114-AS29-Wstate-SappB-20150325.PDF. This quote was chosen because unclassified testimony by any IC official on any IC program offers a rare glimpse into program specifics.

[125] Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, January 5, 2012, p. F-8.

[126] Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), p. 4-14. See also Jeffrey Richelson, *The U.S. Intelligence Community*, 7th ed. (Boulder, CO: Westview Press, 2016), p. 527.

rely on the military departments and defense agencies to provide the forces and equipment necessary to carry out COCOM-run military operations.[127] These COCOMs do not have their own budgets; instead they each provide budgetary input to the military department that serves as their executive agent.[128]

SOCOM is unique—unlike any other COCOM.[129] It was established by Congress in 1987 (P.L. 99-661) with military department-like responsibilities and its own budget to organize, train, and equip its military forces. Thus, SOCOM's MIP budget is submitted separately from the MIP budgets associated with the military services. There is no separate SOCOM NIP program; instead, SOCOM requests for NIP funds go to the CCP, GDIP, and NGP Program Managers for review and incorporation into the annual CCP, GDIP and NGP budget requests.[130]

Like most COCOMs, SOCOM has a joint staff at the headquarters level, and the *J-2* is its manager for SOCOM's intelligence funds.[131] The *J-2* acronym is associated with not only the division of the joint staff associated with intelligence, but also the individual who leads that section.[132]

SOCOM tactical-level intelligence resources are directed toward building up its own organic capabilities and reimbursing support from military departments.[133] The SOCOM JIOC is funded through the DIA MIP.[134]

One recent report in *National Defense* magazine provides a number of insights into SOCOM's intelligence needs. For example, according to the report,

> SOF [special operations forces] has several programs underway to help facilitate that global flow of information, gathered by everything from high-end airborne platforms to troop-worn cameras and tracking devices. [Admiral] McRaven [then-SOCOM Commander] has directed that acquisition efforts be focused first on outfitting an array of aircraft — both manned and unmanned, fixed and rotary wing—with advanced ISR [intelligence, surveillance and reconnaissance] and data storage capabilities that will work in multiple environments.[135]

[127] The role of the military departments is to organize, train and equip their respective forces and provide them to the COCOMs for military operations.

[128] Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), pp. 6-6 and 6-7.

[129] USSOCOM, *Factbook 2012*, at https://fas.org/irp/agency/dod/socom/factbook-2012.pdf.

[130] Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), p. 6-7.

[131] Ibid.

[132] On a typical joint staff the J-1 is associated with Personnel; the J-3 with Operations; the J-4 with Logistics; the J-5 with Strategy, Plans, and Policy; the J-6 with Communications; the J-7 with Force Development; and the J-8 for Force Structure, Resources and Assessment. The headquarters staffs of the military departments are organized in a similar fashion, but use a different letter designation. For example, the intelligence section on the Air Staff is known as the A-2, the counterpart on the Army staff is the G-2 (G for ground), and the counterpart on the Navy Staff is the N-2. The USMC is not a military department; it is a component of the Navy. Its headquarters staff has a Director for Intelligence known as the DIRINT.

[133] Dan Parsons, "U.S. Special Operations Command Seeks Intelligence Capabilities for Duty Worldwide," *National Defense*, National Defense Industry Association Magazine, July 2013, at http://www.nationaldefensemagazine.org/archive/2013/July/Pages/USSpecialOperationsCommandSeeksIntelligenceCapabilitiesforDutyWorldwide.aspx. Parson quotes USSOCOM's intelligence program manager in 2013 as saying, "[W]e're looking to share the data, use other people's data, use other people's tools and applications."

[134] Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, January 5, 2012, p. F-8.

[135] Dan Parsons, "U.S. Special Operations Command Seeks Intelligence Capabilities for Duty Worldwide," *National Defense*, National Defense Industry Association Magazine, July 2013.

General Joseph Votel, the current SOCOM Commander recently testified about the command's reliance on the military services for airborne intelligence specialists:

> [O]ur operational tempo has created an increased need for Tactical Systems Operators (TSOs), which are airborne intelligence specialists provided by the Services. TSOs operate on aircraft that are not programs of record, but are vital to our ability to target enemies on the ground. This creates a situation where the Air Force, as well as the other Services, have an increased manpower bill they have not programmed for, while they provide us with essential intelligence support. For critical and unique enduring capabilities like TSOs, it is essential that we provide sustainable funding that allows the Services to provide sustainable sourcing.[136]

Service-Specific MIP

The military services each maintain their own intelligence collection and analysis capabilities. These organic military intelligence assets focus on the intelligence most urgently required by their parent service.[137]

Air Force MIP

The Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance (ISR) (AF/A2) manages resources associated with the 25th Air Force (AF) and the National Air and Space Intelligence Center (NASIC).[138] Air Force MIP funds programs and people associated with:

- globally integrated ISR;[139]
- electronic warfare;
- airborne national command and control;
- nuclear detection and treaty monitoring;[140]
- information operations;[141]
- cryptology;[142]
- science and technology intelligence; and

[136] Joseph L. Votel, General, U.S. Army Commander USSOCOM, *Statement before the Senate Armed Services Committee*, March 8, 2016, at http://www.socom.mil/Documents/Votel_03-08-16.pdf.

[137] For additional information on service-specific MIP, see Jeffrey Richelson, *The U.S. Intelligence Community*, 7th ed. (Boulder, CO: Westview Press, 2016), p. 527.

[138] The U.S. Air Force Intelligence component can trace its origins to the Army Signal Corps, which flew the first airplanes and conducted aerial trench surveys in World War I.

[139] "Collection operations are carried out during either surveillance or reconnaissance missions. While reconnaissance missions are specifically conducted to obtain information about the threat or the OE [operational environment], surveillance missions consist of the systematic observation of places, persons, or things." See Joint Publication 2-0, *Joint Intelligence*, October 22, 2013, p. I-11.

[140] The Air Force Technical Applications Center performs nuclear treaty monitoring and nuclear event detection. See U.S. Air Force, "Air Force ISR Agency," at http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104553/air-force-isr-agency.aspx.

[141] "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own." See Joint Publication 3-13, *Information Operations*, November 20, 2014.

[142] 25th AF serves as the Air Force's Cryptologic Component for Director, NSA/Chief Central Security Service.

- targeting and analysis operations for Air Force and joint commanders, national policy makers and coalition partners.[143]

Five 25th AF wings are responsible for collecting GEOINT, SIGINT and MASINT.[144] ISR systems range in size from hand-held devices to orbiting satellites. Some collect basic information for a wide range of analytical products; others are designed to acquire data for specific weapons systems. ISR platforms most commonly used by ISR-affiliated wings to collect intelligence are the RC-135 variants, U-2, MQ-1 Predator, MQ-9 Reaper, and the RQ-4 Global Hawk.[145]

Air Force MIP also funds activities associated with the National Air and Space Intelligence Center (NASIC), a Field Operating Agency subordinate to the AF/A2. NASIC analyzes data on foreign aerospace forces and weapons systems to determine performance characteristics, capabilities, vulnerabilities, and intentions. The center also supports weapons treaty negotiations and verification.[146]

Army MIP

U.S. Army intelligence[147] policy, operations (to include training) and budget are the responsibility of the Office of the Deputy Chief of Staff for Intelligence (ODCS/G-2). The Army G-2 coordinates multidisciplinary intelligence collection and analysis throughout the Army, to include GEOINT, SIGINT, HUMINT, MASINT, and CI.[148]

Funding for Army MIP supports people and activities associated with the U.S. Army Intelligence and Security Command (INSCOM).[149] The National Ground Intelligence Center (NGIC) is a subordinate element of INSCOM and is responsible for collecting and disseminating GEOINT and all-source intelligence on foreign ground force capabilities and technologies. Additionally, NGIC employs specialists such as physicists, chemists, and engineers who, along with other technical specialists, evaluate foreign weapon systems in order to evaluate current and future foreign military armament performance and capabilities.[150]Army Cryptologic Operations (ACO) is a subordinate to INSCOM and is the Army's lead cryptologic effort in meeting SIGINT collection requirements.[151] Army Brigade Combat Teams (BCT) have their own organic military intelligence (MI) companies. These companies are devoted to producing, analyzing, and disseminating intelligence information products specific to BCT areas of operations.

---

[143] See *25th AF Strategic Plan 2015*. See also, 25th Air Force, "About Us," at http://www.25af.af.mil/AboutUs/FactSheets/Display/tabid/6260/Article/662963/twenty-fifth-air-force.aspx..

[144] The five Wings: 9th Reconnaissance, 55th, 70th ISR, 363rd ISR, and the 480th ISR.

[145] See U.S. Air Force, "25 AF Frequently Asked Questions," at http://www.25af.af.mil/shared/media/document/AFD-150217-054.pdf.

[146] 25th AF, *Strategic Plan 2015*.

[147] Army intelligence traces its origins to Knowlton's Rangers, a reconnaissance and intelligence unit established by General Washington in 1776. See U.S. Army Intelligence Center Fort Huachuca, *A Brief History of US Army Intelligence* (Fort Huachuca, AZ: Fort Huachuca Museums, n.d) p. 3., at http://usaic.hua.army.mil/History/PDFS/briefmi.pdf.

[148] U.S. Army, "Army Intelligence and Vision," at http://www.dami.army.pentagon.mil/Mission.aspx.

[149] U.S. Army Doctrine Reference Publication 2-0, "Intelligence," August 31, 2012, at http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/adrp2_0.pdf.

[150] INSCOM. "National Ground Intelligence Center," August 4, 2014, at https://www.inscom.army.mil/msc/NGIC.aspx.

[151] INSCOM, "Army Cryptologic Operations," at https://www.inscom.army.mil/MSC/ACO.aspx.

Navy and Marine Corps MIP

U.S. Navy intelligence policy, operations (to include training) and budget are the responsibility of its Director of Naval Intelligence, who also serves as the deputy Chief of Naval Operations for Information Dominance (N-2/N-6).[152] The U.S. Marine Corps (USMC) is a component of the Navy. The USMC headquarters staff has a Director for Intelligence (DIRINT) responsible for USMC intelligence policy, operations and budget.

The Deputy Under Secretary of the Navy (DUSN) for Plans, Policy, Oversight and Integration (PPOI) is responsible for oversight of both Navy and USMC MIP. According to a Navy policy document:

> DUSN PPOI exerts authority over the MIP to ensure that projects adhere to applicable strategy and are resourced properly. This authority is executed on behalf of the UNSECNAV [Under Secretary of the Navy] and in coordination with Service MIP component managers. The Navy Budget Office ensures the MIP projects are properly priced, budgeted, and executed through Departmental PPBE processes, and proposes, coordinates, and processes execution realignments when necessary. The Navy Budget Office coordinates with budget submitting offices (BSOs) and Service intelligence and programming staffs to ensure the MIP is properly displayed in Departmental data, budgets, and submissions to higher authority.[153]

Funds for Navy MIP support people and activities associated with various aspects of maritime intelligence to include:

- strategic, operational, and tactical plans and capabilities of foreign naval forces;[154]
- foreign technologies, sensors, weapons, platforms, combat systems, cyber, and command, control, communication, computers, intelligence, surveillance, and reconnaissance capabilities;[155]
- special collection and analysis for irregular and expeditionary forces;[156]
- information technology and services;[157] and
- cyberspace and cryptologic operations.[158]

Funds for USMC MIP support people and activities related to battlefield intelligence. MIP funds support Marine Air-Ground Task Force intelligence—which consists primarily of organic intelligence units supporting the tactical and operational intelligence requirements of Marine commanders. USMC MIP funded people include analysts who can conduct intelligence-related

[152] For more on this position, see Joe Gradisher,"Vice Adm. Branch takes charge of information dominance and Naval intelligence," *press release* NNS130725, July 25, 2013, at http://www.navy.mil/submit/display.asp?story_id=75580.

[153] SECNAVINST 5000.38A, February 5, 2010.

[154] ONI, "Nimitz Operational Intelligence Center," at http://www.oni.navy.mil/commands/Nimitz.html.

[155] ONI, "Farragut Technical Analysis Center," at http://www.oni.navy.mil/commands/Farragut.html.

[156] ONI, "Kennedy Irregular Warfare Center," at http://www.oni.navy.mil/commands/Kennedy.html. For more information on U.S. Navy irregular warfare, see CRS Report RS22373, *Navy Irregular Warfare and Counterterrorism Operations: Background and Issues for Congress*, by Ronald O'Rourke.

[157] ONI, "Hopper Information Services Center, at http://www.oni.navy.mil/commands/Hopper.html.

[158] U.S. Navy, "FCC/C10F 2014 Fact Sheet," at http://www.public.navy.mil/fcc-c10f/Fact%20Sheets/FCC-C10F%20Fact%20Sheet%202014.pdf.

activities such as intelligence preparation of the battlefield, and target analysis.[159] It also funds activities associated with GEOINT, SIGINT, CI and ISR.

Summary of NIP and MIP Funding Sources for IC Elements

Members of the defense cryptologic community receive additional funds from the Information Systems Security Program (ISSP) for information assurance activities.

Table 3 illustrates that a number of IC elements—CIA, ODNI, and IC elements at the Departments of Energy, Homeland Security, Justice, State and Treasury—receive NIP resources but no MIP resources. Other IC elements, such as DIA, NSA, and NRO have both NIP and MIP funding sources.

While this report focuses on the NIP and MIP, it should be noted that there are other funding streams outside the NIP and MIP. For example, DHS/OIA also manages an intelligence-related program (neither NIP nor MIP) known as the Homeland Security Intelligence Program (HSIP). The HSIP is briefly examined in Appendix D.[160] Members of the defense cryptologic community receive additional funds from the Information Systems Security Program (ISSP) for information assurance activities.[161]

Table 3. Intelligence Community Elements: Funding Sources

National and Military Intelligence Programs

Element	MIP	NIP
Central Intelligence Agency		CIAP
Combatant Commands	DIA MIP SOCOM MIP	GDIP, NGP, CCP
Defense Intelligence Agency	DIA MIP	GDIP
Department of Homeland Security[a]		Department-Specific NIP
Department of Defense	Department-Specific MIP OSD MIP	CCP, GDIP, NGP, NRP (associated with NSA, DIA, NGA and NRO)
Departments of Energy, Justice, State and Treasury		Department-Specific NIP
National Geospatial-Intelligence Agency	NGA MIP	NGP
National Reconnaissance Office	NRO MIP	NRP
National Security Agency	NSA MIP	CCP
Office of the Director of National Intelligence		ICMA

Source: CRS, based on Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014).

[159] U.S. Marine Corps, Marine Corps Warfighting Publication 2-1, Intelligence Operations, at http://www.marines.mil/Portals/59/Publications/MCWP%202-1%20Intelligence%20Operations.pdf.

[160] 6 U.S.C. §121. See also, the IAA for FY2013, P.L. 112-277 §501, Jan. 14, 2013. According to 6 U.S.C. §121a, the HSIP exists solely within the Department of Homeland Security (DHS) to fund those "intelligence activities of the Office of Intelligence and Analysis … that serve predominantly departmental missions."

[161] For more on the ISSP, see Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), p. 4-6.

Notes:

a. DHS also has an intelligence-related program called the Homeland Security Intelligence Program. The HSIP does not fall under the NIP or MIP. (For more on HSIP, see **Appendix D**.)

b. Acronyms: CCP—Consolidated Cryptologic Program; CIAP—CIA Program; ICMA—Community Management Account; GDIP—General Defense Intelligence Program; OSD—Office of the Secretary of Defense; NGP—National Geospatial-Intelligence Program; NRP—National Reconnaissance Program.

c. See Figure 3.4 in Mark Lowenthal, *Intelligence: From Secrets to Policy*, 6th ed. (Thousand Oaks, CA: Sage/CQ Press, 2015), p. 67, for a budgetary view of the IC.

Managing NIP and MIP Funds

Director of National Intelligence (DNI)[162]

The DNI has overall responsibility for intelligence support to the President and the day-to-day management of the IC. Both defense and nondefense NIP budgets are determined and controlled by the DNI, from budget development through execution (although the USD(I) acting on behalf of the Secretary of Defense is also key player in defense NIP budget development).[163] E.O. 12333 directs heads of IC elements to provide the "programmatic and budgetary information necessary to support the Director in developing the National Intelligence Program."[164] The Office of the DNI (ODNI), a staff of some 1,500 individuals, works to carry out the DNI's NIP-related responsibilities along with other responsibilities such as those associated with the National Intelligence Council and national intelligence centers (e.g., National Counterterrorism Center and National Counterproliferation Center).[165]

The position of DNI replaced the position of Director of Central Intelligence (DCI) such that the DCI position no longer exists. The DCI position was a *triple-hatted* arrangement in which the DCI simultaneously served as community manager, Director of the Central Intelligence Agency (CIA) and chief intelligence advisor to the President. 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 community manager and principal advisor to the President, and leaving leadership of the CIA to the DCIA.[166] The DNI was given greater budgetary authorities in conjunction with the NIP than the DCI had in conjunction with the NFIP in hopes that the DNI could use those authorities to better integrate the IC horizontally across IC agency lines, and vertically from the federal-level to the intelligence-related entities at the state, local and tribal-levels of government.[167]

[162] See also CRS In Focus IF10470, *The Director of National Intelligence (DNI)*, by Anne Daugherty Miles.

[163] For more on this process see CRS In Focus IF10428, *Intelligence Planning, Programming, Budgeting and Evaluation Process (IPPBE)*, by Anne Daugherty Miles.

[164] E.O. 12333 §1.5.

[165] Jeffrey Richelson, *The U.S. Intelligence Community*, 6th ed. (Boulder, CO: Westview Press, 2012), p. 470. For more on the ODNI, see "Office of the Director of National Intelligence," at http://www.dni.gov/index.php/about/organization. See also the section on the ODNI in **Appendix C**.

[166] For more on the DNI position, see CRS In Focus IF10470, *The Director of National Intelligence (DNI)*, by Anne Daugherty Miles.

[167] James Clapper, DNI, "Remarks," IATA AVSEC World Conference, October 27, 2014, Grand Hyatt Hotel, Washington D.C., at https://www.dni.gov/index.php/newsroom/speeches-and-interviews/202-speeches-interviews-2014/1127-remarks-as-delivered-by-the-honorable-james-r-clapper-director-of-national-intelligence.

The IRTPA strengthened the DNI's budget authorities (in relation to department secretaries) by providing certain powers to control spending and participate in the budget process. For example, the IRTPA:

- authorizes the DNI to "develop and determine" the NIP budget, based on budget proposals provided by IC elements heads and after obtaining the advice of the Joint Intelligence Community Council (JICC);[168]
- directs the DNI to "monitor implementation," and "ensure the effective execution of the annual budget for intelligence and intelligence related activities;"[169]
- stipulates that the Director of the Office of Management and Budget (OMB), at the exclusive direction of the DNI, may direct (*apportion*) how congressionally appropriated funds will flow from the Treasury Department to each of the cabinet level agencies containing IC elements—to better ensure that the funds are spent as directed;[170]
- stipulates that the DNI may allot appropriations directly, providing the DNI an additional opportunity to control spending at the sub-cabinet agency and department level;[171]
- requires the DNI to notify Congress if a departmental comptroller refuses to act in accordance with a DNI spending directive;[172]
- provides the DNI with enhanced "transfer and reprogramming authority."[173]
- permits the DNI, with OMB approval, to transfer or reprogram funds and personnel, but within certain limits;[174]
- directs the Secretary of Defense to consult with the DNI before transferring or reprogramming MIP funds;[175]

[168] P.L. 108-458 §102A(c)(1)(B) and 50 U.S.C. §3024(c)(1)(b). Previous authorities directed the DCI to "develop" (but not determine) the NIP budget. The IRTPA (50 U.S.C. §3022) established the JICC to assist the DNI in "developing and implementing a joint, unified national intelligence effort to protect national security by: (1) advising the Director on establishing requirements, developing budgets, financial management, and monitoring and evaluating the performance of the intelligence community, and on such other matters as the Director may request; and (2) ensuring the timely execution of programs, policies, and directives established or developed by the Director." According 50 U.S.C. §3022(b) JICC members include the Attorney General, the Secretaries of State, Defense, Treasury, Energy and Homeland Security, and others designated by the President.

[169] P.L. 108-458 §102A and 50 U.S.C. §3024(c)(4).

[170] P.L. 108-458 §102A and 50 U.S.C. §3024(c)(5). The DNI could, for example, decide to withhold funds until recipients comply with DNI spending priorities, a possibility never available to DCIs. The role of OMB is discussed more fully in the "NIP and MIP Budget Process (IPPBE and PPBE)" section below.

[171] P.L. 108-458 §102A and 50 U.S.C. §3024(c)(5).

[172] P.L. 108-458 §102A(1)(c)(7)(B).

[173] Reprogramming is the shifting of funds within an appropriations account to use them for purposes other than those contemplated at the time of appropriation; it is the shifting of funds from one object class to another within an appropriation or from one program activity to another. Transfers shift budgetary resources from one appropriations or fund account to another. For more on this topic see CRS Report R43098, *Transfer and Reprogramming of Appropriations: An Overview of Authorities, Limitations, and Procedures*, by Michelle D. Christensen. See also See Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), pp. 5-3, 5-4, and 6-16.

[174] P.L. 108-458 §102A and 50 U.S.C. §3024(d). For example, the DNI can annually reprogram or transfer up to $150 million, provided that sum is less than 5 percent of the affected agency or department's budget, and the he DNI must consult with the Director of OMB and the head of the affected agency before acting.

[175] P.L. 108-458 §102A and 50 U.S.C. §3024(d)(1)(B).

- directs the DNI to consult with the Secretary of Defense to ensure that defense NIP program budgets are adequate to satisfy the national intelligence needs of the DOD."[176]
- stipulates that the DNI serve as the exclusive milestone decision authority on major IC acquisitions;[177] and
- directs the DNI to determine, coordinate, and consolidate "services of common concern."[178]

Intelligence Community Directive (ICD) 104 provides additional information on the DNI's roles and responsibilities as program executive of the NIP.[179] According to this policy document, the DNI duties include the following:

- designate NIP Program Managers;
- develop and determine the parameters of NIP programs;
- develop and determine the NIP budget, and in doing so:
  - provide guidance to the heads of IC elements,
  - receive guidance from the cabinet secretaries who have IC elements in their departments, and from the DCIA; and
- manage NIP appropriations.

The MIP is managed by the USD(I) in coordination with the DNI. **Figure 2** illustrates their shared authorities. The IRTPA directed the DNI to (1) participate in the development of the MIP, and (2) provide guidance to MIP managers in the development of their annual MIP budgets.[180]

Under Secretary of Defense for Intelligence (USD(I))/Director of Defense Intelligence (DDI)

The IRTPA authorizes the Secretary of Defense to develop the MIP budget and directs him or her to "consult" with the DNI before transferring or reprogramming MIP funds.[181] The MIP is managed by the USD(I) *on behalf of* the Secretary of Defense.[182] The position of USD(I) was created in 2002 by then-Secretary of Defense Donald Rumsfeld. The USD(I) was made "Principal

[176] P.L. 108-458 §102A and 50 U.S.C. §3024(p).

[177] P.L. 108-458 §102A and 50 U.S.C. §3024(q). The DNI's authority is limited only insofar as the acquisitions concern DOD programs. In this instance, he must share the authority with the Secretary of Defense. A "milestone authority" is a term associated with the individual who has overall responsibility for a program. The milestone authority has the authority to approve entry of an acquisition program into the next phase of the acquisition process and is accountable for cost, schedule, and performance reporting to higher authority, including congressional reporting. For more on the acquisition process in general and the DOD in specific, see CRS Report RL34026, *Defense Acquisitions: How DOD Acquires Weapon Systems and Recent Efforts to Reform the Process*, by Moshe Schwartz.

[178] P.L. 108-458 §102A and 50 U.S.C. §3024(r).

[179] ICD 104, "National Intelligence Program (NIP) Budget Formulation and Justification, Execution, and Performance Evaluation," April 30, 2013, at http://www.dni.gov/files/documents/ICD/ICD%20104.pdf.ICD 104 also outlines the roles and responsibilities of the Assistant DNIs who manage the NIP budget process, particularly the role of the Chief Financial Officer (CFO). See also ICD 116, "Intelligence Planning, Programming, Budgeting and Evaluation," September 14, 2011, at https://www.dni.gov/files/documents/ICD/ICD_116.pdf.

[180] P.L. 108-458 §102A and 50 U.S.C. §3024(c).

[181] P.L. 108-458 §102A and 50 U.S.C. §3024(d).

[182] The position of USD(I) was created by the National Defense Authorization Act for FY2003 (P.L. 107-314 §901).

Staff Assistant (PSA) and advisor to the Secretary of Defense and Deputy Secretary of Defense regarding intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters."[183]

The USD(I) position is *dual-hatted*[184]—the incumbent acting as both the USD(I) within the Office of the Secretary of Defense, and Director of Defense Intelligence (DDI) within the Office of the DNI.[185] When acting as the USD(I), the incumbent reports directly to the Secretary of Defense and serves as the Secretary's principal advisor regarding defense intelligence matters. When acting as DDI, the incumbent reports directly to the DNI and serves as his principal advisor regarding defense intelligence matters. Working together, the USD(I)/DDI and DNI oversee a number of interagency activities designed to facilitate the seamless integration of NIP and MIP intelligence efforts. **Figure 2** illustrates their overlapping and complementary authorities. **Figure G-1** (**Appendix G**) illustrates a number of the ways in which NIP and MIP integration takes place.

The section in DOD Directive 5143.01 pertaining to the USD(I)'s role as "MIP Executive" lists the following responsibilities:

- provide perspectives and forecasts on threats and the impact of resource decisions, identifies priorities, proposes programmatic and fiscal guidance, and develop budget justification material;
- provide policy guidance and oversight to the DOD components within the MIP and NIP;
- coordinate with the ODNI to develop, synchronize, and implement annual NIP and MIP priorities; and
- consult and coordinate with the Under Secretary of Defense (Comptroller)/Chief Financial Officer on MIP budgetary matters, and the DNI on MIP and NIP budgetary matters.[186]

Each military service dedicates resources to "Battlespace Awareness" (BA)—the ability to understand the disposition and intentions of potential adversaries as well as the characteristics and conditions of the operational environment. The USD(I) is responsible for policies and funds associated with the Battlespace Awareness Capability Portfolio. Capability portfolios represent one way in which the DOD manages its DOD-wide assets and activities in order to reduce overlap and duplication. The BA portfolio consists of systems or programs whose primary mission is not intelligence, but has a secondary mission to provide intelligence while conducting its primary mission. For example, the MQ-1 and MQ-9 aircraft have been procured by the Air Force for their strike capability, but their sensor suites collect intelligence before, during, and after the strike making it an "Other DOD" program of interest to the BA Portfolio. The BA

[183] For more on USDI roles and responsibilities, see DOD Directive 5143.01, *Undersecretary of Defense for Intelligence*, first issued November 25, 2005, last updated April 22, 2015, at http://fas.org/irp/doddir/dod/d5143_01.pdf.

[184] Senior executives are often referred to as *dual-hatted, triple-hatted*, and so on, when they are charged with a number of different roles and responsibilities and associated titles.

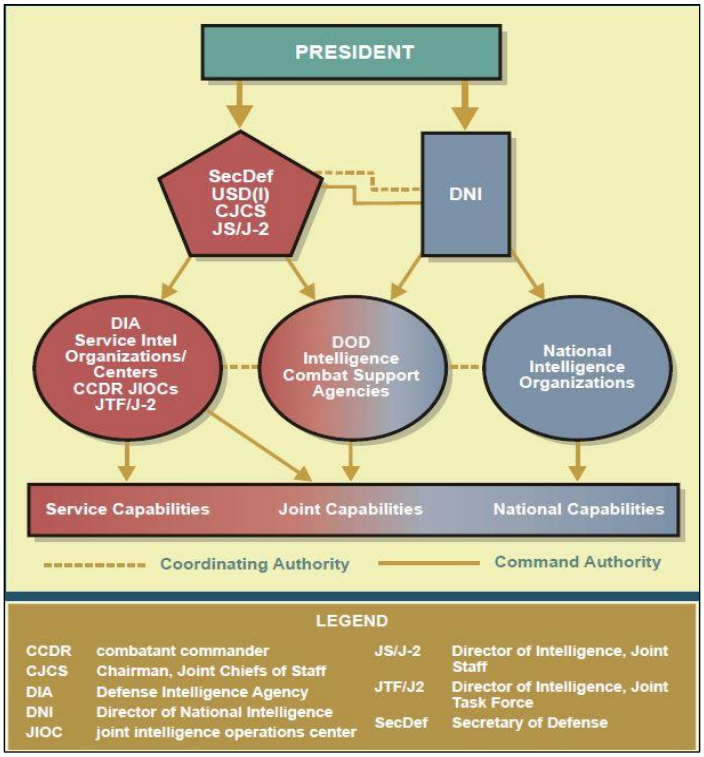
[185] See Michael McConnell, DNI and Robert Gates, Secretary of Defense, "Memorandum of Agreement," May 2007, *news release* no. 637-07, May 24, 2007, "Under Secretary of Defense for Intelligence to be Dual-Hatted as Director of Defense Intelligence," at http://www.defense.gov/Releases/Release.aspx?ReleaseID=10918. See also ODNI, "Under Secretary of Defense for Intelligence to be Dual-Hatted as Director of Defense Intelligence," news release, May 24, 2007, at https://www.dni.gov/index.php/newsroom/press-releases/172-press-releases-2007.

[186] DOD Directive 5143.01 (3) (p)(2).

Portfolio manager must consider these programs within the portfolio trade space, as their capabilities may be duplicative of MIP programs. [187]

Non-intelligence funds associated with the BA portfolio are classified and are not included in the NIP. (They are included in the DOD budget.) In 2014, then-USD(I) Vickers testified: "The BA portfolio includes significant additional resources. Defense Intelligence collectively encompasses the defense portion of the National Intelligence Program (NIP), the MIP and the BA portfolio."[188]

Figure 2. Authorities of the DNI and USD(I)



Source: Figure A-3, Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, January 5, 2012, p. A-12.

Program and Component Managers

There is often confusion among IC professionals and observers over how the positions of Program and Component Manager are related to the positions of IC functional manager, IC element head, and other management titles. In fact, the same individual may wear all of these *hats* and more. The position titles confer different requirements and authorities. **Table E-1** (**Appendix E**) provides a table listing IC leaders in terms of a number of their management titles.

NIP Program Managers exercise daily control over the intelligence resources (manpower and dollars) associated with national-level IC capabilities in accordance with DNI guidance and

[187] CRS interview with USD(I) professional, September 13, 2016.

[188] Michael Vickers, Statement for the Record, HASC Subcommittee on Intelligence, Emerging Threats and Capabilities, April 4, 2014, at http://docs.house.gov/meetings/AS/AS26/20140404/102043/HHRG-113-AS26-Wstate-VickersM-20140404.pdf.

policy.[189] A Program Manager is responsible for the program's annual budget and oversees the expenditure of the funds allocated to the program. The Program Managers whose funds span several agencies consolidate and prioritize budget and manpower inputs. Intelligence Community Directive (ICD) 104 provides overall policy on the NIP budget process to include a description of the Program Manager's roles and responsibilities.[190]

MIP Component Managers are responsible for managing intelligence resources associated with tactical-level service-specific IC activities in accordance with USD(I) guidance and policy.[191] Their specific management duties include:

- responding to guidance from the USD(I);
- aligning resources within in the MIP—i.e., adding, moving, removing programs, functions, and activities to and from the MIP;
- monitoring performance of doctrine, organization, training, materiel, leadership and education, personnel and readiness, and facilities for assigned tasks as they pertain to the MIP; and
- serving as a members of the ISR Intelligence Council (ISRIC).[192]

IC functional managers are associated with managing IC-wide intelligence disciplines like signals and geospatial intelligence—developing future capability requirements, plans, strategy, doctrine, policy, and directives for the entire intelligence enterprise.[193] The IC-wide duties of functional managers may include advising other IC element heads on uniform policies and procedures, determining collection capabilities and gaps, and developing technical architectures.[194] As an example, Robert Cardillo, Director of NGA has explained his functional manager responsibilities this way:

> As the functional manager for GEOINT, I oversee the formulation of current and future GEOINT requirements and evaluate the performance of sensor systems to meet those needs. As I look to the future, our task is less about finding the proverbial needle in a haystack, but finding — and then holding at risk — one particular needle in a stack of needles…. We must sustain the spatial and temporal access to ensure our customers understand and can respond to adversaries that continue to evolve and adapt.[195]

---

[189] IC Directive 104, "National Intelligence Program (NIP) Budget Formulation and Justification, Execution, and Performance Evaluation," April 30, 2013, at http://www.dni.gov/files/documents/ICD/ICD%20104.pdf.

[190] ICD 104, "National Intelligence Program (NIP) Budget Formulation and Justification, Execution, and Performance Evaluation," April 30, 2013, at http://www.dni.gov/files/documents/ICD/ICD%20104.pdf.

[191] DOD Directive 5205.12 (3) (c). According to this directive, 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.

[192] DOD Directive 5205.12 Enclosure 2 (8). For more on the ISR Council, 10 U.S.C. §426.

[193] The IAA for FY2014 §306 codifies the 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. See also IC Directive 113, "Functional Managers." At present, the functional managers for SIGINT, HUMINT (and OSINT), GEOINT, and MASINT are the Directors of NSA, CIA, NGA and DIA respectively. For more on IC functional managers and their associated INTs see **Appendix A** and IC Directive 113, *Functional Managers*, May 19, 2009.

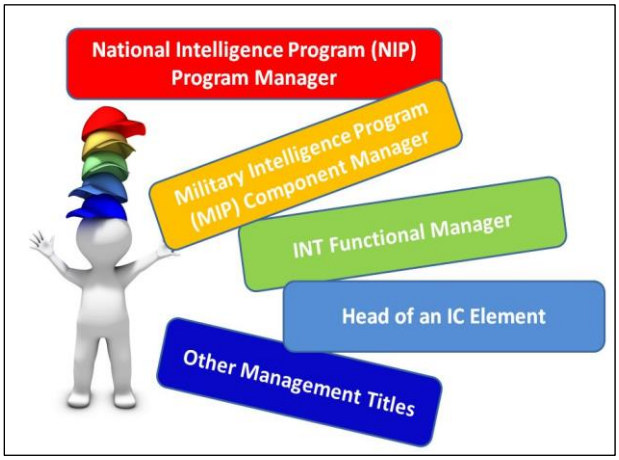
[194] E.O. 12333, "U.S. Intelligence Activities," 46 *Federal Register* 59941, (as amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)), §1.3(b)(12)

[195] Testimony of NGA Director Robert Cardillo, "Statement for the Record," in U.S. Congress, House Armed Services Committee, Subcommittee on Strategic Forces, *Fiscal Year 2016 National Security Space Hearing*, 114th Cong., 1st sess., March 25, 2015, at http://docs.house.gov/meetings/AS/AS29/20150325/103106/HHRG-114-AS29-Wstate-(continued...)

IC element heads, such as the Directors of NGA or DIA, are responsible for leading and executing the mission of their respective element. For example, the Director of DIA is responsible for ensuring that DIA is structured and manned sufficiently in order to satisfy the military and military-related intelligence requirements of the DOD and DNI.[196] They support the Functional Managers by providing function-related information, coordinating new activities or significant changes to existing function-related activities.[197]

There are a number of other management titles within the IC that fall outside the scope of this report. For example, National Intelligence Managers (NIMs) serve as the principal substantive advisors on intelligence related to designated countries, regions, topics, or functional areas.

Figure 3. Selected Intelligence Community Management *Hats*



Source: CRS

Note: The applicable management hat depends largely on the nature of the issue. For more on "IC Leaders and Selected Management 'Hats,'" see **Appendix E**.

The Director of DIA currently wears all five hats depicted in **Figure 3**.

- As Program Manager for the GDIP, the Director of DIA consolidates input from DIA, the COCOMs, and the Military Services, to produce and justify one GDIP budget request, in accordance with guidance from the DNI, and then manages the execution of those funds once they are appropriated.[198]
- As a Component Manager for DIA's MIP resources, he or she consolidates input from DIA and the COCOMs into one DIA MIP budget request, in accordance with guidance from the USD(I), and then manages the execution of those funds once they are appropriated.[199]

(...continued)

CardilloR-20150325.pdf.

[196] According to DOD Directive 5240.01, the Service Secretaries of the Air Force, Army and Navy are responsible for organizing, staffing, training and equipping the intelligence assets of the Military Departments, including CI, SIGINT, GEOINT, MASINT, and HUMINT, to support operational forces, national-level policymakers, and the acquisition community. See DODD 5240.01, "DOD Intelligence Activities," August 27, 2007, certified through August 27, 2014

[197] IC Directive 113 (F)(7), *Functional Managers*, May 19, 2009.

[198] DIA's GDIP Program office is called the Defense Intelligence Resource Management Review Office (DIRMO). It also manages DIA's MIP funds. Similarly, the Director of NSA has a CCP Program Office.

[199] The MIP requests from the Military Services go to the USD(I) separately, not through the Director of DIA.

- As Functional Manager for MASINT his or her focus is on ensuring that MASINT associated activities are standardized and integrated across the IC.
- As Director of an IC element, his or her primary focus is agency-centric, e.g., issues like DIA mission, organization and structure.
- As Joint Functional Component Commander for Intelligence, Surveillance and Reconnaissance (JFCC-ISR), he or she is responsible for ISR allocation strategic planning globally.[200]

NIP and MIP Budget Process (IPPBE and PPBE)

Management and oversight of intelligence programs is complicated by the fact that they are resourced through two separate budget processes—one entirely within the IC and one entirely within the DOD. The DNI manages the NIP budget through the Intelligence Planning, Programming, Budgeting & Evaluation Process (IPPBE) process; the MIP and its accompanying budget is managed separately by the USD(I) through the DOD's Planning, Programming, Budgeting, & Execution (PPBE) process.[201] The key players in both systems must work in concert with to facilitate the integration of NIP and MIP intelligence efforts.[202]

The DNI's Chief Financial Officer and USD(I)'s MIP Resource Manager are particularly important to the process of creating the NIP Congressional Budget Justification Books (CBJBs) and MIP Congressional Justification Books (CJBs), respectively. Both sets of books consist of a number of volumes and are classified. They are submitted to the congressional authorizing and appropriating committees each year as part of the President's Budget.[203] **Table F-1** (**Appendix F**) summarizes a number of key elements of the IPPBE and PPBE to demonstrate important similarities and differences in the two processes. **Figure G-1** (**Appendix G**) illustrates the process developed to integrate the two budget systems.

The budget documents reflect IC and DOD intelligence-related priorities, as depicted in a number of strategy documents such as the Quadrennial Defense Review, National Security Strategy, National Military Strategy, National Intelligence Priorities Framework (NIPF) and National Intelligence Strategy. The NIPF is the IC's current classified system for rank ordering intelligence requirements.[204] Overseers within the executive and legislative branches try to ensure analytically based, fiscally constrained resource decisions within the context of these types of overarching policy documents.

Within the Executive Office of the President, the Office of Management and Budget (OMB) issues fiscal guidance for agency budget development—as part of the normal federal budget process. Guidance on the NIP goes to the ODNI, and guidance on the MIP goes through the Office of the Secretary of Defense (OSD) to the USD(I).[205] Negotiations are at the NIP top-line

[200] For more on this position see Factsheet on "Joint Functional Component Commander for Intelligence, Surveillance and Reconnaissance (JFCC-ISR)," U.S. Strategic Command, at https://www.stratcom.mil/factsheets/6/JFCC_ISR/. See also Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, January 5, 2012, p. II-15.

[201] For more on the PPBE, see CRS In Focus IF10429, *Defense Primer: Planning, Programming, Budgeting and Execution Process (PPBE)*, by Lynn M. Williams.

[202] For more on the IPPBE, see CRS In Focus IF10428, *Intelligence Planning, Programming, Budgeting and Evaluation Process (IPPBE)*, by Anne Daugherty Miles.

[203] For more on the congressional portion of the IPPBE and PPBE processes, see Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Enterprises, 2014).

[204] For more on the NIPF, see IC Directive 204, *National Intelligence Priorities Framework*, January 2, 2015.

[205] Gordon Adams, "The Office of Management and Budget: The President's Policy Tool," Chapter Three, pp 55-78, in (continued...)

level, not at the individual component level. OMB may also issue/negotiate guidance in key areas (e.g., counterterrorism, information sharing, cyber security, and so on.) OMB budget examiners review component budget submissions along with ODNI and USD(I) and ultimately provide guidance to the DOD and IC through *passback*.[206]

Once the budget goes to the Congress, OMB works with the agencies to defend their budgets while legislation is drafted, debated, passed and signed by the President. OMB may send Statements of Administration Policy (SAP) to Capitol Hill designed to shape the final contents of legislation. SAPs typically outline what the Administration likes least and most about pending legislation. OMB apportions funds that have been appropriated by Congress and reapportions when necessary. It reviews and approves agency transfers and reprogramming notifications, and holds mid-year execution reviews with ODNI and OSD.[207]

Recall from the earlier section on the DNI, that the IRTPA stipulates that at the DNI's exclusive direction, the Director OMB shall apportion the flow of congressionally appropriated funds from the Treasury Department to each of the Cabinet level agencies containing IC elements. If an agency fails to comply with certain of the DNI's priorities, the DNI can withhold that agency's funding. The DNI is also authorized to "allot" or "allocate" appropriations directly at the sub-Cabinet agency and department level. If a departmental comptroller refuses to act in accordance with a DNI spending directive, the law requires that the DNI notify Congress of such refusal.[208] OMB apportions funds to OSD where they go directly to the ODNI's Chief Financial Officer (CFO) (they *pass through* OSD to the ODNI).

Congressional Action

Congressional Overseers of IC Programs

Prior to the creation of the intelligence committees in the 1970s, oversight of the IC relied on formal and informal communication and collaboration among disparate standing committees.[209]

(...continued)

The National Security Enterprise, Edited by Roger George and Harvey Rishikof, (Washington D.C.: Georgetown U. Press, 2011).

[206] *Passback* is OMB's response to the agency's request. OMB examiners say that they can be an agency's "harshest critic and biggest advocate." For more on *passback*, see CRS Report R42633, *The Executive Budget Process: An Overview*, by Michelle D. Christensen.

[207] CRS Report R42633, *The Executive Budget Process: An Overview*, by Michelle D. Christensen. OMB can use footnotes to place restrictions on the spending of obligated funds until certain conditions are met. OMB can use the budget authority "carrot" to force some kind of action from a reluctant bureaucracy. This type of use of OMB footnotes makes their use similar to that of *fences* in legislative language.

[208] P.L. 108-458 §102A and 50 U.S.C. §3024(c)(5).

[209] Prior to 1975, other key players included the House and Senate Appropriations Committees (HAC and SAC), Judiciary Committees (HJC and SJC), what was then known as the House International Relations Committee (HIRC) and is now known as the House Foreign Affairs Committee (HFAC), and the Senate Foreign Relations Committee (SFRC). The HJC and SJC had responsibility for the FBI and "questions of law." (House precedents state that the Judiciary Committee "reports on important questions of law relating to subjects naturally within the jurisdiction of other committees." *Hinds' Precedents*, Vol. IV, §4063.) The HIRC and SFRC had responsibility for the Department of State and its intelligence-related activities. The Hughes-Ryan Amendment, enacted in 1974, gave additional intelligence oversight authorities to the HIRC and SFRC because the act required that any presidential "finding" that a covert operation was necessary to national security must be reported to "congressional intelligence committees"—defined at that time to include the foreign relations committees. For more background see Frank J. Smist, *Congress Oversees the Intelligence Community*, 2nd ed. (Knoxville: U. of Tennessee Press, 1994); Britt Snider, *The Agency and the Hill: CIA's Relationship with Congress 1946-2004*, (Washington D.C.: CIA's Center for the Study of Intelligence, (continued...)

Oversight responsibilities for intelligence in general, and the Central Intelligence Agency (CIA) in particular, belonged primarily to the HASC and SASC. The HASC and SASC had legislative jurisdiction over all intelligence-related activities (national- or tactical-level).[210]

The SSCI and HPSCI were established in 1976 and 1977, respectively, to better integrate (not replace) the interests, responsibilities, and depth of intelligence-related expertise of all the intelligence-related standing committees and to respond to perceptions of widespread abuse by certain intelligence agencies.[211] One goal was consolidated authority over the entire IC and enhanced collaboration among oversight committees.[212] Another goal was 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."[213]

Many committees have jurisdictional claims to oversight on IC-related topics, not only because IC elements are spread across so many separate Cabinet departments within the executive branch, but also because some IC-related topics challenge fundamental principles such as privacy and human rights. Currently, based on House and Senate rules, only the House Permanent and Senate Select Committees on Intelligence (HPSCI and SSCI),[214] House and Senate Armed Services Committees (HASC and SASC) and House and Senate Appropriations Committees (HAC and SAC) either authorize or appropriate funding for IC programs.[215] Committees like the Judiciary, Foreign Affairs/Relations, and Homeland Security Committees tend to draft freestanding, intelligence-related legislation. The Judiciary Committees take the lead on legislation concerning domestic surveillance that affects the policies and procedures of the entire IC—the USA PATRIOT Act,[216] for example.[217]

(...continued)

2008); and Loch Johnson, *A Season of Inquiry* (Lexington, KY: University Press of Kentucky, 1985).

[210] Frank Smist, *Congress Oversees the Intelligence Community*, 2nd ed. (Knoxville: U. of Tennessee Press, 1994), p. 5.

[211] See U.S. Congress, Senate, *A resolution to establish a Standing Committee of the Senate on Intelligence Activities*, 94th Cong., 2nd sess., S.Res. 400, May 19, 1976; and U.S. Congress, House, *Resolution to amend the Rules of the House of Representatives and establish a Permanent Select Committee on Intelligence*, 95th Cong., 1st sess., H.Res. 658, July 14, 1977.

[212] To enhance communication between committees, committee membership rules called for representation of four standing committees dealing with intelligence on the select committees—Armed Services, Judiciary, International Affairs/Foreign Relations, and Appropriations—the so-called "crossover members."

[213] U.S. Congress, Senate, *A resolution to establish a Standing Committee of the Senate on Intelligence Activities*, 94th Cong., 2nd sess., S.Res. 400, May 19, 1976, §1.

[214] The "congressional intelligence committees," as defined in 50 U.S.C. §401a (6), consist of the SSCI and HPSCI.

[215] When discussing the jurisdiction of congressional committees, there is a difference between oversight jurisdiction and legislative jurisdiction related to subject matter referral. Oversight jurisdiction refers to the authority of a committee to review, investigate, or monitor an agency, operation, or program. Subject matter referral encompasses a panel's authority to report legislation or have introduced measures referred to it. The House and Senate Parliamentarians are the definitive authorities on questions relating to the jurisdiction of congressional committees. For specifics, see CRS Report 98-175, *House Committee Jurisdiction and Referral: Rules and Practice*, by Judy Schneider, and CRS Report 98-242, *Committee Jurisdiction and Referral in the Senate*, by Judy Schneider.

[216] P.L. 107-56, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.

[217] Based on interviews with committee staffers, the more an issue overlaps with a committee's key mission, the more the committee asserts its jurisdictional equities. In essence, the Judiciary Committees tend to focus on all things considered "legal issues." The Justice Department falls within their jurisdiction and thus the FBI and DEA intelligence (continued...)

The SSCI and HPSCI serve a similar function but are not mirror images of one another. They are different in numerous ways, to include organizational structure, membership, term limits, and their jurisdictions over intelligence budgets. In the years since their creation, the HPSCI and SSCI have had exclusive jurisdiction over authorizing the portion of the NIP budget that pertains to the CIA and the Office of the DNI (ODNI), but beyond those two areas, budget authorizing jurisdiction has been shared with the armed services committees.[218]

NIP funding is authorized in the annual Intelligence Authorization Act (IAA). Currently, the HPSCI asserts exclusive jurisdiction over the NIP but that is not true of the SSCI. The SSCI shares jurisdiction over defense NIP with the SASC. MIP funding is authorized as part of the HASC and SASC's annual National Defense Authorization Act (NDAA) process. The HPSCI participates in the NDAA conference process on MIP-related matters, but the SSCI does not. MIP authorizations are included in the classified Schedule of Authorizations accompanying both the NDAA and IAA.[219]

Authorization and Appropriation (*A&A*)

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 [appropriated] 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."[220] 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."[221] If and when intelligence authorization bills fail to pass, the IC relies on

(...continued)

components. More broadly focused than just FBI and DEA, the Judiciary committees consider any IC activity that potentially violates U.S. law to be within their jurisdiction. The HFAC and SFRC focus on foreign policy and therefore the State Department is its primary agency of concern. They are particularly interested in intelligence oversight when embassies are concerned, or when the United States is considering specific policy actions such as sanctions or humanitarian intervention. The House Committee on Homeland Security and the Senate Homeland Security and Governmental Affairs Committees (HCHS and SHSGAC) are particularly interested in any domestic uses of intelligence.

[218] Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), p. 8-1. The CIA and ODNI are independent agencies and fall under no Cabinet Department.

[219] Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), p. 8-1.

[220] S.Res. 400, §12; H.Res. 658, §11(I). (Both resolutions provided an exception for continuing appropriations bills or resolutions.) See Dan Elkins, *Managing Intelligence Resources*, 4th Edition, (Dewey, AZ: DWE Press, 2014), p. 7-8.

Separate and distinct from one another, the authorization and appropriations processes determine budget authority for agencies and programs. The authorization committees provide the legal authority for action. An authorization can establish or continue a federal agency, program, policy, project, or activity. Further, it may establish policies and restrictions and deal with organizational and administrative matters. It may also, explicitly or implicitly, authorize subsequent congressional action to provide appropriations. By itself, however, an authorization does not provide funding for government activities. 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. For more on this topic, see CRS Report R42098, *Authorization of Appropriations: Procedural and Legal Issues*, by Jessica Tollestrup and Brian T. Yeh.

[221] 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). According to the H. Rept. 99-106 (Part 1) to accompany H.R. 2419 (which became P.L. 99-169), p. 8: "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 (continued...)

language in appropriation bills that both authorizes and appropriates funds, until such time as an authorization bill is passed;[222]

In terms of process, each year the House and Senate intelligence committees receive the NIP and MIP budget justification books (CBJBs and CJBs) from which they produce their respective versions of an Intelligence Authorization Act (IAA). Each committee produces an unclassified bill, an unclassified report, and a classified "Schedule of Authorizations" (included within the "Classified Annex," or simply "the Annex") that provide detailed guidance to the nation's intelligence agencies. The Annex contains the schedule of authorization budget numbers as well as committee guidance and requirements that directly pertain to the classified material and may not be disclosed publicly.[223] Committee reports state that the Schedule of Authorizations "is incorporated by reference in the Act and has the legal status of public law."[224] Both intelligence committees make the Annex available for review by Members of their respective chambers.[225]

Following passage of these bills, a conference process resolves the various differences between the House and Senate versions. In recent years the conference process has been informal—consisting primarily of staff-level discussions comparing the two versions of the bill and seeking common ground for settling whatever differences exist. After initial staff discussions, the House and Senate committee leaders may become involved. If these informal and unofficial conversations appear productive, they may continue until a tentative agreement is reached, even though no conference committee has yet been created. If the tentative agreement proves acceptable to other interested Representatives and Senators, a formal conference committee may be unnecessary.[226]

The IAA for FY2016 was remarkable in terms of final bill passage. It was signed into law as part of the "Consolidated Appropriations Act of 2016," P.L. 114-113 (Division M)—marking the first

(...continued)

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." 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.

[222] See, for example, language in P.L. 110-116 §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."

[223] U.S. Congress, House Permanent Select Committee on Intelligence, *Intelligence Authorization Act for FYs 2014-2015*, report to accompany H.R. 4681, May 27, 2014, 113th Cong., 2nd sess., H.Rept. 113-463 (Washington D.C.: GPO, 2014), p. 18.

[224] 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), pp. 1-2: "Other than for limited unclassified appropriations, primarily the Intelligence Community Management Account, the classified nature of United States intelligence activities precludes any further disclosure, including by the Committee, of the details of its budgetary recommendations. Accordingly, the Committee has prepared a classified annex to this report that contains a classified Schedule of Authorizations. The classified Schedule of Authorizations is incorporated by reference in the Act and has the legal status of public law. The classified annex is made available to the Committees on Appropriations of the Senate and the House of Representatives and to the President. It is also available for review by any Member of the Senate subject to the provisions of Senate Resolution 400 of the 94th Congress (1976)."

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

[226] For more on the conference process, see CRS Report 98-696, *Resolving Legislative Differences in Congress: Conference Committees and Amendments Between the Houses*, by Elizabeth Rybicki.

time in the history of congressional intelligence committees that the intelligence authorization act was part of an appropriations bill, not a freestanding intelligence authorization bill, debated as such, in both chambers of Congress.[227]

When the authorization and appropriation match, the IC budget community colloquially refers to it as an *A & A*; when they do not match, it is an *A not A*.[228] Discrepancies between what is authorized and what is appropriated (*A not A*) may reflect committee policy disagreements or may simply occur because the authorization and appropriation processes are separate. There is no conference process to resolve differences between the separate authorization and appropriation bills. The IC has a number of procedures in place to deal with authorization and appropriation discrepancies. For example:

- if the appropriation *is greater than* the amount authorized, the IC needs permission from the authorizers to spend the additional amount;
- if the appropriation *is smaller than* the amount authorized, the program may be able to operate at the level dictated by the smaller appropriation; and
- if the appropriation *lacks any matching authorization*, it will either be terminated or not allowed to begin, unless the agency is able to convince the authorizing committees to authorize the program retroactively.[229]

Enduring Issues

Based on the FY2017 President's Budget request, the IC programs discussed in this report currently equate to approximately $70 billion dollars (or roughly 11%) of national defense spending.[230] Observers point to a number of issues that may affect the ability of IC and DOD leadership to make the best use of those resources. [231] To conclude this report, this section addresses issues associated with IC-wide integration, transparency and balance.

Integration

Integrating NIP and MIP Budget Processes

The IPPBE and PPBE processes are overseen, managed, organized and structured differently. For example, the PPBE relies on program elements as its basic building blocks while the IPPBE relies on expenditure centers. The PPBE is organized around the military services while the IPPBE is organized around capabilities. (See **Appendix F** for a side-by-side comparison of the IPPBE and PPBE.) It is unclear to what degree the integrated IPPBE/PPBE processes may help or hinder efficient management of IC programs but an illustrative example such as the joint IC/DOD

[227] For more on the inclusion of legislative provisions in omnibus appropriations acts, see CRS Report RL32473, *Omnibus Appropriations Acts: Overview of Recent Practices*, by James V. Saturno and Jessica Tollestrup.

[228] An authorization without a matching appropriation is said to be *hollow budget authority* (a colloquial term) because it has no actual resources to support the authorized activity.

[229] For more on *A&A*, and *A not A*, see Dan Elkins, *Managing Intelligence Resources*, 4th Edition, (Dewey, AZ: DWE Press, 2014), p. 7-8.

[230] See CRS Report R44381, *Intelligence Spending: In Brief*, by Anne Daugherty Miles.

[231] Problems associated with the legislative process (such as the lack of timely authorization and appropriation bills) often complicate (and/or create) a number of resource management-related issues. See for example, Jon Harper, "Secretary Carter Warns about Continuing Resolutions," *National Defense*, September 16, 2015, at http://www.nationaldefensemagazine.org/blog/lists/posts/post.aspx?ID=1958.

acquisition of a common overhead satellite architecture suggests that the joint process makes efficient use of IC-related resources difficult at best. In the case of overhead satellite architecture, congressional overseers have repeatedly raised concerns for many years.[232] A 2008 House Intelligence Committee report revealed its frustration with both the IC and DOD. It stated:

> [T]he Intelligence Community and DOD seem at odds with each other over satellite program requirements. Without adequately defining the requirements of the combatant commanders, the Air Force and Intelligence Community are forced to hit an ever-moving or invisible target in managing overhead program requirements. …. The competition between DOD and the Intelligence Community for mission-specific requirements must be better coordinated by the ODNI, USD(I) and USD(AT&L) [Under Secretary of Defense for Acquisition, Technology and Logistics].[233]

The report found that programs jointly funded in NIP and MIP, "requiring joint decisions by the DNI and DOD, result in delayed program starts."[234] Despite the findings and recommendations offered in the 2008 report, problems acquiring the overhead satellite architecture persist.

The IAA for FY2016 (P.L. 114-113, Division M, §312) requires the DNI, in collaboration with the Secretary of Defense, and the CJCS, to develop a strategy, with milestones and benchmarks, to ensure that there is a comprehensive interagency review of policies and practices for planning and acquiring national security satellite systems and architectures, including the capabilities of commercial systems and partner countries, consistent with the National Space Policy issued on June 28, 2010. Where applicable, this strategy is to account for the unique missions and authorities vested in the DOD and IC. The provision has a lengthy explanation in the accompanying Senate Report. The views of Senators Warner, King, Rubio, Hirono, and Mikulski echo the HPSCI findings published in 2008:

> Satellite systems and architectures should also be designed in such a way that a number of elements common to multiple spacecraft could be standardized, to reduce costs, simplify execution and preserve a competitive industrial base; and the entire overhead satellite architecture of the United States, including programs funded by the Department of Defense or by an element of the intelligence community, commercial providers, and foreign partners, should be viewed and treated as an integrated whole, not simply as a series of independent and unrelated satellite systems.[235]

[232] U.S. Congress, House Permanent Select Committee on Intelligence, *Report on the Challenges and Recommendations for United States Overhead Architecture*, 100th Cong., 2nd sess., H.Rept. 110-914, October 3, 2008 (Washington D.C.: GPO, 2008), p. 6: "The Committee has raised many of these issues before.… [T]he Administration appears to have ignored the language in multiple intelligence authorization bills." This issue was chosen because it is one of the few programs jointly funded by NIP and MIP that is publicly discussed in unclassified congressional documents.

[233] U.S. Congress, House Permanent Select Committee on Intelligence, *Report on the Challenges and Recommendations for United States Overhead Architecture*, 100th Cong., 2nd sess., H.Rept. 110-914, October 3, 2008 (Washington D.C.: GPO, 2008), p. 11.

[234] Ibid, p. 2.

[235] U.S. Congress, Senate Select Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 2016*, 114th Cong., 1st sess., S.Rept. 114-83 to accompany S. 1705, July 16, 2015, Additional Views of Senators Warner, King, Rubio, Hirono, and Mikulski, p. 12.

Coalition of the Willing[236]

It is unclear how well the NIP and MIP programs are structured to handle IC-wide programs like the IC's information technology (IT) modernization effort—the IC Information Technology Enterprise (IC ITE).[237] IC ITE is focused 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 pool IT resources, cut costs, increase data storage capabilities, increase mission agility and efficiency, and increase the ability to protect all levels of data.[238] However, IC ITE does not belong to any one agency, and is not a collection capability like the *INTs.* Thus adequate funding may depend more on voluntary contributions—*a coalition of the willing*—than on DNI budgetary authorities. As all resources are finite, money used for IC ITE means less money available for agency-specific priorities.

Coalition of the willing is also heard in reference to agencies like DHS that contain a number of autonomous intelligence-related activities. While many DHS components are engaged in strategic intelligence activities, there is no mandated coordination of such activities within DHS because they are not NIP funded. Coordination and collaboration appears to be based more often on the relationships between key players than on department regulations.

Transparency

Total intelligence-related spending is almost impossible to calculate and its management and oversight is completely decentralized. IC funding alone is divided into two budget categories. The NIP and MIP are managed within the executive branch separately, justified to Congress separately, and overseen by congressional committees separately. IC programs fund only a portion of intelligence activities in the U.S.[239]

Intelligence-related programs that are not part of the IC include, for example, the large Office of Intelligence within DHS's Immigration and Customs Enforcement (ICE) division. The ICE Office of Intelligence is not included in the IC because theoretically, ICE activities primarily support the DHS mission to protect the homeland. The IC does not include state or local intelligence-related entities such as the New York Police Department's (NYPD's) Intelligence Division & Counter-Terrorism Bureau because of the NYPD's focus on domestic law enforcement.

Furthermore, there is no one source that provides a list of all intelligence-related programs in the U.S. government. A 2008 RAND study written by IC expert Gregory Treverton includes a graphic that attempts to illustrate and link the hundreds of organizations spread across the federal government that comprise the *Domestic Intelligence Enterprise*.[240] A 2010 investigation by *Washington Post* journalists Dana Priest and William Arkin reported that there are "3,984 federal,

[236] "Coalition of the willing" generally refers to an alliance where members agree to collectively work toward some commonly defined goal. While it was originally associated with group of allied countries in a military intervention, especially the United States and its allies in the Iraq War, it is currently used to describe any alliance of willing participants.

[237] IC ITE is commonly pronounced as "eyesight."

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

[239] For more on IC spending, see CRS Report R44381, *Intelligence Spending: In Brief*, by Anne Daugherty Miles.

[240] Gregory Treverton, "Reorganizing U.S. Domestic Intelligence: Assessing the Options," *Monograph*, RAND Corporation, 2008, Figure B.1, at http://www.rand.org/pubs/monographs/MG767.html. Gregory Treverton is currently the Chairman of the National Intelligence Council.

state and local organizations working on domestic counterterrorism."[241] Priest and Arkin describe some of the difficulties associated with calculating the cost of such programs:

> The Department of Homeland Security [DHS], for example, does not know how much money it spends each year on what are known as state fusion centers, which bring together and analyze information from various agencies within a state.... [T]the bulk of the spending every year comes from state and local budgets that are too disparately recorded to aggregate into an overall total.[242]

Furthermore, congressional oversight is distributed across a number of committees. Committee interactions with IC officials occur generally in closed sessions for any discussion of program or operation specifics. Classified transcripts are maintained by the committees and are made available on a limited basis to Members of Congress. Since there is no automatic declassification system for congressional documents, it is unclear if, or when, such materials will become available to the public.

Financial Auditability

There is a 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 first stipulated that 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.[243] 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.[244]

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

> 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 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 [Business Transformation Office] 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

[241] Dana Priest and William Arkin, "Top Secret America: Monitoring America," *Washington Post*, July 20, 2010, at http://projects.washingtonpost.com/top-secret-america/.

[242] Ibid.

[243] U.S. Congress, Senate Select Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 2002*, Report to accompany S. 1428, 107th Cong., 1st sess., September 14, 2001, S.Rept. 107-63, p. 16.

[244] 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.

> would provide valuable macro-level data and, once established, offer insight into financial trends within the Intelligence Community.[245]

The IAA for FY2014 (P.L. 113-126 §309) directs the DNI and the Directors of the, CIA, DIA, NSA, NRO, and NGA to undergo full financial audits beginning with FY2014 financial statements. How well the agencies are meeting this requirement is unclear.

Balance

In the end, Congress is often faced with having to balance resources (money and manpower) and priories across many competing demands. Are the resources (both money and manpower) and priorities of the IC appropriately balanced? In a worldwide threats briefing to Congress, current DNI James Clapper listed a number of national security issues facing the United States. These included: violent extremists, migration and displaced people, government instability, cyber espionage and other cyber-related threats, state-sponsored terrorism, weapons of mass destruction, and China's and Russia's nuclear missile force and anti-satellite missile programs.[246] Theoretically, the funds dedicated to intelligence-related activities across the federal government should reflect a balance between these strategic priorities on the one hand, and resources on the other, but no one outside the IC knows how many resources are actually devoted to the many tasks at hand, or how well those resources are distributed and balanced between and within government agencies.

The NIP budget funds intelligence capabilities that support national priorities. DNI Clapper has frequently remarked that his job is to prioritize and balance resources among competing demands. In a July 2016 interview he reiterated that view:

> One of the reasons we have DNI is to prioritize and keep some balance among all the competing demands that are placed on us [the IC] because in the end, there's a finite resource here. Every year the Congress gives us so many dollars and so many people that are appropriated to us. And those are numbers, and we have to allocate those across a whole variety of threats and concerns that people have. So it is not a trivial proposition to surge from this issue this week to surge to that one next week … and so one of the things I try to do is to try to … maintain some balance because there is just so much resource… and you have to attend to all of these threats … and everything is zero sum. So if you move resources in the Intelligence Community from one problem to another, there's no bullpen of relief pitchers waiting to go into the game here because everybody is occupied. The Congress doesn't give us extra bodies to just sit around and wait until the next surge.[247]

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

[246] Office of the Director of National Intelligence, "IC's Worldwide Threat Assessment Opening Statement," February 9, 2016, pp. 1-3, at http://www.dni.gov/files/documents/2016-02-09SSCI_open_threat_hearing_transcript.pdf.

[247] Remarks of DNI James Clapper, 7th Annual Aspen Security Forum, Interview and Q&A moderated by Jim Sciutto, Chief National Security Correspondent, CNN, July 28, 2016, Video at 39 minute mark, at http://aspensecurityforum.org/media/live-video/.

Further Reading

Table 4. Selected References on IC Programs and Management

Government Policy Documents:
DOD Directive 5143.01 *Undersecretary of Defense for Intelligence*, first issued November 25, 2005, last updated April 22, 2015.
DOD Directive 5205.12. *Military Intelligence Program*, November 14, 2008, certified current through November 14, 2015.
DOD Directive 5240.01. *DOD Intelligence Activities*, August 27, 2007, certified through August 27, 2014.
Executive Order 12333. *United States Intelligence Activities,* December 4, 1981, As Amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008).
IC Directive 104. *National Intelligence Program (NIP) Budget Formulation and Justification, Execution, and Performance Evaluation*, April 30, 2013.
IC Directive 116. *Intelligence Planning, Programming, Budgeting and Evaluation Process (IPPBE)*
IC Directive 204, *National Intelligence Priorities Framework*, January 2, 2015.
Joint Publication 2-0, *Joint Intelligence*, October 22, 2013.
Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations,* January 5, 2012.
Office of the DNI. *U.S. National Intelligence: An Overview 2011*.
U.S. Code Title 10. *Armed Forces* and Title 50. *War and National Defense*
CRS Products:
CRS Report R44381, *Intelligence Spending: In Brief*, by Anne Daugherty Miles.
CRS In Focus IF10428, *Intelligence Planning, Programming, Budgeting and Evaluation Process (IPPBE)*, by Anne Daugherty Miles.
CRS In Focus IF10429, *Defense Primer: Planning, Programming, Budgeting and Execution Process (PPBE)*, by Lynn M. Williams.
CRS In Focus IF10469, *The U.S. Intelligence Community (IC)*, by Anne Daugherty Miles.
CRS In Focus IF10470, *The Director of National Intelligence (DNI)*, by Anne Daugherty Miles.
Books and Articles:
Elkins, Dan. *Managing Intelligence Resources*, 4th ed., Dewey, AZ: DWE Press, 2014.
Lowenthal, Mark, *Intelligence: From Secrets to Policy*, 6th ed, Thousand Oaks, CA: Sage/CQ Press, 2015.
Mirabello, Robert. "Budget and Resource Management," *Intelligencer: Journal of U.S. Intelligence Studies*, vol. 20, no. 2, (Fall/Winter 2013).
Richelson, Jeffrey. *The U.S. Intelligence Community*, 7th ed., Boulder, CO: Westview Press, 2016.

Note: Other than the books and articles, all references are available online. Check to ensure that you have the most current version of these documents.

Appendix A. IC Collection Disciplines

Table A-1. Intelligence Community Collection Disciplines and Functional Managers

Discipline	Functional Manager	Description	Examples
Geospatial Intelligence (GEOINT)	**NGA Director**	Interpreting and analyzing information describing, visually depicting, and accurately locating physical features and human activities on the Earth.	Still and motion images acquired through platforms such as satellites, aircraft, or unmanned aerial vehicles. Printed maps, charts, and publications; digital databases; photographs; or digitized maps and charts. Geospatial positional data using a coordinate-based system to identify the physical location and orientation of natural or man-made objects.
Imagery Intelligence (IMINT)	**NGA Director**	Imagery intelligence (IMINT) is a subset of GEOINT Interpreting and analyzing imagery and collateral materials.	Electro-optical (EO) imagery produced in the infrared, near infrared, visible, and ultraviolet spectrums. Infrared imagery derived from emissions or reflections that depict environmental thermal contrasts. Radar imagery formed from analyzing reflected radio waves. Lidar imagery derived from analyzing light reflected by aiming a pulsed laser at a remote object.
Human Intelligence (HUMINT)	**CIA Director**	Interpreting and analyzing information collected through human sources.[a] The collection of information openly (*overtly*) or secretly (*covertly*) by a human source (verbally or via a document).	Information obtained through direct and indirect questioning of overt and/or clandestine human sources. Interrogations that obtain information through questioning a captured or detained person. Debriefings that obtain information through questioning cooperative human sources such as defectors; refugees or displaced persons; or freed hostages.
Open-Source Intelligence (OSINT)	**CIA Director**	Interpreting and analyzing information that any member of the public can obtain through legal channels. OSINT processing transforms (converts, translates, and formats) text, graphics, sound, and motion video in response to user requirements.	Media reports published through newspapers, magazines, radio, online news outlets, and television channels. Social media updates published or posted to internet forums or social networking sites such as Twitter, Facebook, and YouTube. ODNI Open Source Enterprise provides translations of foreign broadcast and print media. Publicly available government information or data. Academic and professional literature, often scientific in nature, obtained through review of books, journal papers, conference presentations, working papers, and other electronic and print publications.

Discipline	Functional Manager	Description	Examples
Measurement and Signature Intelligence (MASINT)	**DIA Director**	Interpreting and analyzing scientific data or measurements derived from technical sensors or systems. Highly technical information is used to detect, and track the distinctive physical characteristics of targets and events in order to characterize and identify them.	Electro-optical (EO) data produced in the infrared (IR), near IR, visible, and ultraviolet spectrums. Radar data derived from reflected radio waves that can determine the range, angle, or velocity of remote objects. Radio frequency or electromagnetic pulse emissions associated with nuclear testing or other high energy events. Geophysical data such as acoustic, seismic, or magnetic phenomena. Material signatures associated with specific compounds or substances such as chemicals or biological materials. Detecting nuclear radiation produced by the decay of radioactive substances or by nuclear fission.
Signals Intelligence (SIGINT)	**NSA Director**	Interpreting and analyzing information derived from foreign communications systems.[b]	See COMINT, ELINT, and FISINT
Communications Intelligence (COMINT)	**NSA Director**	COMINT is a subset of SIGINT Interpreting and analyzing information derived from intercepted speech or text-based foreign communications.	Diplomatic communications between nation-states and diplomatic posts. Intragovernmental communications between government agencies and components. Communications by hostile non-state actors, such as terrorist organizations.
Electronic Intelligence (ELINT)	**NSA Director**	ELINT is a subset of SIGINT Interpreting and analyzing information derived from intercepted foreign electronic signals that do not contain speech or text.	Tracking foreign electromagnetic signal emissions from military and civilian devices such as air defense systems and radars. Identifying foreign vessels and vehicles by electromagnetic signal emissions.
Foreign Instrumentation Signals Intelligence (FISINT)	**NSA Director**	FISINT is a subset of SIGINT Interpreting and analyzing information derived from technical analysis of data intercepted from testing or operational deployment of foreign systems.	Telemetry signatures from foreign missiles or spacecraft. Foreign command and control systems. Identification friend or foe systems.

Sources: CRS, based on Joint Publication 2-0, "Joint Intelligence," October 22, 2013; ODNI, "U.S. National Intelligence – An Overview," 2013; Jeffrey T. Richelson, *The US intelligence Community* 7th ed. (Boulder, CO: Westview Press, 2015); U.S. Coast Guard, *Intelligence*, May 2010; Mark Lowenthal, *Intelligence: From Secrets to Policy*, 6th ed. (Thousand Oaks, CA: Sage/CQ Press, 2015).

Notes:

a. The Coast Guard law enforcement intelligence element personnel use the term Law Enforcement Intelligence Collection (LEIC) rather than HUMINT when describing their collection activities.

b. The Coast Guard also collects signals using law enforcement and regulatory authorities and calls them Law Enforcement Technical Collection (LETC) Activities.

c. On December 1, 1995, DCI approved declassification of "the fact of" SIGINT collection to include COMINT, ELINT and FISINT. See James P. Cavanaugh, Chief Office of Policy, "Declassification of the Fact of Overhead SIGINT -- Information Memorandum," N5P/010/96, April 10, 1996 and Bruce Berkowitz, *NRO at 50 Years: A Brief History,* Center of the Study of National Reconnaissance, NRO, September 2011, p. 26,

Appendix B. Intelligence Programs: In Brief

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

managers and brief descriptions

National Intelligence Program	
Defense NIP	
Consolidated Cryptologic Program (CCP)	The NSA Director manages the CCP. Funds NSA and intelligence activities related to national-level SIGINT and information assurance (IA) across the IC. For example, the U.S. Coast Guard has a SIGINT collection entity as do each of the military services. SIGINT collection operations target electromagnetic communication systems such as radios and cellular phones, radar, and signals emanating from foreign missile tests. Information assurance activities are designed to keep defense communications systems secure.
General Defense Intelligence Program (GDIP)	The DIA Director manages the GDIP. Funds DIA and a wide range of national-level defense intelligence activities to include: (1) the intelligence centers that support the services and unified combatant commands (e.g., the Defense Joint Intelligence Operations Center); (2) defense HUMINT; (3) biometric and identity intelligence; and (4) medical intelligence. Other examples of GDIP-funded activities include: IC Infrastructure; national-level activities related to CI; and the collection, processing and dissemination of MASINT.
National Geospatial-Intelligence Program (NGP)	The NGA Director manages the NGP. Funds NGA and national-level GEOINT-related activities throughout the IC. NGA predominately relies on overhead reconnaissance platforms to provide the raw imagery it needs to produce finished intelligence products. Examples of GEOINT products range from three-dimensional maps and charts to computerized databases. For example, "the Globe" is an NGP investment that consolidates its legacy search tools into a single enterprise search system.
National Reconnaissance Program (NRP)	The NRO Director manages the NRP. Funds NRO and NRO efforts to develop, build, launch, and operate satellites associated with "multi-INT" collection—meaning that they collect a variety of signals from FISINT, COMINT, ELINT, and various forms of MASINT. The NRP provides the IC with capability to provide intelligence on topics like imminent military aggression, early warning of foreign missile launches, battle damage assessments, tracking high-value individuals, and monitoring treaty agreements and peacekeeping operations.
Special Reconnaissance Program (SRP)	Information concerning SRP management is not available at this time. Funds procurement of special intelligence gathering devices (to include research and development), and specialized reconnaissance collection activities, in response to tasking procedures established by the DNI.
Nondefense NIP	
Central Intelligence Agency Program (CIAP)	The CIA Deputy Director manages the CIAP. Funds CIA activities to include HUMINT and OSINT. The CIAP funds everything related to the CIA. It includes funding for activities such as covert and clandestine operations, research and development of technical collection systems related to all-source analysis, operating the IC's open source center, training for analysts and agents, and operating the entire CIA infrastructure. The CIAP funded development of the U-2 spy plane, for example.

CIA Retirement and Disability System (CIARDS)	The CIA Deputy Director manages CIARDS. Funds pension benefits to a selected group of the CIA's workforce who were first hired before 1984 and were not enrolled in the Civil Service Retirement System. CIARDS is a CIA-only program, and is not part of the CIAP. It unique because its costs are driven by the number of recipients eligible as opposed to mission requirements.
Community Management Account (ICMA)	The DNI manages ICMA. Funds expenditures associated with personnel and day-to-day activities of the organizational elements that make up the ODNI. It funds the staffs of the DNI, the Principal Deputy DNI, Deputy and Associate DNIs, and all activities associated with the ODNI's mission and support activities.
Department of Energy NIP	DOE's Office of Intelligence and Counterintelligence (DOE/IN) Director manages DOE NIP. Funds analysts who provide expertise in nuclear, energy, science and technology and cyber intelligence. DOE NIP provides technically based intelligence analyses of foreign nuclear-related terrorist activities. Its counter-intelligence effort is focused on protecting its personnel, technologies, facilities, and intellectual property from foreign collection efforts (particularly cyber threats).
Department of Homeland Security NIP	The Under Secretary of DHS for Intelligence and Analysis (DHS/I&A) manages DHS Office of Intelligence Analysis (OIA) NIP. Funds analysts who provide expertise on homeland security-related topics such as U.S. critical infrastructure. OIA combines information collected by DHS components as part of their operational activities (e.g., at airports, seaports, and border) with foreign intelligence from the IC; law enforcement sources; private sector; and open sources.
	The Assistant Commandant for Intelligence and Criminal Investigations (CG-2) manages USCG NIP. Funds analysts and collection activities in order to provide expertise in all things related to illegal smuggling of weapons, drugs, and migrants.
Department of Justice NIP	The National Security Branch (NSB) Director manages Federal Bureau of Investigation (FBI) NIP. Funds counterterrorism analysts and interagency efforts such as Joint Terrorism Task Forces. FBI NIP related activities include: producing analysis designed to prevent: theft of sensitive information and advanced technologies; and use of chemical, biological, and nuclear weapons.
	The Director, Office of National Security Intelligence (ONSI) manages Drug Enforcement Agency (DEA) NIP. Funds analysts who provide expertise on drug trafficking, and drug-related criminal activities.
Department of State NIP	The Assistant Secretary of State for Intelligence and Research (AS/INR) manages State NIP. Funds analysts who provide expertise on issues as diverse as economic security, terrorist group financing, strategic arms control, political-military issues, and cyber for the Secretary of State and other key policymakers. An example of State NIP related spending is "INR Watch"—a 24-hour, seven-day-a-week center for monitoring, evaluating, alerting, and reporting time-sensitive intelligence to department and INR principals and serves as liaison to other IC operations centers.
Department of Treasury NIP	The Assistant Secretary of Treasury for the Office of Intelligence and Analysis (AS/OIA) manages Treasury NIP. Funds analysts who provide financial and economic expertise. Financial intelligence analysts focus on terrorist financing, counterfeiting, money laundering, funds transfers, weapons sales, and other national security-related financial transactions. Economic intelligence analysts focus on the strengths and vulnerabilities of national economies. OIA established joint intelligence, military, and law enforcement cells in Iraq and Afghanistan to help identify and interdict funding streams to terrorist and insurgent networks.

Military Intelligence Program	
DIA, NGA, NRO, and NSA MIP	The Directors of DIA, NGA, NRO, and NSA manage separate MIP funds. Fund those agency activities that support tactical-level operations not funded by the GDIP, NGP, NRP, or CCP, respectively. For example, the NRO uses some of its MIP funds to counter improvised explosive devices; identify and track high-value targets; and improve battlespace awareness.
OSD MIP	The USD(I) manages OSD MIP. Funds those OSD-managed special technologies programs with DOD-wide application, not funded otherwise. For example, it funds the Advanced Sensors Application Program; Foreign Materiel Acquisition and Exploitation Program, and the Horizontal Fusion Program.
U.S. Special Operations Command (SOCOM) MIP	The SOCOM Director of Intelligence (SOCOM/J2) manages SOCOM MIP. Funds analysts and activities directed toward building up SOCOM's own organic capabilities and reimbursing support from military departments. SOCOM MIP is funding several current acquisition efforts focused on outfitting aircraft—both manned and unmanned, fixed and rotary wing—with advanced ISR and data storage capabilities that will work in multiple environments.
Air Force MIP	The Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance (ISR) (AF/A2) manages Air Force MIP. Funds tactical-level systems, people and activities associated with air/space operations. Air Force ISR platforms most commonly used by air wings to collect intelligence are the RC-135, U-2, MQ-1 Predator, MQ-9 Reaper, and the RQ-4 Global Hawk.
Army MIP	The Deputy Chief of Staff for Intelligence (DCS/G-2) manages Army MIP. Funds tactical-level systems, people and activities associated with intelligence support to ground operations. Army MIP related activities include GEOINT, SIGINT, HUMINT, MASINT, and CI. Army MIP employs physicists, chemists, engineers, and other technical specialists, to analyze foreign weapon systems in order to provide intelligence on current and future foreign military armament performance and capabilities.
Navy MIP	The Director of Naval Intelligence, who also serves as the deputy Chief of Naval Operations for Information Dominance (N-2/N-6) manages Navy MIP. Funds tactical-level systems, people and activities associated with maritime operations. Navy MIP funds activities related to understanding the capabilities of foreign naval forces; foreign technologies, sensors, weapons, platforms, combat systems, and cyber capabilities; special collection and analysis for irregular and expeditionary forces; and cyberspace and cryptologic operations.
Marine Corps MIP	The Director for Intelligence (DIRINT) manages Marine Corps MIP. Funds tactical-level systems, people, and activities associated with littoral (the region along a shore) and ground operations. Marine Corps MIP funds intelligence-related activities such as intelligence preparation of the battlefield, and target analysis. It also funds activities associated with GEOINT, SIGINT, CI, and ISR.

Source: CRS, based on agency websites; Joint Publication 2-0, "Joint Intelligence," October 22, 2013; Office of the Director of National Intelligence, "U.S. National Intelligence – An Overview," 2013; Jeffrey T. Richelson, *The US intelligence Community*, 7th ed. (Boulder, CO: Westview Press, 2015); U.S. Coast Guard*, Intelligence*, May 2010, and Dan Elkins, *Managing Intelligence Resources,* 4th ed. (Dewey, AZ: DWE Press, 2014).

Note: The descriptions are not comprehensive; rather they are representative of the primary focus of each entity.

Appendix C. CIARDS and ICMA

The Central Intelligence Agency (CIA) Retirement and Disability System (CIARDS) and Community Management Account (ICMA or CMA) are seldom discussed in IC-related literature. They are unique IC programs because they were both created in statute, funding for each is disclosed in every Intelligence Authorization Act (IAA), and they are openly discussed in a number of congressional reports. For example, the IAA for FY2016 authorized an appropriation of $514 million for CIARDS and an appropriation of $516 million and 785 positions for the ICMA.[248] CIARDS is also unique within the NIP because its costs are driven by the number of recipients eligible as opposed to mission requirements.[249]

CIA Retirement and Disability System (CIARDS)

Overview

The CIA operates various retirement systems that cover its employees: the regular civil service retirement system for the majority of its employees and CIARDS. The CIA's regular civilian service retirement system includes both the Civil Service Retirement System (CSRS) and the Federal Employees Retirement System (FERS)—employee coverage depending on date of entry into federal service and by type of job performed.[250] All retirement benefits for CIA employees (CSRS, FERS or CIARDS) are administered by CIA, to protect employee personnel information.[251]

Most CIA employees first hired into federal service prior to 1984 are covered by CSRS and may be eligible for benefits identical to other CSRS covered employees in the federal government.[252] However, certain pre-1984 CIA employees were covered by CIARDS. When Congress created FERS in 1986, CIARDS, like CSRS, was closed to new entrants hired in 1984 or later. Thus, the CIARDS account applies only to those CIA employees who were covered under CIARDS (i.e., first hired before 1984).

As with other federal employees, all CIA employees who joined the agency after December 31, 1983, are covered by FERS. The FERS Act (P.L. 99-335) provided for those CIA employees, who qualified for CIARDS-like retirement, by creating two special categories known as *Section 302* and *Section 303* employees (for the applicable provisions in FERS and the Central Intelligence Agency Retirement Act of 1964 for Certain Employees, respectively). Under FERS, Section 302 and 303 employees are eligible for retirement benefits similar to those available to federal law enforcement officers.[253]

[248] P.L. 114-113 Division M. Title 50 in U.S.C. has extensive provisions for the CIARDS system.

[249] Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), p. 4-6.

[250] For more on CSRS and FERS, see CRS Report 98-810, *Federal Employees' Retirement System: Benefits and Financing*, by Katelin P. Isaacs.

[251] The Office of Personnel Management (OPM) administers CSRS and FERS benefits for non-CIA employees.

[252] Under CSRS, most employees do not pay Social Security taxes or earn Social Security benefits. Instead, they receive a defined benefit annuity (or traditional "pension").

[253] See also, CRS Report R42631, *Retirement Benefits for Federal Law Enforcement Personnel*, by Katelin P. Isaacs.

Background

The *Central Intelligence Agency Retirement Act of 1964 for Certain Employees* (CIARA) (P.L. 88-643, Title II) created CIARDS to meet the needs of certain CIA employees who were less likely than other federal employees to be in federal service long enough to qualify for CSRS retirement benefits. A Senate Armed Services Committee report accompanying CIARA explains that creating CIARDS not only addressed a CIA need, but also created equity with systems already in place for law enforcement professionals and Foreign Service officers:

> With respect to Central Intelligence Agency employees engaged in conducting and supporting intelligence activities abroad, it has been the experience of the Agency that because of the conditions of service, not all of these employees can anticipate serving the period of time required in order to retire under the civil service retirement provisions. A special retirement system is therefore needed in order for some of these employees to retire at an earlier age and with a less severe financial penalty than the present civil service system imposes. The precedents for this type of legislation may be found in the provisions now applicable to certain personnel of the Federal Bureau of Investigation and other Federal investigative and criminal detection activities, and the separate provisions now applicable to Foreign Service officers.[254]

Discussions concerning the original intent for CIARDS occurred in 1973, during hearings associated with amending CIARDS.[255] According to testimony by then-DCIA James Schlesinger, the purpose of CIARA was

> to provide a retirement system for those CIA employees who are actually involved in supporting or conducting our U.S. intelligence operations abroad. As they become older and move into their early 50's, it is often not possible, because of the rigorous conditions of service, for them to usefully serve the further period of time that would otherwise be required to qualify them for immediate retirement under the normal civil services rules.[256]

During a House Armed Services Committee hearing on CIARDS, Representative Stratton recalled that CIARDS was set up "due to the special character of CIA work, it was possible that an individual might burn himself out, or might have his cover removed at an early age and therefore would be required to retire at an early age."[257]

According to one former CIA employee who is a current CIARDS beneficiary, the program was also used for other reasons to include (1) as an incentive for those CIA employees who elected to serve overseas, and (2) as compensation for those CIA employees whose work as field agents made them unsuitable for most types of post CIA employment.[258]

CIARDS Eligibility

In order to participate in CIARDS, CIA employees had to meet the definition of CIARDS *participant*. As the law was originally written, selected CIA employees must have completed at least 15 years of *qualifying service*. Qualifying service, determined by the CIA Director (DCIA),

---

[254] U.S. Congress, Senate Committee on Armed Services, *Retirement and Disability System for Certain Employees of the Central Intelligence Agency*, 88th Cong., 2nd sess., September 21, 1964, S. Rept. 88-1589, p. 2

[255] P.L. 93-31 allowed the DCIA to designate more CIA employees for the system.

[256] Testimony of Honorable James Schlesinger, DCIA, U.S. Congress, House, Committee on Armed Services, Special Subcommittee on Intelligence Hearings on H.R. 6167 and S. 1494, Report 93-7, March 30, 1973, p. 2.

[257] Remarks of Representative Stratton, U.S. Congress, House, Committee on Armed Services, Full Committee Consideration of S. 1494, Report 93-8, April 12, 1973, p. 2.

[258] Interview, August 17, 2016.

included duties "in support of Agency activities abroad hazardous to life or health or… so specialized because of security requirements as to be clearly distinguishable from normal government employment."[259]

In 1992, Congress passed the "CIARDS Technical Corrections Act of 1992" as part of the IAA for FY1993 (P.L. 102-496, Title VIII) to update and restate CIARA. The 1992 version incorporated the many changes made between 1964 and 1992 mandated by statute, executive order, and necessity (e.g., the change from CSRS to FERS). Under the new legislation, CIA employees who have completed 5 years of *qualifying service* are eligible, and the definition of *qualifying service* has remained unchanged. CIA employees under CIARDS are eligible for retirement at age 50 with at least 20 years of service; or at any age with at least 25 years of service.[260] These employees are also subject to mandatory retirement at the discretion of the DCIA.

CIARDS Funding

Most CIARDS participants make the required employee contribution of 7% of pay. For individuals who are covered by Social Security, employee contributions are offset by Social Security contributions.[261] The required agency contribution on behalf of CIARDS-covered employees is set out in current law at 7.0% of pay for most participants.[262]

The DCIA manages the CIARDS Fund in the U.S. Treasury. CIA is responsible for the government's portion of the pension plan. Current law requires the DCIA to have actuarial calculations made of the funding status of the CIARDS Fund at least once every five years.[263] These actuarial calculations are used to produce estimates of the annual appropriations needed to meet the normal cost of the CIARDS for each year minus the required employee contributions.[264] The combination of CIARDS employee and agency contributions do not cover the normal cost of benefit payments. Therefore, the CIARDS Fund has accrued an unfunded liability and additional appropriations are required to (1) finance CIARDS benefit payments, which are mandatory entitlements,[265] and (2) pay down the unfunded liability of CIARDS in order to maintain its solvency.

Appropriations

The appropriated payment of funds to the CIARDS is set out as an entitlement under 50 U.S.C. §2091(d) & (e). This funding has been part of annual appropriations acts since Fiscal Year

[259] P.L. 88-643.

[260] See 50 U.S.C. §2055.

[261] CIARDS employee contributions are set out under 5 U.S.C. §2021(a)(2). Under 50 U.S.C. §2021(a)(2)(A), most CIARDS employees contribute 7% of pay. For individuals who are covered by Social Security, employee contributions are offset by Social Security contributions. 50 U.S.C. §2021(a)(1) (as amended by P.L. 112-96) defines a CIARDS "revised annuity employee" as an employee who first enters service under the CIARDS (or re-enters service covered by the CIARDS with less than five years of previous CIARDS service) after December 31, 2012. CIARDS contributions for "revised annuity employees" are set at 9.3% of pay, offset by Social Security contributions.

[262] CIARDS agency contributions are set out under 5 U.S.C. §2021(a)(3). The CIA contributes 7.0% of pay on behalf of most CIARDS participants. For CIARDS "revised annuity employees"—as defined in Footnote 5 above—the CIA contributes 4.7% of pay.

[263] 50 U.S.C. §2901(b).

[264] Actuaries use a concept called "normal cost" to estimate the amount of money that must be set aside each year from employer and employee contributions to pre-fund pension benefits.

[265] 50 U.S.C. Chapter 83.

1977.[266] The dollar amount in the IAA represents the amount of money the Congress has authorized the DNI to receive in order to meet the actual CIARDS pension payments anticipated in a given fiscal year.

The appropriated entitlement payment of funds to finance the non-employee contribution portion of CIARDS was established in 1976, in statute titled, "An Act to amend the Central Intelligence Agency Retirement Act of 1964 for Certain Employees" (P.L. 94-522, Section 102). P.L. 94-522 also specified that annual appropriations to the CIARDS Fund were authorized to include amounts to pay down unfunded liabilities; more specifically,

> each fiscal year in such sums as may be necessary to provide the amount equivalent to (1) interest on the unfunded liability computed for that year at the interest rate used in the then most recent valuation of the System, and (2) that portion of disbursement for annuities for that year which the Director estimates is attributable to credit allowed for military service, not to exceed the following percentages of such amounts: 70 per centum for 1977; 80 per centum for 1978; 90 per centum for 1979; and 100 per centum for 1980 and for each fiscal year thereafter.[267]

Community Management Account

The ICMA replaced an account used to support the DCI's Intelligence Community Staff (ICS) from 1972 through 1992.The ICMA was established in 1992 to support a Community Management Staff (CMS) created by then-DCI Robert Gates to coordinate cross-program activities, improve budget oversight, and strengthen community management.

When the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 (P.L. 108-458) abolished the position of DCI and the DCI's CMS, it created the new position of DNI assisted by an ODNI. The ODNI absorbed the functions of the old CMS and gained new ones. Although the CMS was abolished, the CMA continued and is sometimes referred to as the ICMA. The ICMA funds expenditures associated with personnel and day-to-day activities of the organizational elements that make up the Office of the Director of National Intelligence (ODNI).

Intelligence Community Staff

The Intelligence Community Staff (ICS) was created in response to a 1971 directive from President Nixon, issued in response to recommendations made by then-Director of the Office of Management and Budget, James Schlesinger.[268] President Nixon directed DCI Richard Helms[269] to plan and review all intelligence activities, produce national intelligence, chair and staff all community committees, and reconcile intelligence requirements and priorities with budgetary constraints.[270] DCI Helms responded, in part, by renaming and expanding the authority of the

[266] P.L. 94-522, Title I, Sec. 102.

[267] P.L. 94-522 §102.

[268] James Schlesinger, *A Review of the Intelligence Community*, March 10, 1971, at http://nsarchive.gwu.edu/NSAEBB/NSAEBB144/document%204.pdf. See also U.S. President (Richard Nixon), "Organization and Management of the U.S. Foreign Intelligence Community," November 5, 1971, at http://nsarchive.gwu.edu/NSAEBB/NSAEBB144/document%206.pdf.

[269] Helms served under DCI McCone as his Deputy Director for Plans and under DCI Raborn as DDCI. Douglas F. Garthoff, *Directors of Central Intelligence as Leaders of the U.S. Intelligence Community 1946-2005* (Washington, DC: GPO, 2005), p. 53.

[270] Douglas F. Garthoff, *Directors of Central Intelligence as Leaders of the U.S. Intelligence Community 1946-2005* (Washington, DC: GPO, 2005), p. 69.

National Intelligence Programs Evaluation (NIPE) Staff—formalizing the name change to the "Intelligence Community Staff" on March 1, 1972.[271]

Language authorizing the IC Staff is included in the SSCI's first IC budget authorization bill from 1977. According to S. 1539, Section 201(a): "There is authorized to be appropriated for the Intelligence Community Staff for fiscal year 1978 the sum of $8,950,000 to provide the support necessary to permit the Director of Central Intelligence to fulfill his responsibility for directing the substantive functions and managing the resources of the Intelligence Community."[272]

Language in the Senate Select Committee on Intelligence (SSCI) Report 95-214 is instructive in regards to committee intent as to the responsibilities of the IC Staff:

> The Intelligence Community Staff requested $10.5 million and 196 personnel in fiscal year 1978 to support the Director of Central Intelligence in fulfilling his responsibilities for overall management and direction of the intelligence community. This includes: (1) developing national intelligence requirements and priorities, (2) assessing the performance and quality of national intelligence collection and production activities, (3) improving the community's long-range planning process, and (4) monitoring the allocation and management of community resources.[273]

The IC Staff was authorized in subsequent IAAs, until 1992, when it was statutorily replaced with the previously discussed Community Management Staff (CMS) in the IAA for FY1993 (P.L. 102-496).

Community Management Staff

The end of the Cold War prompted many efforts to reform and reorganize the IC. According to a 1992 House Permanent Select Committee on Intelligence (HPSCI) report, the committee perceived a "lack of consistently exercised central management authority," and desired a DCI "ultimately accountable for the performance of its [the IC's] components."[274] Then-DCI Robert Gates commissioned a number of task forces to review the operation of elements of the IC and make recommendations for change. Acting upon those recommendations, Gates abolished the ICS and created the CMS in order to:

- "Strengthen centralized coordination and management;"
- "Identify cross program trade-offs;"
- "Establish divisions of labor;"
- "Reduce unneeded or unwanted duplication of effort;"

[271] The NIPE Staff was created by DCI John McCone in response to a memorandum from President Kennedy. The NIPE Staff "oversaw all kinds of community coordination matters except those involving analytic products such as NIEs." See Douglas F. Garthoff, *Directors of Central Intelligence as Leaders of the U.S. Intelligence Community 1946-2005* (Washington, DC: GPO, 2005), pp. 41&45, at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/directors-of-central-intelligence-as-leaders-of-the-u-s-intelligence-community/dci_leaders.pdf. Garthoff quotes from U.S. President (John F. Kennedy), "Memorandum for: Director of Central Intelligence," January 16, 1962, available at https://s3.amazonaws.com/static.history.state.gov/frus/frus1961-63v07-09mSupp/pdf/d255.pdf. See also Mark Lowenthal, *U.S. Intelligence: Evolution and Anatomy*, 2nd ed. (Westport, CT: Praeger, 1992), p. 32: The NIPE Staff analyzed IC programs and evaluated the effectiveness of the U.S. Intelligence Board in implementing priority national intelligence objectives.

[272] U.S. Congress, SSCI, S. 1539, "Intelligence Authorization Act for FY1978," 95th Cong., 1st sess., July 29, 1977.

[273] U.S. Congress, SSCI, Senate Report 95-214 to accompany S. 1539, 95th Cong., 1st sess., pp. 3-4. See also E.O. 11905 §3(b), "United States Foreign Intelligence Activities," February 18, 1976.

[274] U.S. Congress, HPSCI, H.Rept. 102-544, Pt 1, to accompany H.R. 5095, 102nd Cong., 2nd sess., June 2, 1992, p. 4.

- "Evaluate competitive proposals for investment from the Community;"
- "Look for efficiencies and cost savings;"
- "Manage the overall intelligence requirements process, to ensure coordination among the major collection disciplines;" and
- "Evaluate performance in satisfying policymaker needs for information."[275]

The new CMS was headed by an executive director for IC affairs, located within CIA headquarters, and unlike the ICS (which was staffed almost exclusively by CIA personnel), was staffed by employees from across the IC.[276] The staff included the new position of open source coordinator

> who will catalog the entire intelligence community's open source (that is, unclassified) holdings, establish a comprehensive requirements system for acquiring new open sources, improve the sharing of such sources throughout the community, and work with the managers of the other types of intelligence collection to ensure that they do not spend time and resources collecting intelligence that can be collected openly.[277]

The IAA for FY1993 (P.L. 102-496, Section 104) endorsed DCI Gates's management decision by recognizing a new "Community Management Staff."[278] According to SSCI Report 102-324,

> Section 104 authorizes appropriations and personnel levels for fiscal year 1993 for the Community Management Staff of the Director of Central Intelligence. This provision supersedes what had, in previous authorization bills, been the separate, public authorization for the Intelligence Community Staff. Pursuant to recent action by the Director of Central Intelligence, the existing Intelligence Community Staff was formally abolished, and many of its functions were dispersed to other elements within the Intelligence Community. To carry out the DCI's residual responsibilities for the Intelligence Community, the DCI created an Executive Director for Intelligence Community Affairs to head a smaller Community Management Staff located at CIA headquarters.[279]

Office of the DNI

The IRTPA of 2004 (P.L. 108-458) created the new position of DNI assisted by an ODNI. The ODNI absorbed the functions of the old CMS and gained new ones. The ICMA now funds the staffs of the DNI, the Principal Deputy DNI (PDDNI), Deputy and Associate DNIs, and all activities associated with the ODNI's mission and support activities (MSAs)—those offices and organizations directly responsible for providing IC-wide substantive intelligence, CI, strategic

[275] Testimony of DCI Robert N. Gates, "Joint Hearing before the SSCI and HPSCI on S. 2198 and S. 421 to Reorganize the U.S. Intelligence Community," S.Hrg. 102-1052, 102nd Cong., 2nd sess., April 1, 1992, p. 14.

[276] Mark Lowenthal, *U.S. Intelligence: Evolution and Anatomy*, 2nd ed. (Westport, CT: Praeger, 1992), p. 36.

[277] Mark Lowenthal, *U.S. Intelligence: Evolution and Anatomy*, 2nd ed. (Westport, CT: Praeger, 1992), p. 109.

[278] The IAA for FY1993 included a number of provisions designed to strengthen the DCI. For example, P.L. 102-496 §705 represented the first time in which the DCI's three separate roles were specified statute as head of IC, principal intelligence advisor, and head of the CIA. As head of the IC, the DCI's duties included "developing the community's budget, setting collection requirements and priorities, eliminating unneeded duplication, coordinating the community's relationships with foreign intelligence services, and protecting intelligence sources and methods from unauthorized disclosure." See Michael Warner, Editor, *Central Intelligence: Origin and Evolution*, Center for the Study of Intelligence (Washington D.C.: CIA, 2001), p. 12, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Origin_and_Evolution.pdf.

[279] U.S. Congress, SSCI, "Authorizing Appropriations for Fiscal Year 1993," S.Rept. 102-324 to accompany S. 2991, 102nd Cong., 2nd sess., July 21, 1992, p. 15.

analysis, research and development, and training and education.[280] Some of the larger MSAs include:

- Cyber Threat Intelligence Integration Center (CTIIC);
- National Counterterrorism Center (NCTC);
- National Counterproliferation Center (NCPC);
- National Counterintelligence and Security Center (NCSC);
- National Intelligence University (NIU);
- Intelligence Advanced Research Projects Activity (IARPA); and
- National Intelligence Council (NIC).

A number of ODNI offices focus on IC-wide concerns such as acquisition, budget, human capital, policy and strategy, and systems 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 including compliance with U.S. law, investigating allegations of fraud, waste, and abuse, and other issues.[281]

[280] Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014), pp. 2-2 and 4-12. See also Jeffrey Richelson, *The U.S. Intelligence Community*, 7th ed. (Boulder, CO: Westview Press, 2016), pp. 498-499. According to Richelson, the approximate size of the ODNI staff is 1,500 individuals, which includes those permanently assigned to the Centers.

[281] "Office of the Director of National Intelligence," at http://www.dni.gov/index.php/about/organization.

Appendix D. Homeland Security Intelligence Program (HSIP)

When the DHS Office of Intelligence and Analysis (OIA) was incorporated into the IC, there was no separate HSIP, although OIA's customers were extremely diverse. It was entirely funded through the NIP. In the words of Francis Taylor, the current Under Secretary for Intelligence and Analysis (DHS/I&A), "I&A has one of the broadest customer bases in the IC, ranging from the Secretary, to DHS policymakers and operators, to thousands of state and local officials and private sector partners—each of whom have different information classification requirements and limitations."[282]

In time, the DNI and DHS leadership argued that because OIA supported both an IC-wide mission and a department-specific mission, it needed both NIP funds to support DNI requirements, and separately controlled HSIP funds to support DHS requirements. In response, the congressional intelligence committees established the HSIP within DHS/OIA to include those "intelligence activities ... that serve predominantly departmental [DHS] missions."[283] For example, some of DHS's cyber support, and some of the governance activities associated with the Homeland Security Intelligence Council staff have been funded with HSIP dollars.

In S.Rept. 112-192, accompanying the IAA for FY2013, the Senate Intelligence Committee stated its support of the concept, but maintained its jurisdiction over the HSIP:

> The OIA is currently funded through the NIP. The Committee supports the request of the Secretary and DNI to fund OIA through the NIP and a new HSIP but is continuing to study the question of whether other intelligence activities of the Department should be included in the HSIP. The Committee intends to continue oversight of and authorize the HSIP.[284]

The IAA for FY2015 (P.L. 113-293 §324) requires the DHS/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 HSIP.

According to the Joint Explanatory Statement accompanying the IAA for FY2015:

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

[282] Remarks of Francis X. Taylor, "Additional Prehearing Questions for Mr. Francis X. Taylor upon his nomination to be the Under Secretary for Intelligence and Analysis of the Department of Homeland Security," Senate Select Committee on Intelligence document, n.d., p. 6, at http://www.intelligence.senate.gov/sites/default/files/hearings/taylorprehearing.pdf.

[283] 6 U.S.C. §121a. See also, the IAA for FY2013, P.L. 112-277 §501, Jan. 14, 2013.

[284] U.S. Congress, Senate Select Committee on Intelligence, *The Intelligence Authorization Act for FY2013*, report to accompany S. 3454, 112th Cong., 2nd sess., S.Rept. 112-192, July 30, 2012 (Washington D.C.: GPO, 2012), p. 11.

> reporting to Congress regarding the overall resources and personnel required in support of the Department's intelligence activities.[285]

In summary, within DHS, the NIP budget funds activities within the OIA that support national-level, IC-wide roles and responsibilities. The NIP does not fund OIA department-specific activities. The NIP budget provides *no funds* to operate DHS intelligence activities such as its Immigration and Customs Enforcement (ICE) Office of Intelligence because ICE is not an IC element. Because it is not part of the NIP, management of the HSIP does not belong to the DNI; it belongs to the Secretary of Homeland Security.

Thus, the Secretary of DHS manages intelligence-related budgets (that fall outside the NIP) that include: department specific, intelligence-related activities *of an IC component*; and intelligence-related activities of *non-IC components* within their departments. The same can be said of the Secretary of Defense, who manages the MIP and intelligence-related activities of non-IC components within the DOD. Other department secretaries, such as the Attorney General, and the Secretary of Treasury manage the intelligence-related activities of non-IC components within their departments, not the DNI. It is unclear how well the myriad of intelligence-related activities that fall outside the NIP or MIP are managed, coordinated or overseen on a day-to-day basis.

[285] "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.

Appendix E. IC Leaders and Selected Management *Hats*

Table E-1. U.S. Intelligence Community Leadership *Hats*

Concurrent Management Responsibilities

Element	Element Head	Selected Concurrent Management Responsibilities[a]
Non-Department of Defense		
Office of the Director of National Intelligence (ODNI)	Director of National Intelligence (DNI)	**Principal Intelligence Advisor** to the President and NSC **IC Community Manager** **Program Executive** for National Intelligence Program (NIP) funds
Central Intelligence Agency (CIA)	Director of the Central Intelligence Agency (D/CIA)	**Functional Manager**[b] for Human and Open Source Intelligence (HUMINT and OSINT) **Program Manager**[c] for CIA Program (CIAP) and CIA Retirement and Disability System (CIARDS) NIP funds
Department of Energy, Office of Intelligence and Counterintelligence (DOE/IN)	Director, Office of Intelligence and Counterintelligence (D/OICI)	**Program Manager** for DOE's NIP funds
Department of Homeland Security, Office of Intelligence and Analysis (DHS/I&A)	Under Secretary for Intelligence and Analysis (US/I&A)	**Program Manager** for DHS I&A's NIP and Homeland Security Intelligence Program (HSIP) funds
Department of Homeland Security, U.S. Coast Guard, Intelligence Division (USCG/IN)	Assistant Commandant for Intelligence, U.S. Coast Guard (CG-2)	**Program Manager** for USCG/IN's NIP funds
Department of Justice, Drug Enforcement Administration, Office of National Security Intelligence (DEA/ONSI)	Assistant Administrator and Chief of Intelligence (AACI)	**Program Manager** for DEA's NIP funds
Department of Justice, Federal Bureau of Investigation, Intelligence Branch (FBI)	Intelligence Branch Executive Assistant Director (NSB/EAD)	**Program Manager** for the FBI's NIP funds
Department of State, Bureau of Intelligence and Research (State/INR)	Assistant Secretary of State for Intelligence and Research (AS/INR)	**Program Manager** for INR's NIP funds
The Department of the Treasury, Office of Intelligence and Analysis (Treasury/OIA)	Assistant Secretary of the Treasury for Intelligence and Analysis (AS/I&A)	**Program Manager** for Treasury's NIP funds **National Intelligence Manager**[d] for Threat Finance and Transnational Organized Crime

Element	Element Head	Selected Concurrent Management Responsibilities[a]
Department of Defense		
DOD-wide		
Office of the Under Secretary of Defense for Intelligence (OUSD(I))	Under Secretary of Defense for Intelligence (USD(I)) and Director of Defense Intelligence (DDI)	**Program Executive** for Military Intelligence Program (MIP) funds
Defense Intelligence Agency (DIA)	Director of the Defense Intelligence Agency (D/DIA)	**Functional Manager** for Measurement Intelligence (MASINT) **Program Manager** for General Defense Intelligence Program (GDIP) NIP funds **Component Manager**[e] for DIA's MIP funds **Joint Functional Component Commander** for Intelligence, Surveillance and Reconnaissance (JFCC-ISR)
National Geospatial-Intelligence Agency (NGA)	Director of the National Geospatial-Intelligence Agency (D/NGA)	**Functional Manager** for Geospatial-Intelligence Intelligence (GEOINT) **Program Manager** for National Geospatial-Intelligence Program (NGP) funds **Component Manager** for NGA's MIP funds
National Reconnaissance Office (NRO)	Director of the National Reconnaissance Office (D/NRO)	**Program Manager** for National Reconnaissance Program (NRP) NIP funds **Component Manager** for NRO's MIP funds
National Security Agency/Central Security Service (NSA/CSS)	Director, National Security Agency (DIRNSA)	**Functional Manager** for Signals Intelligence (SIGINT) **Program Manager** for Consolidated Cryptologic Program (CCP) NIP funds **Component Manager** for NSA's MIP funds **Commander**, U.S. Cyber Command **Chief,** Central Security Service (CHCSS)
Service-Level		
Office of the Deputy Chief of Staff, G-2, U.S. Army (ODCS G-2)	U.S. Army Deputy Chief of Staff, G-2 (DCS G-2)	**Component Manager** for the U.S. Army's MIP funds
Marine Corps Intelligence Department (MCID)	Marine Corps Director of Intelligence (DIRINT)	**Component Manager** for the USMC's MIP funds
U.S Navy	Deputy Chief of Naval Operations for Information Dominance and Director of Naval Intelligence (N2/N6)	**Component Manager** for the USN's MIP funds

Element	Element Head	Selected Concurrent Management Responsibilities[a]
U.S. Air Force	Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, Headquarters U.S. Air Force (AF/A2)	**Component Manager** for the USAF's MIP funds
U.S. Special Operations Command Intelligence	U.S. SOCOM Director of Intelligence (J-2)	**Component Manager** for SOCOM's MIP funds

Sources: ODNI.gov (http://www.odni.gov/); respective agency or component websites; OUSD(I); DEA; and Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014).

Notes:

a. There may be other management hats associated with these positions. The list of concurrent management responsibilities is not intended to be exhaustive.

b. Functional managers act as the principal adviser to the DNI for their respective intelligence function and in the same capacity for the Secretary of Defense.

c. Program Managers manage NIP programs for the DNI.

d. National Intelligence Managers (NIMs) serve as the principal substantive advisors on intelligence related to designated countries, regions, topics, or functional areas.

e. Component Managers manage MIP programs for the USD(I).

Appendix F. Budget Processes (IPPBE and PPBE)

Table F-1. IPPBE and PPBE Side-by-Side

	Intelligence Planning, Programming, Budgeting and Evaluation (IPPBE)[a]	DOD Planning, Programming, Budgeting and Execution (PPBE)[b]
Applies to	NIP funds associated with all 17 IC elements	MIP funds associated with all DOD IC elements.
Guidance	IC Directive 116	DOD Directive 7045.14
Budget Orientation	Functional—organized around intelligence capabilities	Organizational—Organized around the military services
Budget Building Blocks	Expenditure Centers, Projects, Sub-Projects and Activities	Program Elements
Budget Categories	Mission Management; Collection and Operation; Processing and Exploitation; Analysis and Production; Enterprise Management; Research and Technology; and Enterprise Information Technology	Operations and Maintenance (O&M); Military Personnel; Research, Development, Test, and Evaluation (RDT&E); Procurement; Military Constructions (MilCon); and Shipbuilding.
Role of Managers	Program Managers as intermediaries between DNI and NIP funded organizations.	Component Managers deal directly with OSD.
Planning Phase	The Assistant DNI for Systems and Resources Analysis (ADNI/SRA) leads[c] this phase.	Under Secretary of Defense for Policy (USD(P)) leads this phase.
	Documents such as the Quadrennial Defense Review, the National Security Strategy and the National Military Strategy, the National Intelligence Priorities Framework and National Intelligence Strategy provide input into the planning phase to try to ensure that threats, long-term strategy, larger force structure/readiness concerns and cost effectiveness are addressed in the planning phase.	
Programming Phase	The ADNI/SRA leads the programming phase.	The Director of Cost and Program Evaluation (CAPE) leads this phase.
	The primary objective of this phase is to provide analytically based, fiscally constrained options to frame DNI and USD(I)/DDI resource decisions.	
Budgeting Phase	Budgeting and execution comprise one phase (unlike the PPBE) led by the ADNI/Chief Financial Officer (ADNI/CFO). The ODNI CFO is responsible for producing the Congressional Budget Justification Books (CBJBs) justify the details associated with each of the NIP programs to Congress	The Under Secretary of Defense Comptroller/ Chief Financial Officer (Comptroller) reviews the budget submissions from the military services. The OUSD(I) Director for MIP Resources is responsible for producing the Congressional Justification Books (CJBs) that justify the MIP Programs to Congress.
	The primary objective is to develop, defend, execute, and manage the NIP and MIP portions of the President's budget. Programs are reviewed to ensure: appropriate funding and fiscal controls and whether it can be realistically executed in the requested budget year.	
Execution Phase	Managed by the CFO. The ADNI/CFO manages the NIP budget spending.	*The "E" in the PPBE stands for "execution,"* not evaluation. The Comptroller, together with the military services (and defense agencies), manage MIP budget spending.
	Once the budget is enacted by Congress, the execution phase spends appropriated funds as directed by Congress in the authorization and appropriation bills.	
Evaluation	*The "E" in the IPPBE stands for "evaluation,"* not execution. Responsibility for the evaluation	Not formally considered a phase, evaluation occurs throughout the fiscal year. The CAPE

	Intelligence Planning, Programming, Budgeting and Evaluation (IPPBE)[a]	DOD Planning, Programming, Budgeting and Execution (PPBE)[b]
Phase	function is shared but the SRA tends to lead.	leads.
	Evaluation is a continuous process to assess the effectiveness of programs, activities, major initiatives, and investments. Responsibility for the evaluation function is shared.	
Protection of Funds	NIP *fence* (protected from use by other organizations within their respective agencies)	MIP *protected* (limited protection from use by military services for non-intelligence purposes).

Source: CRS, based primarily on Dan Elkins, *Managing Intelligence Resources*, 4th ed. (Dewey, AZ: DWE Press, 2014). See also Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, January 5, 2012, p. F-9.

Notes:

a. See also CRS In Focus IF10428, *Intelligence Planning, Programming, Budgeting and Evaluation Process (IPPBE)*, by Anne Daugherty Miles.

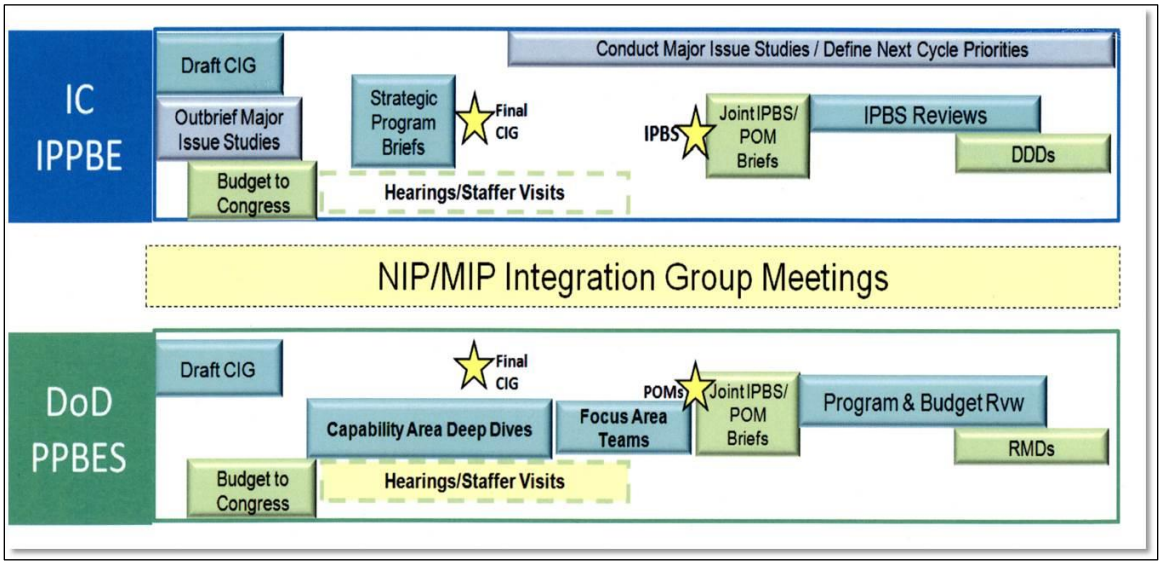
b. See also CRS In Focus IF10429, *Defense Primer: Planning, Programming, Budgeting and Execution Process (PPBE)*, by Lynn M. Williams.

c. While each phase has a designated lead player on the ODNI staff, that person (and his or her staff) works in concert with many others during all phases of the IPPBE process.

Appendix G. NIP MIP Program Integration

Figure G-1. National and Military Intelligence Program Integration

Integrating the Intelligence Community's Intelligence Planning, Programming, Budgeting and Evaluation process with the DOD's Planning, Programming, Budgeting and Execution System



Source: IPPBE Training Document.

Notes:

a. Acronyms: CIG—Consolidated Intelligence Guidance; DDD—DNI Decision Documents; IPBS—Intelligence Program Budget Submission; POM—Program Objectives Memorandum; RMDs—Secretary of Defense Resource Management Decisions.

b. Theoretical timeline (subject to change): January/February for the Draft CIG and Budget submission to Congress; March April for Strategic Program Briefs by the Program Managers; April for final CIG; February through June for congressional Hearings/Staffer Visits; July/August for the Joint IPBS POM Briefs; October-January for the DDDs and RMDs.

c. See also Dan Elkins, *Managing Intelligence Resources*, 4th ed., (Dewey, AZ: DWE Press, 2014) and CRS products on the IPPBE and PPBE.

Appendix H. Selected Acronyms

A-2	Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, Headquarters U.S. Air Force (AF/A2)
A&A	Authorization with matching Appropriation
A not A	Authorization with no matching Appropriation or the reverse
CCP	Consolidated Cryptologic Program
CBJB(s)	Congressional Budget Justification Book(s) for NIP Programs
CG-2	U.S. Coast Guard Assistant Commandant for Intelligence
CI	Counterintelligence
CIA	Central Intelligence Agency
CIAP	Central Intelligence Agency Program
CIARDS	Central Intelligence Agency Retirement and Disability System
CJB(s)	Congressional Justification Books for MIP Programs
CJCS	Chairman of the Joint Chiefs of Staff
CMA (ICMA)	Community Management Account, also known as the Intelligence Community Management Account (ICMA)
COCOM	Combatant Command
COMINT	Communications Intelligence
CT	Counterterrorism
DCI	Director of Central Intelligence—position replaced with DNI
DCIA	Director of the CIA
DDI	Director of Defense Intelligence
DEA/OSNI	Drug Enforcement Administration, Office of National Security Intelligence
DIA	Defense Intelligence Agency
DIRINT	U.S. Marine Corps Director of Intelligence
DIRNSA	Director, National Security Agency
DHS/OIA	Department of Homeland Security/Office of Intelligence and Analysis
DNI	Director of National Intelligence
DOD	Department of Defense
DOE/I&CI	Department of Energy, Intelligence and Counter Intelligence Division
ELINT	Electronic Intelligence
E.O.	Executive Order
FBI/NSB	Federal Bureau of Investigation, National Security Branch
FISINT	Foreign Instrumentation Signals Intelligence
G-2	U.S. Army Deputy Chief of Staff for Intelligence
GDIP	General Defense Intelligence Program
GEOINT	Geospatial Intelligence

HPSCI	House Permanent Select Committee on Intelligence
HUMINT	Human Intelligence
IAA	Intelligence Authorization Act
IMINT	Imagery Intelligence
IPPBE	Intelligence Planning, Programming, Budgeting, and Evaluation system
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458)
ISR	Intelligence, Surveillance and Reconnaissance
J-2	Joint Staff Director of Intelligence
JCS	Joint Chiefs of Staff
JIOC	Joint Intelligence Operations Center
MASINT	Measurement and Signals Intelligence
MIP	Military Intelligence Program
N-2	Deputy Chief of Naval Operations for Information Dominance (N-2)
NGA	National Geospatial-Intelligence Agency
NGP	National Geospatial-Intelligence Program
NIM(s)	National Intelligence Manager(s)
NIP	National Intelligence Program
NIPF	National Intelligence Priorities Framework
NRO	National Reconnaissance Office
NRP	National Reconnaissance Program
NSA/CSS	National Security Agency/Central Security Service
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
ONI	Office of Naval Intelligence
OSD	Office of the Secretary of Defense
OSINT	Open Source Intelligence
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
PPBE	Planning, Programming, Budgeting, and Execution system—DOD budget process
SCI	Sensitive Compartmented Information
SIGINT	Signals Intelligence
SSCI	U.S. Senate Select Committee on Intelligence
State/INR	Bureau of Intelligence and Research, U.S. Department of State
Treasury/OIA	Department of the Treasury, Office of Intelligence and Analysis
Treasury/OTFI	Department of the Treasury, Office of Terrorism and Financial Intelligence
USCG/IN	U.S. Coast Guard Intelligence Division, Department of Homeland Security
USD(I)	Under Secretary of Defense (Intelligence)
USSOCOM or SOCOM	U.S. Special Operations Command
WMD	Weapons of Mass Destruction

Author Contact Information

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

Acknowledgments

Heidi Peters, Information Research Specialist, Knowledge Services Group, contributed greatly to the contents of this report, most particularly to the tables in the Appendices.