The U.S. Intelligence Community: Selected Cross-Cutting Issues

name redacted
Analyst in Intelligence and National Security Policy

April 12, 2016

Congressional Research Service
7-....
www.crs.gov
R44455

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

This report focuses on cross-cutting management issues that affect the Intelligence Community's (IC's) ability to counter "pervasive and emerging threats" to the United States and balance resources both appropriately and wisely. As the IC's senior manager, these issues ultimately fall within the Director of National Intelligence's (DNI's) area of responsibility. The DNI is charged with integrating the community of intelligence agencies so that they operate effectively as one team.

There are no easy solutions to the challenges examined in this report. The IC's efforts to demonstrate progress are hampered by difficulties such as the IC's diffuse structure—a confederation of separately managed component parts; the unique demands of operating in secret; the interrelationships between many issues; and diminishing resources.

The issues selected for examination in this report were chosen because they affect a number of agencies and are widely discussed by professionals within and external to the IC (and are not so complex that they need their own separate report).

1. **Budget.** Are the resources in the IC budget (the national and military intelligence programs) managed and balanced appropriately to meet the needs of every agency and the IC mission as a whole?
2. **Analysis.** The heart and soul of the intelligence function; analysis is the responsibility of every IC agency. How to improve analysis is an enduring focus of reform efforts.
3. **"Big Data**." The IC Information Technology Enterprise (IC ITE) is a major initiative focused on many of the challenges and opportunities associated with the current ocean of available information. How well is the IC putting vast amounts of unstructured data to valuable use?
4. **Diversity**. New initiatives designed to improve diversity in the entire IC workforce have been a recurring theme in intelligence-related legislation and IC policy directives over the past decade. Can anything else be done?
5. **Global coverage.** The IC's need to prepare for and respond to any and all crises and threats—worldwide—is referred to as global coverage. Do expectations about what the IC can and should cover need be adjusted?
6. **Continuous Evaluation** (CE). The expanded use of publicly available data when reviewing the backgrounds of a security clearance holder is the new standard for all IC agencies. What is the CE issue from a privacy and civil liberties perspective?
7. **Polygraphs.** Although polygraphs are required by every agency, their reliability and validity are questionable. As the IC moves toward CE, are they still necessary?
8. **Transparency**. What more can be done IC-wide to enhance public understanding of intelligence activities through greater transparency while still protecting national security?

While the eight issues are different in many ways, they are similar in that they shine a light on important questions that can be applied to any IC issue in terms of balance, best practices, integration, privacy and civil liberties, transparency, and trust.

Contents

Tables

Appendixes

Contacts

Introduction

At the heart of congressional oversight over most intelligence-related issues is the concern that the Intelligence Community (IC): (1) has the resources it needs in order to counter threats to the United States, (2) has balanced its resources appropriately across a wide variety of programs and activities, and (3) is using those resources wisely in accordance with statute, legislative intent, and values.[1]

When Director of National Intelligence (DNI) James Clapper released the 2014 National Intelligence Strategy (NIS), he described the "pervasive and emerging threats"[2] facing the United States this way:

> While key nation states such as China, Russia, North Korea and Iran will continue to challenge U.S. interests, global power is also becoming more diffuse. New alignments and informal networks, outside of traditional power blocs and national governments, will increasingly have significant impact in global affairs. Competition for scarce resources such as food, water and energy is growing in importance as an intelligence issue as that competition exacerbates instability, and the constant advancements and globalization of technology will bring both benefits and challenges.[3]

Most recently, in his annual worldwide threats briefing to Congress, DNI James Clapper reiterated many of the challenges mentioned in the quote above, and described a situation as one in which "unpredictable instability has become the 'new normal.'"[4]

There are many issues associated with the IC's ability to counter threats, balance its resources, and use those resources wisely. A partial-list is representative of the wide range of topics currently being discussed in public forums, reports, conferences, journals, and white papers: CIA's new "Mission Centers" and Directorate for Digital Innovation; CIA management and notification reforms in regards to covert operations; National Security Agency's (NSA's) reorganization—"NSA 21"—designed to integrate two directorates: signals and information assurance; NSA's concerns over encryption and "going dark"; business concerns over access to, and the ability to retain, IC contracts; the use of social media to identify possible terrorist activity; and a new National Background Investigations Bureau (NBIB) within Office of Personnel Management.

Some issues are agency centric—affecting a single agency—such as the NSA's encryption concerns. Other issues, such as intelligence analysis, affect more than one IC agency and are considered cross-cutting. They impact the DNI's ability to horizontally integrate the IC agencies (often referred to as "stovepipes") so that the IC operates effectively as one team.[5] This report focuses on eight issues associated with the horizontal leadership and management of the IC. These cross-cutting issues include: (1) the IC budget process, (2) analysis, (3) big data, (4) diversity, (5) global coverage, (6) continuous evaluation, (7) polygraphs, and (8) transparency.

---

[1] CRS Report RL30240, *Congressional Oversight Manual*, by (name redacted) et al.

[2] Office of the Director of National Intelligence (ODNI), "DNI Unveils 2014 National Intelligence Strategy," ODNI news release no. 40-14, September 18, 2014, at http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1243-dni-unveils-2014-national-intelligence-strategy. NIS 2014 is the most current NIS.

[3] ODNI, "DNI Unveils 2014 National Intelligence Strategy," ODNI news release no. 40-14, September 18, 2014.

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

[5] IC agencies are sometimes referred to as 'stovepipes' (and/or 'silos of excellence') in that each offers depth of expertise and specialized skill sets, but also meaning that information tends to flow vertically—up and down the management hierarchy—often with little coordination and/or collaboration between them.

They were chosen because they affect a number of agencies and are widely discussed by professionals within and external to the IC (and are not so complex that they need their own separate report).

The following section briefly describes several relevant aspects of the IC important to understanding the issues being examined: 17 elements (or components) of the IC; two key leadership positions—the Director of National Intelligence and the Under Secretary of Defense for Intelligence; key agency overseers—the Inspectors General; the national and military intelligence budget programs; and the National Intelligence Strategy.

Background

The U.S. Intelligence Community (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 of Homeland Security (DHS) intelligence elements:

4. Office of Intelligence and Analysis (I&A)
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)

Intelligence Community Leadership

The IC is led and managed on a daily basis by the Director of National Intelligence (DNI), with the assistance of the leadership team within the Office of the DNI (ODNI). The DNI is the principal intelligence advisor to the President and community manager. He has authority to develop and determine the national intelligence program budget.[6] The position of DNI was created by the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 (P.L. 108-458). The IRTPA gives the DNI more extensive authorities to coordinate the nation's intelligence effort than those formerly possessed by Director of Central Intelligence (DCI).

The core mission of the DNI and by extension, the ODNI, is to lead the IC in intelligence integration—synchronizing collection, analysis, and counterintelligence so that they are fused—effectively operating as one team.[7] Remarks by DNI James Clapper explain his understanding of the rationale for creating the DNI position:

> It's about helping them [the intelligence agencies] to recognize the cultural strengths and capabilities that each of the 17 Intelligence Community elements brings to the table and then getting them to think as a community, bringing our best and most appropriate community resources to bear against our toughest community problems.
>
> That's what I've referred to as 'intelligence integration,' and it's been my theme for the past four years, because I believe that's what the 9/11 Commission had in mind and what was instantiated in law by the Intelligence Reform and Terrorism Prevention Act of 2004. I believe it's the prerequisite to reaching the 9/11 Commission's goal that we act jointly as an integrated Intelligence Community.
>
> That's integration 'horizontally,' across agency lines, with each agency on equal footing and stature. But I also believe we have to work toward 'vertical' integration from federal to state, and to local, tribal, and territorial governments and their law-enforcement to other government agencies, like the FAA & TSA, and also to industry partners.[8]

The ODNI, a staff of some 1,500 individuals, works to carry out the DNI's responsibilities.[9] 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 such as compliance with U.S. law, investigating allegations of fraud, waste, and abuse, and other issues.[10]

Within the Department of Defense (DOD), the Under Secretary of Defense (Intelligence) [USD(I)] is a second key figure in IC leadership—with significant authorities to direct and control intelligence agencies within the DOD (NSA, DIA, NGA, NRO, and intelligence components of the military services) with the assistance of the leadership team within the Office of the USD(I) [OUSD(I)].[11] The USD(I) is the principal intelligence advisor to the Secretary of

---

[6] IC Directive (ICD) 104 provides overall policy to include a description of the DNI's roles and responsibilities as program executive of the NIP.

[7] ODNI, *U.S. National Intelligence: An Overview 2013*, pp 1-2, at http://www.dni.gov.

[8] DNI James R. Clapper, IATA – AVSEC World, *Remarks*, October 27, 2014, Washington DC, http://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.

[9] Jeffrey Richelson, The U.S. Intelligence Community, 6th Edition, (Boulder, CO: Westview Press, 2012), p. 470.

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

[11] The position of USD(I) was created by the National Defense Authorization Act for FY2003 (P.L. 107-314, §901). The law divided the duties associated with the former Assistant Secretary of Defense for Command, Control, (continued...)

Defense, the DOD's principal interface with the CIA and other non-defense elements of the IC, and represents the DOD on intelligence operations at the National Security Council (NSC).[12]

In May 2007, the Secretary of Defense and DNI formally agreed in a Memorandum of Agreement (MOA) that the position of USD(I) would be "dual-hatted"—the incumbent acting as both the USD(I) within the Office of the Secretary of Defense (OSD) and Director of Defense Intelligence (DDI) within the ODNI in order to improve the integration of national and military intelligence.[13]

Efforts to address cross-cutting issues can be hampered by difficulties associated with managing the IC's confederation of separately managed component parts. Most intelligence offices/agencies have a dual mission: (1) support national-level intelligence related activities managed by the DNI and (2) support operational-level intelligence related activities managed by their parent department. Only the individuals assigned to the ODNI report to the DNI. Senior leaders in the remaining 16 agencies are selected by, and report to, the director of their parent department. While DNI concurrence in the selection process for most IC agency heads is required by law, the DNI has limited authority to control programmatic activities within these entities.[14]

Inspectors General (IGs)

Many cross-cutting issues require independent entities within the IC to oversee executive branch activities. Agency Inspectors General (IGs) perform an important reporting function by ''keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies relating to the administration of ... programs and operations and the necessity for and progress of corrective action."[15]

IGs are an independent oversight tool throughout American government.[16] The Inspector General Act of 1978 (P.L. 95-452) established IGs at various departments and agencies government-wide. Some of these IGs are appointed by the President with the advice and consent of the Senate and

(...continued)

Communications and Intelligence, or ASD/C3I, into two positions—one position responsible for managing the intelligence portfolio, and one position responsible for supervising information systems across the DOD.

[12] Biography of Marcel Lettre, "Under Secretary of Defense for Intelligence," at http://www.defense.gov/About-DoD/Biographies/Biography-View/Article/602729/marcel-lettre.

[13] Michael McConnell, DNI and Robert Gates, Secretary of Defense, "Memorandum of Agreement," May 2007. Then-USD(I) James Clapper said that the creation of the DDI position was a way to better "strengthen the relationship between the DNI and the DOD … (and) to facilitate staff interaction and promote synchronization." The MOA did not alter the statutory responsibilities or authorities of either the Secretary of Defense or the DNI. See DOD news release No 637-07, May 24, 2007, "Under Secretary of Defense for Intelligence to be Dual-Hatted as Director of Defense Intelligence.," at http://www.defense.gov/Releases/Release.aspx?ReleaseID=10918.

[14] According to 50 U.S.C. §3041(b)(1), "[T]he head of the department or agency having jurisdiction over the position shall obtain the concurrence of the Director of National Intelligence before appointing an individual to fill the vacancy or recommending to the President an individual to be nominated to fill the vacancy. If the Director does not concur in the recommendation, the head of the department or agency concerned may not fill the vacancy or make the recommendation to the President (as the case may be). In the case in which the Director does not concur in such a recommendation, the Director and the head of the department or agency concerned may advise the President directly of the intention to withhold concurrence or to make a recommendation, as the case may be. This section in U.S.C. does not apply to the selection of Director, CIA.

[15] Inspector General Act of 1978 as amended through P.L. 114-113, enacted December 18, 2015, §2(1-3).

[16] See CRS Report R43722, *Offices of Inspectors General and Law Enforcement Authority: In Brief*, by (name redacted); and the IG portion of CRS Report R43793, *Intelligence Authorization Legislation for FY2014 and FY2015: Provisions, Status, Intelligence Community Framework*, by (name redacted) .

others administratively appointed by the heads of their respective federal entities.[17] IGs are authorized to "conduct and supervise audits and investigations relating to the programs and operations" of the government and "to promote economy, efficiency, and effectiveness in the administration of, and ... to prevent and detect fraud and abuse in, such programs and operations."[18] Some have raised concerns over whether an overzealous IG might pose a threat to agency operations.[19] For example, while the CIA has had an administratively established IG since 1952, it was only in 1989 that Congress enacted legislation statutorily mandating an "independent" IG at CIA, appointed by the President with the advice and consent of the Senate.[20] Before that, CIA IGs were appointed by the Director of the CIA.[21]

The IAA for FY2010 (P.L. 111-259, Section 405) established an independent IG of the IC, appointed by the President with the advice and consent of the Senate, to report directly to the DNI. To enhance the IG's independence within the ODNI, the IG may be removed only by the President, who must communicate the reasons for the removal to the congressional intelligence committees.[22] According to the accompanying Senate Report: "The IG will keep both the DNI and the congressional intelligence committees fully and currently informed about problems and deficiencies in Intelligence Community programs and operations and the need for corrective actions."[23]

Within the IC, the IGs of CIA, NSA, NRO, and the Departments of Defense, Energy, Homeland Security, Justice, State, and the Treasury are appointed by the President with the advice and consent of the Senate.[24] Only DIA and NGA remain "designated Federal entities" as defined by the Inspector General Act of 1978.[25] As such, the heads of DIA and NGA administratively appoint their affiliated IGs.[26]

The DOD created the IG for Intelligence position in 1976, "to provide for independent oversight of the legality and propriety of all defense foreign intelligence and foreign counterintelligence activities" in the DOD.[27] In 1982, the DOD's IG for Intelligence became the Assistant to the

[17] See the Inspector General Act of 1978, as amended, §8G(2) for those IGs who are administratively appointed.

[18] Inspector General Act of 1978, §2(1-3). http://legcounsel.house.gov/Comps/Inspector%20General%20Act%20Of%201978.pdf.

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

[20] IAA for FY1990 (P.L. 101-193), Title VIII, "Inspector General for Central Intelligence Agency." According to Britt Snider, p. 1., "Creating an independent statutory IG at the CIA did not gain political momentum until after the Iran-contra scandal of 1986-87, although all the investigations of the CIA that took place in the mid-1970s had pointed out serious defects in the IG function." For more on the position's history, see Afsheen John Radsan, "One Lantern in the Darkest Night—The CIA's Inspector General," 2010, at http://open.mitchellhamline.edu/.

[21] Britt Snider, "Creating a Statutory IG at the CIA," *Studies in Intelligence*, vol. 44, no 5, (August 3, 2011), p. 1. See also 50 U.S.C. §403(q) and CIA Act of 1949 §17. Until the creation of the DNI position in 2005, the Director of the CIA was also the Director of Central Intelligence.

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

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

[24] The IAA for FY2014 (P.L. 113-126, Sections 402 and 412) added the IGs of NRO and NSA to the list of those presidentially appointed, Senate confirmed. See S.Rept. 113-120, p. 9. See also CRS Report R43793, *Intelligence Authorization Legislation for FY2014 and FY2015: Provisions, Status, Intelligence Community Framework*, by (name redacted) .

[25] Inspector General Act of 1978, as amended, §8G(2)

[26] For more on the IC IG and administratively appointed IGs in the IC, see S.Rept. 111-55, p. 40.

[27] Historical Office of the Secretary of Defense, *Department of Defense Key Officials: 1947-2014*, June 2014, pp. 14-15, at http://history.defense.gov/Portals/70/Documents/key_officials/Key%20Officials_June%202014.pdf.

Secretary of Defense for Intelligence Oversight [ATSD(IO)].[28] According to DOD Directive 5148.11, the ATSD(IO) is responsible for:

> [I]ndependent oversight of all intelligence, counterintelligence, and intelligence-related activities (referred to collectively in this directive as "intelligence activities")—in the DoD. In this capacity, the ATSD(IO) inspects all intelligence or intelligence-related activities conducted by any of the DoD Components to ensure that these activities comply with federal law, Executive orders (E.O.s), Presidential Directives, Intelligence Community (IC) Directives, and DoD issuances.[29]

Intelligence Spending Programs

There is often confusion over what constitutes the IC budget partly because there are two separate IC spending programs: (1) the National Intelligence Program (the "NIP"), which covers the programs, projects, and activities of the intelligence community oriented towards the strategic needs of decision makers, [30] and (2) the Military Intelligence Program (the "MIP"), which funds defense intelligence activities intended to support tactical military operations and priorities. [31] A more accurate total of intelligence spending is a combination of the two.

Many cross-cutting issues (such as technology integration) affect, and are affected by, the difficulties associated with integrating two separately managed spending programs. The NIP and MIP are managed and overseen by the DNI and USD(I) respectively, under different authorities.[32] Funding associated with the NIP and MIP is roughly 70 billion dollars. In Fiscal Year (FY) 2015, for example, the aggregate amount (base and supplemental) appropriated totaled $66.8 billion—with the NIP ($50.3 billion) roughly triple the size of the MIP $16.5 billion).[33] The DNI and USD(I) work together in a number of ways to facilitate the "seamless integration" of NIP and MIP intelligence efforts.[34] Some programs may receive both NIP and MIP resources.[35] **Table 1** provides an overview of NIP and MIP spending over the past decade.[36]

---

[28] *Department of Defense Key Officials: 1947-2014*, p. 16.

[29] DODD 5148.11, "Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO))," April 24, 2013, §3, at http://dtic.mil/whs/directives/corres/pdf/514811p.pdf.

[30] The 'topline' number for the NIP was classified until 2007—with two exceptions (October 1997 and March 1998). The exceptions are discussed later in this report. 'Topline' is a frequently used colloquial term referring to any aggregated budget total. When the media refers to the 'Black Budget,' it is usually referring to the NIP, not the MIP. See for example, Dana Priest, "The Black Budget," *Washington Post,* August 29, 2013, at http://www.washingtonpost.com/wp-srv/special/national/black-budget/.

[31] Dan Elkins, *Managing Intelligence Resources*, 4th Edition (Dewey, AZ: DWE Press, 2014): Chapter 4, p. 4-12. See also CRS Report R44381, *Intelligence Spending: In Brief*, by (name redacted) , for more information on intelligence funding over the past several decades, with an emphasis on the period from 2007-2017—the period in which total national and military intelligence program spending dollars have been publicly disclosed on an annual basis.

[32] The USD(I) position was created by Secretary of Defense Donald Rumsfeld in 2003, codified in the *National Defense Authorization Act for FY2003* (P.L. 107-314, §901). For more on the USD(I) position, see the McDonnell article cited in footnote 13. DOD Directive 5205.12, signed in November 2008, established policies and assigned responsibilities, to include the USD(I)'s role as program executive of the military intelligence program, acting on behalf of the Secretary of Defense.

[33] See ODNI, "DNI Releases Budget Figure for 2015 National Intelligence Program," news release no. 24-15, October 30, 2015, at http://www.dni.gov/index.php/newsroom/press-releases/210-press-releases-2015/1279-dni-releases-budget-figure-for-2015-national-intelligence-program. See also DOD, "DOD Releases Figure for 2015 Military Intelligence Program," Release No: NR-416-15, October 30, 2015, at http://www.defense.gov/News/News-Releases/News-Release-View/Article/626734/department-of-defense-releases-budget-figure-for-2015-military-intelligence-pro.

[34]See Michael McConnell, DNI and Robert Gates, Secretary of Defense, "Memorandum of Agreement," May 2007, (continued...)

At the present time only the NIP aggregate (or top-line) figure must be disclosed based on a directive in statute.[37] The DNI is not required to disclose any other information concerning the NIP budget, whether the information concerns particular intelligence agencies or particular intelligence programs. In 2010, the Secretary of Defense began disclosing MIP appropriations figures on an annual basis and in 2011 disclosed those figures back to 2007.[38] These actions have provided public access to previously classified budget numbers for national and military intelligence activities.

Table 1. Intelligence Spending, FY2007-2017

numbers in billions, rounded

	FY07	FY08	FY09	FY10	FY11	FY12	FY13[a]	FY14	FY15	FY16	FY17
NIP[b]	$43.5	$47.5	$49.8	$53.1	$54.6	$53.9	$49.0 ($52.7)	$50.5	$50.3	$53.9	$53.5
MIP[c]	$20.0	$22.9	$26.4	$27.0	$24.0	$21.5	$18.6 ($19.2)	$17.4	$16.5	$17.9	$16.8
NIP MIP Total	$63.5	$70.4	$76.2	$80.1	$78.6	$75.4	$67.6 ($71.9)	$67.9	$66.8	$71.8	$70.3

Source: CRS, using numbers available at http://www.dni.gov, http://www.defense.gov, and http://www.whitehouse.gov.

Notes:

a. $52.7B was reduced by amount sequestered to $49.0B, DNI press release, October 30, 2013; $19.2B was reduced via sequestration to $18.6B, DOD press release, October 31, 2013. Automatic spending cuts were required under the Budget Control Act of 2011 (P.L. 112-25).

b. National Intelligence Program (NIP) topline numbers are public in accordance with *Implementing Recommendations of the 9/11 Commission Act of 2007*, P.L. 110-53, §601. NIP numbers include base budget and Overseas Contingency Operations (OCO) dollars.

c. Military Intelligence Program (MIP) numbers include base budget and OCO dollars.

d. Values in columns for Fiscal Years 2016 and 2017 are requested dollars.

The National Intelligence Strategy (NIS)

The IC's "blueprint" or master plan; the National Intelligence Strategy (NIS) shapes priorities for IC agencies. It describes the "strategic environment, sets priorities and objectives, and focuses resources on current and future budgets, acquisitions and operations decisions."[39] Enterprise

(...continued)

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.

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

[36] For more on intelligence spending programs, see CRS Report R44381, *Intelligence Spending: In Brief*, by (name redacted) .

[37] P.L. 110-53 §601(a).

[38] Department of Defense, "DOD Releases Military Intelligence Program Top Line Budget for Fiscal 2007, 2008, 2009," DOD *news release* no. 199-11, March 11, 2011, available at http://archive.defense.gov/Releases/Release.aspx?ReleaseID=14328. The release of the MIP topline was not directed by statute. According to this news release, it was a decision made by the Secretary of Defense.

[39] Office of Director of National Intelligence, "DNI Unveils 2014 National Intelligence Strategy," *news release* 40-14, September 18, 2014, at http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1243-dni-(continued...)

objectives are particularly germane to a discussion of cross-cutting issues because they are management focused and IC-wide in scope. They "support the IC's mission"—to provide "timely, insightful, objective, and relevant intelligence to inform decisions on national security issues and events." [40]

NIS 2014 describes enterprise objectives (EOs) as follows:

- Integrated mission management—optimize capabilities to achieve unity of effort;
- Integrated enterprise management—improve IC integration and interoperability;
- Information sharing and safeguarding—improve collaboration while protecting information;
- Innovation—improve research and development, tradecraft,[41] and processes;
- People—build a more agile, diverse, inclusive, and expert workforce;
- Partnerships—improve intelligence through partnership.[42]

The cross-cutting issues examined below affect, and are affected by, NIS EOs. Improvements made in the name of in one area can jeopardize improvements in another. For example, efforts to improve "Diversity" (a cross-cutting issue examined in the section below) may include initiatives designed to promote inclusiveness while simultaneous efforts to improve the EO for "Information Safeguarding" promote exclusiveness. In tradeoffs between competing values such as diversity and security, has the IC found the right balance in its governing policies?

Selected Cross-Cutting Issues

The Intelligence Community Budget

The IC budget was selected because in an era of diminished resources and diverse threats, it is an issue that affects every IC agency. In his annual worldwide threats briefing to Congress, DNI James Clapper listed a number of national security issues facing the United States to include: violent extremists, migration and displaced people, government instability, cyber espionage and other cyber-related threats, state sponsored terrorism, weapons of mass destruction, China's and Russia's nuclear missile force and anti-satellite missile programs.[43] Theoretically, IC budget reflects a balance between these strategic priorities on the one hand, and resources on the other.

To accomplish this balancing act for the NIP, the DNI has the assistance of the Assistant Director of National Intelligence for Systems and Resource Analysis (ADNI/SRA). It is the SRA's job to help the DNI make "proactive, balanced, and effective resource decisions on issues of national

(...continued)

unveils-2014-national-intelligence-strategy?highlight=WyJzdHJhdGVneSJd.

[40] Office of Director of National Intelligence, "National Intelligence Strategy 2014," September 18, 2014, p. 2, at http://www.dni.gov/files/documents/2014_NIS_Publication.pdf.

[41] "Tradecraft" is a word used throughout the IC to mean the specific techniques associated with a particular intelligence activity. For example, analytic tradecraft refers to the body of methods used to perform intelligence analysis. Depending on context, spy tradecraft may refer to specific techniques (such as safe cracking) used by individual spies, or to a specific techniques (such as encryption) used by a particular agency (such as the NSA).

[42] Office of Director of National Intelligence, "National Intelligence Strategy 2014," September 18, 2014, p. 11.

[43] Office of the Director of National Intelligence (ODNI), "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.

importance."[44] The SRA helps the DNI determine if the NIP is balanced appropriately in terms of national priorities as defined by the NIS and the National Intelligence Priorities Framework (NIPF).[45]

The classified NIPF rank orders strategic priorities, and according to IC Directive (ICD) 204, the NIPF "is the primary mechanism to establish, disestablish, manage, and communicate national intelligence priorities." ICD-204 goes on to say that the NIPF "reflects customers' priorities for national intelligence support" meaning the priorities of both strategic- and tactical-level consumers of intelligence information, and "ensures that enduring and emerging national intelligence issues are addressed."[46]

The MIP is managed separately—by the USD(I) within the DOD's budgeting system. In the DOD, a position comparable to the SRA is the Cost and Program Evaluation Office or the "CAPE" (pronounced as one word "cāpe").[47] CAPE is a key player in helping the USD(I) achieve similar goals for the MIP in terms of the National Military Strategy (NMS), National Defense Strategy (NDS), National Security Strategy (NSS), and the Quadrennial Defense Review (QDR).[48]

The Consolidated Intelligence Guidance (CIG) provides guidance from both the DNI and the USD(I) to those individuals managing NIP and MIP resources in order to keep both programs consistent with both DOD and IC strategic priorities.

The NIP and MIP are managed separately and they are justified to Congress separately.[49] The congressional intelligence committees have exclusive jurisdiction over the NIP but share jurisdiction over the MIP with the congressional armed services committees.

Issues to Consider

1. The NIP and MIP are managed within the executive branch separately, justified to Congress separately, and overseen by congressional committees separately.
    - Are there better ways to harmonize the NIP and MIP budgets to potentially improve management and oversight?
    - How well do the NIP and MIP programs work together to address NIS, NSS, NMS, NDS, and QDR strategic priorities?
2. How balanced is the total IC budget? For example, how are resources allocated to balance

[44] ODNI/SRA, "Systems and Resource Analysis: Who We Are," accessed February 23, 2016, at http://www.dni.gov/index.php/about/organization/systems-and-resource-analyses-who-we-are.

[45] ODNI/SRA, "Systems and Resource Analysis: What We Are," accessed February 23, 2016, at http://www.dni.gov/index.php/about/organization/systems-and-resource-analyses-what-we-do.

[46] ICD-204 (D), "National Intelligence Priorities Framework," January 2, 2015, at http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf. The NIPF is a classified document.

[47] DOD, "CAPE'S MISSION" and "CAPE'S GOALS," accessed February 23, 2016, at http://www.cape.osd.mil/.

[48] Dan Elkins, *Managing Intelligence Resources*, 4th Edition, (Dewey, AZ: DWE Press, 2014), p. 6-3.

[49] The NIP is managed through the Intelligence Planning, Programming, Budgeting and Evaluation (IPPBE) system is justified in one set of budget documents called Congressional Budget Justification Books (CBJBs). The MIP is managed through the DOD's Planning, Programming, Budgeting and Execution (PPBE) system and justified in a separate set of budget documents called Congressional Justification Books (CJBs). For more on the two management processes, see Dan Elkins, *Managing Intelligence Resources*, 4th Edition, (Dewey, AZ: DWE Press, 2014), pp. 8-6 to 8-8.

- Strategic priorities versus tactical priorities?
- NIP and MIP resources within a single agency like NSA or DIA?

3. How balanced is the NIP budget? For example, how are resources allocated to balance:
    - The highest threats against the lowest threats (according to the NIPF)? or
    - Analysis against collection? or
    - Information technology (IT) against training and education?
4. How balanced is the MIP budget? For example, how are resources allocated to balance:
    - Service-specific requirements against Combatant Command requirements? or
    - Competing inter-service requirements between Army, Air Force, Navy, and Marine Corps?

Improving Analysis

Analysis was chosen as an issue because it is the primary function of the IC. Every IC component has a responsibility to support its organization's mission and the greater national security community. Nonetheless, as many point out, intelligence "is not clairvoyance,"[50] and surprises happen. Surprises are often termed intelligence 'failures' and thus, the issue of how to improve analysis is, and may always be, a focus for reform efforts.

Numerous efforts to improve analysis over the past decade have largely been driven by concerns raised about flawed analysis prior to the terrorist attacks of September 11, 2001 (9/11), and the flawed analysis in the IC's 2002 National Intelligence Estimate (NIE) regarding Iraq's Weapons of Mass Destruction (WMD) program. An after action report issued by the *WMD Commission* identified as "serious shortcomings" in the IC's analytic effort:

> Our investigation revealed serious shortcomings; specifically, we found inadequate Intelligence Community collaboration and cooperation, analysts who do not understand collection, too much focus on current intelligence, inadequate systematic use of outside experts and open source information, a shortage of analysts with scientific and technical expertise, and poor capabilities to exploit fully the available data.
>
> Perhaps most troubling, we found an Intelligence Community in which analysts have a difficult time stating their assumptions up front, explicitly explaining their logic, and, in the end, identifying unambiguously for policymakers what they do not know. In sum, we found that many of the most basic processes and functions for producing accurate and reliable intelligence are broken or underutilized.[51]

The focus on flawed analysis specifically related to 9/11 and WMD cast doubt on the quality of IC analysis in general—the validity and reliability of intelligence products—an important part of analytical "tradecraft."[52] Policymakers and their staffs wondered if any IC analytical judgment

[50] Mark Lowenthal and Ron Marks, "Intelligence Analysis: Is it as Good as it Gets?" *International Journal of Intelligence and Counterintelligence*, vol. 28, no. 4 (2015): 662-665, p. 663.

[51] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States* (Washington, DC: GPO, 2005), p. 389. (*WMD Commission Report*)

[52] Analytical tradecraft has two components: (1) Teaching analysts the agency's writing style and learning about IC collection sources so as to know which sources to draw upon; and (2) Professional and ethical values, standards, and (continued...)

could be trusted. Consumers asked for more rigorous analysis—giving greater scrutiny to the analysts' assumptions and methodology, and sometimes asking to see the raw intelligence itself. Thus, the goal of many reforms over the past decade has been to improve the credibility of the IC's analytical products in the eyes of its customers.

The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 (P.L. 108-458) includes a provision that requires the DNI to ensure "accurate analysis of intelligence." The legislation calls for the DNI "to assign an individual or entity to be responsible for ensuring that finished intelligence products produced by any element or elements of the intelligence community are timely, objective, independent of political considerations, based upon all sources of available intelligence, and employ the standards of proper analytic tradecraft."[53]

One of the most far reaching IC-wide efforts to improve an analyst's critical thinking and writing skills has been the publishing and promulgation of Intelligence Community Directive (ICD) Number 203, "Analytic Standards" in 2007. ICD 203 governs the production and evaluation of intelligence analysis and analytical products.[54] Assessments are mixed on whether the standards have improved intelligence analysis.[55]

Other initiatives include restructuring of analytic cells, advanced research facilities, more systematic use of advanced (structured) analytic techniques,[56] acquisition of technology that enables better collaboration and communication between analysts,[57] improved and expanded use of data-mining tools, joint duty assignments, and academic outreach initiatives. (Several of these initiatives are discussed in greater detail later in this report.)

A recent article by IC experts Mark Lowenthal and Ron Marks concludes that in the wake of so many reforms to improve analysis, what we have now "may be as good as it can be expected to get."[58] They suggest that policymakers adjust expectations and accept that intelligence will sometimes be wrong, but also suggest a more robust "lessons learned" capability within the IC:[59]

(...continued)

expectations. See Mark Lowenthal, "Intelligence Analysis: Management and Transformation Issues," pp. 220-238, in *Transforming U.S. Intelligence,* Edited by Jennifer Sims and Burton Gerber (Washington, DC: Georgetown University Press, 2007), p. 233.

[53] P.L. 108-458, §1011 (50 U.S.C. 403-1). The DNI responded by appointing Thomas Fingar as first Deputy Director of National Intelligence for Analysis (DDNI/A) in 2005. In 2010, the DNI reorganized the IC's leadership structure, replacing the DDNI/A with a Deputy DNI for Intelligence Integration (DDII).

[54] ICD 203, "Analytic Standards," most current version is January 2, 2015, at http://www.dni.gov/index.php/intelligence-community/ic-policies-reports/intelligence-community-directives.

[55] See for example, Von H. Pigg, "Common Analytic Standards: Intelligence Community Directive #203 and U.S. Marine Corps Intelligence," Small Wars Journal, 2009, at http://smallwarsjournal.com/blog/journal/docs-temp/260-pigg.pdf; Robert Cardillo, "Intelligence Community Reform: A Cultural Evolution," *Studies in Intelligence* , vol. 54, no. 3 (2010), at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-54-no.-3/a-cultural-evolution.html. See also Richard Immerman, "Transforming Analysis: The Intelligence Community's Best Kept Secret," Intelligence and National Security, vol. 26, nos. 2-3 (April-June 2011): 159-181. This article offers an excellent historical account of the efforts to transform of analysis throughout the last decade.

[56] Structured analytic techniques have been embraced by the IC as a way to help analysts "challenge judgments, identify mental mindsets, stimulate creativity, and manage uncertainty." See for example, CIA, "A Tradecraft Primer" Structured Analytic Techniques for Improving Intelligence Analysis," March 2009, at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf.

[57] See John Gentry, "Has the ODNI Improved U.S. Intelligence Analysis?" *International Journal of Intelligence and CounterIntelligence*, vol. 28, (2015): 637–661, p. 655 for more on initiatives such as the Intelligence Community Integrated Technology Enterprise (ICITE), and A-Space Chat Rooms.

[58] Mark Lowenthal and Ron Marks, "Intelligence Analysis: Is it as Good as it Gets?" *International Journal of*
(continued...)

> There may not always be remedies, but for serious analytic lapses there should be an equally serious intellectual (as opposed to political) inquiry as to what went wrong. The problem may be flawed analysis. But the problem may also be that the answer was not necessarily knowable. This lessons-learned capability should also be a price for allowed occasional analytic fallibility.[60]

Some experts on intelligence analysis within the IC, such as Dr. John Gentry, note that among other things, a major problem with analysis in the IC is the critical thinking and writing skills of newly hired analysts. He argues that problem of "personnel shortcomings" undercuts many efforts to impose higher analytic standards:

> Incomprehensibly, some IC agencies continue to hire for analyst positions people who have trouble with basic cognitive and written communications skills. After identifying weak analysts, many agency managers are unwilling to ask their inappropriately hired people to find other lines of work to which they are better suited—a monument to weak leadership, political correctness, and dysfunctional federal personnel regulations.[61]

Gentry suggests reform of IC hiring practices with an emphasis on hiring "older people with excellent education and/or experience *and* demonstrable good judgment."[62] The section below on diversity suggests that hiring processes in the IC may be poorly designed to hire talented individuals—not only in terms of diversity, but also in terms of acquiring the brightest and best educated.

Gentry also offers another area for improvement that has received little attention—increased awareness of the role of managers of analysts in reform strategies. He argues that "[r]eforms will only be effective if they make managers want to change the ways they and their organizations do business."[63]

> First, and most important,... analysts and managers share responsibility for the performance of their agencies. Managers and their policies usually are root causes of intelligence successes and failures because they shape the demography, training, work assignments, performance standards, and ethics of the analyst corps. Even when individual analysts make mistakes that produce corporate analytic failures, they do so as designated agents of managers.[64]

Issues to Consider:

1. Is the IC recruiting the best educated analysts in terms of their critical thinking and writing skills?

(...continued)

Intelligence and Counterintelligence, vol. 28, no. 4 (2015): 662-665, p. 663.

[59] Mark Lowenthal and Ron Marks, "Intelligence Analysis: Is it as Good as it Gets?" *International Journal of Intelligence and Counterintelligence*, vol. 28, no. 4 (2015): 662-665, p. 663.

[60] Mark Lowenthal and Ron Marks, "Intelligence Analysis: Is it as Good as it Gets?" *International Journal of Intelligence and Counterintelligence*, vol. 28, no. 4 (2015): 662-665, p. 664.

[61] John Gentry, "Has the ODNI Improved U.S. Intelligence Analysis?" *International Journal of Intelligence and CounterIntelligence*, vol. 28, (2015): 637–661, p. 647.

[62] John Gentry, "Has the ODNI Improved U.S. Intelligence Analysis?" *International Journal of Intelligence and CounterIntelligence*, vol. 28, (2015): 637–661, p. 655.

[63] John Gentry, "Managers of Analysts," *International Journal of Intelligence and Counterintelligence*, vol. 31, no. 2 (2016): 154–177, p. 155.

[64] John Gentry, "Managers of Analysts," *International Journal of Intelligence and CounterIntelligence*, vol. 31, no. 2 (2016): 154–177, p. 175.

- What is the IC doing to improve recruitment, education, and retention of its best analysts?
- How is excellence in critical thinking and writing skills rewarded and/or discouraged?

5. How might IC reform efforts work if the role of intelligence analyst manager was taken into account in reform planning and execution?
6. What "lessons learned" and "best practices" mechanisms exist within the IC to enable its professionals to learn from past successes and failures?
7. Do the intelligence services of other countries face similar problems in their analytic communities? Does the IC look beyond U.S. borders for "best practices"?

Addressing Concerns Related to "Big Data"

Across the federal government, agencies are developing systems designed to collect and store vast amounts of unstructured data for possible subsequent analysis. The IC is no exception. The IC-wide effort to deal with large-scale data accumulation, informally referred to as "big data," is another cross-cutting issue that affects every IC agency. Ideally, big data solutions offer a way to meet enterprise objectives that focus on integration, interoperability, collaboration and information protection.

An activities report for the 95th Congress produced by the Senate Select Committee on Intelligence (SSCI) characterizes "the information explosion" as "the most challenging issue before the Committee."[65] The following passage from the 1979 report reveals just how long Congress has been dealing with what many think of as a relatively new issue:

> The increasingly vast amount of knowledge available throughout the world clearly cannot be used without the assistance of new and expensive technology. New analytic innovations and greater intellectual efforts are necessary. The analysis of military questions is reasonably well in hand, but work must be done on political-social analysis and on ways in which analyses of social, cultural and economic behavior may be applied to the problems of foreign policy and defense.[66]

Some efforts to cope with big data are agency-centric. For example, CIA has a new Directorate for Digital Innovation, NSA has initiated a Trusted Systems Research Group, and NSA has partnered with North Carolina State University to fund a new Laboratory for Analytic Science.[67] Other efforts are government-wide. For example, within the DOD and IC, large-scale data collection and analysis projects are conducted by public and private research activities to include: Defense Advanced Research Projects Agency (DARPA); Intelligence Advanced Research and Projects Activity (IARPA); Advanced Research Projects Agency-Energy (ARPA-E); and the National Laboratories.

The IC Information Technology Enterprise (IC ITE, pronounced "eyesight") is an initiative focused on many of the challenges associated with big data. A work in progress, it provides a

[65] U.S. Congress, Senate Committee on Intelligence, *Report to the Senate covering the period May 16, 1977—December 31, 1978*, 96th Cong., 1st sess., May 14, 1979, S. Rept. 96-141 (Washington, DC: GPO, 1979), p. 7.

[66] U.S. Congress, Senate Committee on Intelligence, *Report to the Senate covering the period May 16, 1977—December 31, 1978*, 96th Cong., 1st sess., May 14, 1979, S. Rept. 96-141 (Washington, DC: GPO, 1979), p. 7.

[67] "NSA Announces Partnership with NC State University in Big Data," at https://cims.ncsu.edu/nsa-announces-partnership-with-nc-state-university-in-big-data/.

common IC desktop, secure online collaboration tools, and secure common cloud architectures at the top secret level.[68] The IC's desire is that IC ITE will help the IC to pool IT resources, cut future costs, increase data storage capabilities, increase mission agility and efficiency, and increase the ability to protect all levels of data.[69] The IC's Chief Information Officer (CIO) is responsible for overseeing this IC-wide initiative. The CIO describes IC ITE this way:

> IC ITE moves the IC from an agency centric IT architecture to a common platform where the Community easily and securely shares technology, information, and resources. By managing and providing the Community's IT infrastructure and services as a single enterprise, the IC will not only be more efficient, but will also establish a powerful platform to deliver more innovative and secure technology to desktops at all levels across the intelligence enterprise. These new capabilities, with seamless and secure access to Community-wide information, will positively and deeply change how users communicate, collaborate, and perform their mission.[70]

The IC ITE initiative relies heavily on the IC's industrial base to provide the underlying IT infrastructure. An industry perspective offered by the Intelligence and National Security Alliance (INSA) suggests a number of ways to foster a successful IC ITE implementation, to include:

- Transparency—on the way in which software applications, mission capability and infrastructure will be funded, acquired, and integrated;
- A metrics-driven governance process that constantly incorporates customer feedback; and
- The development of new skill sets in the workforce—to include expertise in areas such as service-level agreements, revenue models, and new cybersecurity capabilities.[71]

The DOD version of IC ITE is the Joint Information Environment (JIE). Its focus is on a common architecture at the secret and unclassified level. It stores and shares data relating to intelligence as well as operational, logistical, and other aspects of the military's warfighting efforts. The Defense Information Systems Agency (DISA) has been given responsibility for the technical aspects of JIE and leads the JIE Technical Synchronization Office (JTSO), which includes agency staff, as well as representation from the military services, IC, and National Guard.[72]

Issues to Consider:

1. Is the IC partnering with industry, other federal agencies, such as the DISA, or other countries to jointly develop big data systems such as IC ITE?

---

[68] On August 16, 2013, the IC ITE initiative reached its initial baseline milestone, with the limited deployment of a common IC desktop, the launch of the first installment of the IC cloud, and the opening of a community-wide applications mall. See Kristin Quinn, "IC ITE Moves Forward: First Round of Deployments for Common Intelligence Community ," October 9, 2013, at http://trajectorymagazine.com/got-geoint/item/1570-ic-ite-moves-forward.html#sthash.vlNRjZgi.dpuf.

[69] For more on IC ITE goals, see Chief Information Officer, Office of the DNI, "IC ITE Strategy: 2016-2020," at http://www.dni.gov/files/documents/CIO/IC%20ITE%20Strategy%202016-2020.pdf.

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

[71] IC ITE Task Force, "IC ITE: Industry Perspectives," Intelligence and National Security Alliance, *White Paper*, September 2014, at http://www.insaonline.org/i/d/a/Resources/iciteperspectives.aspx.

[72] Defense Information Systems Agency, "About Joint Information Environment," at http://www.disa.mil/about/our-work/jie.

- Can the IC point to examples of successful partnering in this area?

2. As IC ITE moves the IC from an agency-centric IT architecture to a common platform where the Community easily and securely shares technology, information, and resources, who owns the information stored in the cloud? Does ownership matter?
3. Has a metrics-driven governance process been established to constantly incorporate feedback as suggested by industry partners?
4. Does IC ITE's common platform help or hinder counterintelligence efforts such as continuous evaluation?
5. Related to the INSA Report recommendations—What human resources/training initiatives exist to:
    - Increase training for the current workforce,
    - Recruit new IT talent,
    - Rotate IT talent with industry, and
    - Collaborate with colleges and universities to develop the necessary curriculums to handle the challenges associated with the collection, management, and analysis of big data?

Diversity

Diversity was selected because initiatives designed to attract and retain a diverse workforce have been recurring themes in intelligence-related legislation and IC policy directives over the past decade.[73] Agency directors regularly remark that greater diversity leads to a greater chance for "mission success" by decreasing the impact of shared, common biases. In June 2015, John Brennan, Director of the CIA, stated, "Diversity—of thought, ethnicities, backgrounds, and experiences—is essential to CIA's mission success, and we need it at every level of our enterprise."[74] DNI Clapper has been also been a vocal advocate for a diverse workforce.[75] The IC has developed a number of policies and programs associated with improving the diversity of its workforce. The IRTPA of 2004 (P.L. 108-458, Section 1011) directed the DNI to lead IC wide efforts in this regard, and to make them consistent with diversity policies in the DOD.[76]

[73] There have also been a number of initiatives designed to attract and retain individuals with critical skills such as certain foreign languages and cyber-related training. Both diversity and critical skills are seen as necessary components of IC mission success.

[74] John Brennan, "Statement from Director John Brennan on Improving Leadership Diversity at CIA," June 30, 2015, at https://www.cia.gov/news-information/press-releases-statements/2015-press-releases-statements/director-brennan-statement-on-improving-leadership-diversity-at-cia.html.

[75] See for example, James R. Clapper, *Statement on IC Equal Employment Opportunity and Diversity*, Office of the DNI, November 16, 2010, at http://www.intelligence.gov/eeo-diversity-statement/. For more on the organizational benefits of diversity, see CRS Report R44321, *Diversity, Inclusion, and Equal Opportunity in the Armed Services: Background and Issues for Congress*, by (name redacted) .

[76] DODD 1020.02E, *Diversity Management and Equal Opportunity in the DOD*, June 8, 2015, Part II, "Definitions," at http://www.dtic.mil/whs/directives/corres/pdf/102002E.pdf. The DOD defines diversity as: "All the different characteristics and attributes of the DOD's total force, which are consistent with DOD's core values, integral to overall readiness and mission accomplishment, and reflective of the Nation we serve." The DOD's *Diversity and Inclusion Strategic Plan* explains that the definition encompasses not only demographic characteristics, but also different backgrounds, skills, and experiences.

IC Directive (ICD) 110 provides policy guidance on Equal Employment and Opportunity (EEO) and Diversity.[77] According to ICD-110,

> [T]the IC will foster diversity in its workforce through the recruitment, development, and retention of minorities, women, persons with disabilities, and individuals of various backgrounds, cultures, generations, perspectives, and ideas, among other aspects. *To combat new and increasingly complex national security threats, the IC shall have a dynamic and agile workforce that reflects diversity in its broadest context*.[78]

The DNI's management team includes an Assistant Director for Human Capital (ADNI/HC) responsible for all human capital related legislative issues, to include the EEO and outreach function.[79] The only publicly available *IC Strategic Human Capital Plan* is dated June 22, 2006.[80] Goal one is to build an "agile, 'all source' workforce,"

- "optimized by its mix of military and civilian employees, contractors, and international and academic partners," and
- "seamlessly integrated to achieve maximum agility and enabled by an enterprise human resource policy and information architecture that allows easy movement across organizational lines."[81]

The IC conducts virtual career fairs where it can place special emphasis on recruiting diverse candidates proficient in mission critical foreign languages and cultural expertise.[82] Other initiatives designed to recruit those who meet critical skills and diversity goals have included:

> targeted IC-wide minority recruiting outreach effort; for example, in FY 2006 the IC recruiting team made visits to national conferences sponsored by the Hispanic Professional Engineers Association, American Indians Science and Engineering Society, Asian Diversity, National Careers for the Disabled, and the Thurgood Marshall Scholarship Fund, in addition to Historically Black Colleges and Universities (HBCUs) and Hispanic Association of Colleges and Universities (HACU) member institutions.[83]

A number of Intelligence Authorization Acts (IAAs) have included provisions designed to increase diversity through reporting requirements, outreach, hiring and retention, and grants to academic institutions. The success of failure of these provisions is not clear from publicly available documents. Legislative efforts to promote diversity include:

---

[77] ICD-110, "Intelligence Community Equal Employment and Opportunity and Diversity," July 1, 2009, at http://www.dni.gov/files/documents/ICD/ICD_110.pdf.

[78] Emphasis added to highlight link between diversity and IC's ability to combat national security threats.

[79] See IC Chief Human Capital Officer, "Who We Are," at http://www.dni.gov/index.php/about/organization/chief-human-capital-office-who-we-are. The ADNI/HC is also known as the Chief Human Capital Officer (CHCO) or "Cheecko." Deborah Kircher is the current ADNI/HC.

[80] ODNI, *The U.S. IC's Five Year Strategic Human Capital Plan: An Annex to the National Intelligence Strategy*, June 22, 2006, at http://www.dni.gov/files/documents/CHCO/human%20capital%20plan-2006.pdf. This is the only plan referenced on the ADNI/HC website. There is no indication that a more recent document exists, even in classified form.

[81] ODNI, *The U.S. IC's Five Year Strategic Human Capital Plan: An Annex to the National Intelligence Strategy*, June 22, 2006, p. 8.

[82] See for example, "Intelligence Community—Virtual Career Fair March 3, 2016," at http://blogs.wayne.edu/engineeringjobs/2016/02/22/intelligence-community-virtual-career-fair-march-3-2016-2pm-8pm-registration-info-in-post/.

[83] Office of the DNI, *The U.S. IC's Five Year Strategic Human Capital Plan: An Annex to the National Intelligence Strategy*, June 22, 2006, p. 20.

- The IAA for FY2003 (P.L. 107-306, Section 324) requires an annual report on hiring and retention of minority employees in the IC. Each report must include disaggregated percentage data from each element of the IC on all employees during the previous fiscal year in reference to (1) racial and ethnic minorities; (2) women; and (3) individuals with disabilities.[84]
- The IAA for FY2004 (P.L. 108-177, Section 319) focuses on improving IC EEO outreach efforts. It required a pilot project designed to promote EEO "using innovative methodologies." One such outreach initiative has been the creation of IC Centers of Academic Excellence (IC CAE). The IC CAE Program's aim is to "increase the pool of eligible applicants in core skills areas, specifically targeting women and racial/ethnic minorities with varied cultural backgrounds, regional and geographical expertise, skills, language proficiency, and related competencies." It does this primarily through a grant program open to all accredited four-year colleges and universities in the United States. Information on this program is available in its Program Plan.[85]
- The IAA for FY2010 (P.L. 111-259, Section 338) requires a report on the plans of each such IC element to increase diversity including specific plans associated with equal employment opportunity and diversity; recruiting and hiring of diverse candidates; retention of diverse Federal employees at the junior, midgrade, senior, and management levels; diversity awareness training and education programs for senior officials and managers of each such element; and performance metrics.
- The IAA for FY2011 (P.L. 112-18, Section 403) requires the IC Inspector General (IG) to submit a report on "the degree to which racial and ethnic minorities in the United States are employed in professional positions in the intelligence community and barriers to the recruitment and retention of additional racial and ethnic minorities in such positions." The IG Report and reports on specific numbers associated with the IC workforce are classified.
- The IAA for FY2016 (P.L. 114-113, Division M, Section 712) allows the DNI to provide grants to historically black colleges and universities, predominantly Black institutions, Hispanic-serving institutions, and Asian American and Native American Pacific Islander-serving institutions. The grants are to provide programs of study in the following educational disciplines: (1) Intermediate and advanced foreign languages deemed in the immediate interest of the intelligence community, including Farsi, Pashto, Middle Eastern, African, and South Asian dialects; and (2) Study abroad programs and cultural immersion programs.

Efforts to promote diversity emphasize the need to *identify, attract, hire and retain* targeted individuals.[86] Anecdotal evidence suggests that although the IC is identifying and attracting well-qualified candidates, it loses many candidates through its lengthy and cumbersome hiring process.

[84] P.L. 107-306 amended U.S.C. 50 §3050. The language has been amended over time (with technical corrections such as changing DCI to DNI) and can be found at http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title50-section3050&num=0&edition=prelim.

[85] "Guidance and Procedures," *IC CAE Program Plan for Fiscal Years 2005-2025*, April 2005, at https://www.nsu.edu/Assets/websites/iccae/pdf/Guidance-and-Procedures.pdf.

[86] See for example, the *DOD Diversity and Inclusion Strategic Plan 2012*, goal 2.

A number of government-wide, long-standing problems are associated with the personnel hiring process such as:

- Fragmented governance and uncoordinated leadership that hinders the ability to meet federal workforce needs;
- Complicated processes and rules;
- Disconnects between front-line hiring managers and government HR specialists.[87]

Despite widespread and long-standing recognition of hiring problems; they persist.[88] The most common complaints appear to be the length of time required and the lack of feedback during the waiting period. The "application timeline" available on the intelligence careers website warns potential applicants to expect a wait of as many as 28 weeks for a job at DIA, NSA, NGA or the ODNI. The security and testing portion make take up to 15 of the 28 weeks, depending on the agency in question.[89] Many talented individuals will accept other job opportunities during a waiting period that may extend 8 months.[90]

Publicly available sources do not reveal to what extent the IC is making its hiring processes more 'user-friendly.' Based on a search of websites associated with IC hiring, there appears to be progress toward a portal for all IC agencies—where those interested in a career in the IC can find out how, when, where and why to apply. The intelligence.careers.gov website identifies all 17 components of the IC, but only DIA, NGA, NSA and the ODNI are "participating agencies" on that site. It may be that a common application form—used as a first step for all IC agencies—is possible and is being developed. It may also be possible that other screening processes, such as psychological testing and evaluation, is being streamlined—so that the first steps in the application process for DIA are identical to those for NGA.[91]

Retention is also an important part of workforce diversity. The *DOD Diversity and Inclusion Strategic Plan* addresses the need to "develop, mentor, and retain top talent from across the total force" through strong mentoring programs, workplace flexibility policies, and efforts to meet personal and professional development goals.[92] The IC may have a need for similar types of retention programs.

Issues to Consider

1. In reference to the IC's *Strategic Human Capital Plan:*

[87] William Jackson, "Do federal hiring processes discourage qualified applicants?" September 10, 2009, at https://fcw.com/articles/2009/09/08/cybereye-it-security-professional-shortage.aspx; and John Stein Monroe, "Five Problems with federal hiring—and 5 reality checks," September 24, 2009, at https://fcw.com/articles/2009/09/08/cybereye-it-security-professional-shortage.aspx.

[88] Websites that post the positive and negative experiences of individuals interviewed for employment, such as http://www.glassdoor.com, reveal that the problems associated with the hiring process are still common despite years of complaints.

[89] The intelligence careers website applies only to DIA, NSA, NGA and ODNI. See "Application Timeline," at https://www.intelligencecareers.gov/icapply.html.

[90] See for example, NGA and ODNI timelines on "Application Timeline," at https://www.intelligencecareers.gov/icapply.html.

[91] Perhaps it will be possible in the future for a candidate to apply for a job in any IC agency with one application. Human Resources personnel could possibly identify and contact the most suitable new hires from a talent pool made up of all applicants.

[92] DOD Diversity and Inclusion Strategic Plan 2012, Goal 3.

- What is the IC's current workforce composition?
- How does the IC define diversity?
- Is any part of today's IC "optimized by its mix of military and civilian employees, contractors, and international and academic partners," and "seamlessly integrated to achieve maximum agility and enabled by an enterprise human resource policy and information architecture that allows easy movement across organizational lines."[93]
- Has the IC's *Strategic Human Capital Plan* been updated since 2006?

2. What progress is being made toward ICD-110's goal of a "dynamic and agile workforce that reflects diversity in its broadest context"?
    - How is progress being measured?
3. How effective have the programs associated with legislative provisions related to diversity been at helping the IC to meet its workforce goals?
4. What steps are being taken to make the hiring process more efficient and effective across the IC?
    - What hiring programs are working well or working poorly?
    - If working well, are "best practices" being shared across the IC?
    - If working poorly, what efforts are being made to improve the programs?
    - Are industry "best practices" being considered to improve IC hiring processes?
    - Are there ways to better integrate the IC's 17 different personnel systems?
    - Do the intelligence services of other countries face similar hiring problems? Does the IC look beyond U.S. borders for "best practices"?
5. What do retention efforts look like across the IC?
    - Should they be more or less uniform?
    - Are "best practices" being shared?

Global Coverage of Threats and Accepting More Risk

Global coverage[94] of threats was selected because the IC's acknowledgment that the IC cannot "cover the world," and that the United States must "accept more risk" has national security

[93] ODNI, *The U.S. IC's Five Year Strategic Human Capital Plan: An Annex to the National Intelligence Strategy*, June 22, 2006, p. 8.

[94] The term is associated with a number of IC leaders, to include former-DNI John Negroponte in his 2007 Annual Threat Assessment: "We know that the nation requires more from our Intelligence Community than ever before because America confronts a greater diversity of threats and challenges than ever before. Globalization, the defining characteristic of our age, mandates global intelligence coverage." Testimony of DNI John Negroponte, in U.S. Congress, Senate Select Committee on Intelligence, *Annual Threat Assessment*, hearings, 110th Cong., 2nd sess., January 11, 2007, S.Hrg. 110-835 (Washington, DC: GPO, 2007) at http://www.intelligence.senate.gov/hearings/current-and-projected-national-security-threats-united-states-january-11-2007. Quote taken from formal opening statement, p. 1, available at http://www.dni.gov/files/documents/Newsroom/Testimonies/20070111_testimony.pdf. This hearing also contains the testimony of DCIA Michael Hayden. According to DCIA Hayden, IC disciplines such as open source intelligence (OSINT) were developed, in part, "to meet the challenge of global coverage."

implications that deserve attention. Global coverage is a concept used to describe the IC's need to prepare for and respond to any and all crises and threats—worldwide.[95] In 2014, DNI Clapper noted the difficulties of providing global coverage in a period of expanding threats and reduced budgets and noted "the inescapable imperative to accept more risk":

> Looking back over my now more than half a century in intelligence, I've not experienced a time when we've been beset by more crises and threats around the globe. My list is long. It includes the scourge and diversification of terrorism, loosely connected and globally dispersed, to include here at home, as exemplified by the Boston Marathon bombing and by the sectarian war in Syria, its attraction as a growing center of radical extremism and the potential threat this poses now to the homeland. …
>
> The stark consequences of this perfect storm are pretty evident. The intelligence community is going to have less capacity to protect our nation and its allies than we've had in the past. …
>
> We're thus faced collectively, and by collectively, I mean this committee, the Congress at large, the executive branch, and most acutely, all of us in the intelligence community, with the inescapable imperative to accept more risk.[96]

The IC has responded to the challenge of doing more with less in a number of ways. Typical of any bureaucracy, the IC begins by allocating fewer resources to lower priority challenges.[97] The National Intelligence Priorities Framework (NIPF) is crucial to this process. Recall from the section above on the IC budget that the NIPF is the principle vehicle for rank-ordering national intelligence priorities. Due to the classified nature of the NIPF, there are no publicly available assessments to indicate how well the NIPF actually reflects the IC's most pressing problems or how well resources are distributed based on NIPF priorities.

Other solutions to global coverage include:

- More robust open-source intelligence capabilities;[98]
- Developing tools for improved warning through social media;[99]
- Expanding the pool of expertise and information with outreach programs (e.g., to subject matter experts in academic institutions) and more robust intelligence sharing arrangements with foreign partners;[100] and
- Facilitating surge capability—the ability to move resources quickly to address immediate, usually ad hoc, needs.[101]

[95] John A. Kringen, "Rethinking the Concept of Global Coverage in the U.S. Intelligence Community," *Institute for Defense Analysis*, May 2015, at https://www.ida.org/~/media/Corporate/Files/Publications/IDA_Documents/IAD/2015/D-5491.pdf. Also available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-59-no-3/pdfs/Keeping-Watch-on-the-World.pdf. According to Kringen, the concept originated in the early 1990s, after the end of the Cold War.

[96] Testimony of DNI James R. Clapper, in U.S. Congress, Senate Armed Services Committee, *Worldwide Threat Assessment*, hearings, 113th Cong., 2nd sess., February 11, 2014, S.Hrg.113-571 (Washington, DC: GPO, 2014) at http://www.armed-services.senate.gov/imo/media/doc/14-07%20-%202-11-14.pdf.

[97] John A. Kringen, "Rethinking the Concept of Global Coverage in the U.S. Intelligence Community," *Institute for Defense Analysis*, May 2015, p. 1.

[98] The Open Source Enterprise (OSE)—established by the DNI in 2005 as the Open Source Center and successor organization to CIA's Foreign Broadcast and Information Service (FBIS)—redesignated OSE in October 2015. OSE has the lead role for OSINT within the community.

[99] Kringen, p. 4.

[100] According to Kringen, p. 4, the DNI's National Intelligence Council (NIC) and State Department's Bureau of Intelligence and Research (INR) are particularly active in outreach activities.

John Kringen,[102] former CIA Director of Intelligence, echoes DNI Clapper's assessment that the IC lacks the necessary resources to provide global coverage.[103] Kringen argues that the IC's current approach is "necessary but insufficient."[104] He believes that the IC needs to do a better job at explaining what the IC can and cannot be expected to do with the resources at its disposal.[105] He also believes the IC needs to develop more robust and systematic assessments of risk and examine lessons learned from past global coverage crises.[106] And finally, Kringen suggests the IC develop new outreach efforts that it can exert in a crisis with little cost.[107] He offers three concrete suggestions:

1. Engage with outside experts in lower priority topic areas and "establish a foundation for collaboration when it may be required";
2. Use targeted investments to take better advantage of government capabilities outside the NIP such as the military components (e.g., Joint Reserve Intelligence Centers) and the law enforcement community.
3. Establish "dedicated 'knowledge broker" units outside the IC—organizations that "serve as a vehicle to reach out to private sector experts, including those from academia, business, and Federally Funded Research and Development Centers to build relationships between private sector researchers and experts within the IC.[108]

Issues to Consider

1. Many argue that as budgets decrease and threats increase, the IC lacks adequate resources to cover the globe.
    - Should the IC be expected to monitor every corner of the world every hour of the day?
    - Should the IC rely more on partnerships with other countries?
2. What steps might the IC take to manage expectations?

(...continued)

[101] Kringen, p. 5: "An enduring concern regarding global coverage accounts is the IC's ability to foresee and to respond rapidly to developments in countries allocated limited collection and analytic resources."

[102] John A. Kringen is an Adjunct Staff Member at the Institute for Defense Analysis (IDA). Before joining IDA in 2012, he served with the Central Intelligence Agency for thirty-three years and was Director of Intelligence during 2005–2008.

[103] John A. Kringen, "Rethinking the Concept of Global Coverage in the U.S. Intelligence Community," Studies in Intelligence, vol 59, no. 3 (September 2015), p. 1, at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-59-no-3/pdfs/Keeping-Watch-on-the-World.pdf. Article also available at John A. Kringen, "Rethinking the Concept of Global Coverage in the U.S. Intelligence Community," Institute for Defense Analysis, May 2015, at https://www.ida.org/~/media/Corporate/Files/Publications/IDA_Documents/IAD/2015/D-5491.pdf.

[104] Kringen, p.7.

[105] Kringen, p. 8.

[106] Kringen, p. 9.

[107] Kringen, p. 9.

[108] Kringen, p. 9. According to Kringen: "One of the recommendations of the WMD Commission that was not implemented was 'the establishment of at least one not-for-profit research institute to serve as a critical window into outside expertise for the Intelligence Community.' The commission envisioned an organization not directly managed by the IC whose principal mission was to serve as a vehicle to reach out to private sector experts, including those from academia, business, and Federally Funded Research and Development Centers.

3. What authorities are needed to enhance cooperation with outside experts?

Security Clearances and Continuous Evaluation

Issues associated with the security clearance process have affected all IC agencies for decades.[109] Current priorities include improving access to relevant information, especially state and local law enforcement records; accelerating the shift to a "continuous evaluation" (CE) model across government; improving risk management approaches, including reduction of the total number of clearance holders and the backlog of periodic reinvestigations; and improving IC-wide management of information technology and resources.[110] A current issue from a privacy and civil liberties perspective is the expanded use of publicly available data when reviewing the backgrounds of security clearance holders.

Security clearance levels correspond to the sensitivity of the information that cleared individuals will be eligible to access.[111] The three levels include:

1. Confidential (C), the unauthorized disclosure of which would "cause damage to the national security,"
2. Secret (S), the unauthorized disclosure of which would "cause serious damage to the national security," and
3. Top Secret (TS), the unauthorized disclosure of which would "cause exceptionally grave damage to the national security."[112]

Individuals who hold security clearances are subject to an initial background investigation followed by periodic reinvestigations.[113] Unlike a periodic reinvestigation, CE is intended to be ongoing and may occur at any time during an individual's period of security clearance eligibility.

The issue of, and need for CE, is associated with a number of factors, to include opportunities presented by new technologies like social media and high-profile security-related incidents such as the Washington Navy Yard shooting by Aaron Alexis and the Edward Snowden disclosures of NSA's collection programs.[114] Both Alexis and Snowden were investigated, adjudicated and

[109] Michelle Christensen, Analyst in Government Organization and Management, contributed to this section. For more on security clearances and the security clearance process, see CRS Report R43216, *Security Clearance Process: Answers to Frequently Asked Questions*, by (name redacted) and (name redacted) .

[110] For more on current priorities and measuring progress to date, see "Cross Agency Priority Goal Quarterly Progress Update: Insider Threat and Security Clearance Reform," FY2015 Quarter 2, power point briefing, at http://fedne.ws/uploads/070615_omb_insiderthreat.pdf.

[111] See Executive Order 12968, "Access to Classified Information," 60 *Federal Register* 40245, August 2, 1995.

[112] Executive Order 13526, "Classified National Security Information," 75 *Federal Register* 707, December 29, 2009. Two major categories of classified information are commonly associated with Top Secret information: Sensitive Compartmented Information (SCI), which refers to intelligence sources and methods, and Special Access Programs (SAPs), which refers to highly sensitive policies, projects, and programs.

[113] Currently, the Office of Personnel Management, Federal Investigative Services (OPM-FIS) oversees the majority of background investigations. For more on security clearances, see CRS Report R43216, *Security Clearance Process: Answers to Frequently Asked Questions*, by (name redacted) and (name redacted) .

[114] The Washington Navy Yard shooting, by a former Navy reservist named Aaron Alexis, took place on September 16, 2013. The disclosures of NSA's collection programs, by contractor Edward Snowden, began in June 2013. For more on the Navy Yard shooting, see Michael Shear and Michael Schmidt, "Gunman and 12 Victims Killed in Shooting at D.C. Navy Yard, New York Times, September 16, 2013, at http://www.nytimes.com/2013/09/17/us/shooting-reported-at-washington-navy-yard.html?pagewanted=all&_r=0. For more on the Snowden leaks, see Dustin Volz, "Everything We Learned from Edward Snowden in 2013," *National Journal*, December 31, 2013, at http://www.nationaljournal.com/s/64142/everything-we-learned-from-edward-snowden-2013.

credentialed through the traditional security clearance process. One DOD investigation of the Navy Yard shooting recommended CE, based in part, on its finding that:

> *[p]otentially useful security-related information often goes unnoticed during the long periods between reinvestigations of cleared individuals*. For example, over a month before the Navy Yard shooting, Alexis displayed psychotic behavior to active duty police force members at Naval Station Newport, to civilian police officers in the town adjacent to the base, and to coworkers. Even earlier, Alexis did not sufficiently self-report his contact with law enforcement during his service in the Navy. These incidents affecting his continued eligibility were not investigated or were missed altogether.[115]

Any individual who has been deemed eligible to hold a security clearance may be subject to CE.[116] The IAA for FY2014 requires that the background of each IC employee, officer, or contractor be "monitored on a continual basis" as long as he or she is eligible to access classified information.[117] Under the IAA for FY2014 and E.O. 13467, the DNI is responsible for determining the standards for CE, including the frequency of evaluations for the most sensitive TS and TS/SCI population.[118]

On December 18, 2015, President Obama signed the Consolidated Appropriations Act, 2016 (P.L. 114-113), which contained the IAA for FY2016.[119] Section 306, titled "Enhanced Security Clearance Programs," requires all agencies under the direction of the DNI, to implement enhanced personnel security clearance checks of employees and contractors who either hold a security clearance or are in a national security sensitive position.[120] Under P.L. 114-113 agencies should "integrate relevant and appropriate information from various sources, including government, publicly available, and commercial data sources, consumer reporting agencies, social media, and such other sources as determined by the Director of National Intelligence."[121] One issue from a privacy and civil liberties perspective is that while the legislation says agencies should use social media when reviewing clearance holders, it doesn't describe exactly how they should use it, what they should look for, or how they should interpret the information they find. The DNI is required to develop such guidelines.

Along with its recommendations for increased use of CE, a DOD report on the Washington Navy shooting recommended use of the Fair Information Practice Principles (FIPP) framework to provide necessary privacy protections. Among other things, the report suggested that a CE framework should include:

---

[115] U.S. Department of Defense, *Security from Within: Independent Review of the Washington Navy Yard Shooting*, November 2013, p. 15, at http://www.defense.gov/Portals/1/Documents/pubs/Independent-Review-of-the-WNY-Shooting-14-Nov-2013.pdf. Emphasis added.

[116] §3.5 of E.O. 12968, as amended by E.O. 13467.

[117] P.L. 113-126, §501; 128 Stat. 1411.

[118] Ibid; §3.5 of E.O. 12968, as amended by E.O. 13467. This responsibility is also noted in Appendix A of U.S. Office of Management and Budget, *Suitability and Security Processes Review Report to the President*, February 2014, at http://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf (hereafter, OMB *Security Processes Review*), p. 24.

[119] The law contains 17 divisions. The IAA for FY2016 can be found in "Division M", under "TITLE III—GENERAL PROVISIONS."

[120] P.L. 114-113 §306 (a) amends 5 U.S.C. by adding §11001 (Chapter 110—Enhanced Personnel Security Programs). "Covered individuals" are defined in §11001 (e) (3). "Covered agencies" are defined as those specified in P.L. 108-458, §3001: (1) The term ``agency'' means-- (A) an executive agency (as that term is defined in Section 105 of title 5, United States Code); (B) a military department (as that term is defined in Section 102 of title 5, United States Code); and (C) an element of the intelligence community.

[121] P.L. 114-113 §306 (a): §11001 (b) (1).

- transparency,
- individual consent,
- legal authorities,
- data minimization (only information that is relevant and necessary),
- data use limited to investigation purposes only, and
- safeguards to ensure data accuracy, integrity and security.[122]

P.L. 114-113, Section 306 requires agency Inspectors General (IGs) to ‘‘conduct at least 1 audit to assess the effectiveness and fairness, which shall be determined in accordance with performance measures and standards established by the Director of National Intelligence, to covered individuals of the enhanced personnel security program of the agency.’’[123] The audit is to begin two years after the date of the implementation of the enhanced personnel security program.

Issues to Consider:

1. What does the IC’s continuous evaluation framework look like? Does it include privacy protections consistent with the Fair Information Practice Principles (FIPP) framework?
2. Has the program been evaluated by any independent office, such as the IG, to assess its compliance with DNI standards? If so, what was the result of the evaluation?
3. Is the IC sharing CE “best practices” with foreign intelligence services?

Polygraph Examinations

The permissible use of polygraph examinations is a controversial topic. It is related to security clearances but treated separately in this report because polygraph examinations are not necessary to the security clearance process. For example, no one in the legislative branch is subject to polygraph examinations. Concerns are repeatedly raised about alleged privacy violations, “out-of-scope” reporting of criminal activities, “false-positives” and other polygraph inaccuracies, examiner and agency inconsistencies, and over-zealous and inconsistent examiners.[124] Defenders of the polygraph praise its effectiveness in detecting lies and eliciting admissions of guilt regarding past security violations. They also praise the polygraph’s deterrent effect—e.g., its ability to deter future security violations and to deter employment applications from potentially poor security risks.[125]

[122] U.S. Department of Defense, *Security from Within: Independent Review of the Washington Navy Yard Shooting*, November 2013, pp. 17-18, at http://www.defense.gov/Portals/1/Documents/pubs/Independent-Review-of-the-WNY-Shooting-14-Nov-2013.pdf.

[123] P.L. 114-113 §306 (a): §11001 (d).

[124] See for example, newspaper articles released by the McClatchy news service included in Appendix C, Nancy Bloomberg, Office of the Inspector General, *Special Review of the NRO Polygraph Program, Final Report (Redacted*), Project Number 2012-006 S, March 31, 2014, p. iv, at http://fas.org/irp/nro/ig-polygraph.pdf. See also Shankar Vedantum, “Polygraph Test Results Vary Among Agencies,” *Washington Post*, June 20, 2006, at http://www.washingtonpost.com/wp-dyn/content/article/2006/06/19/AR2006061901415_2.html.

[125] See for example, National Research Council, *The Polygraph and Lie Detection* (Washington, DC: National Academies Press, 2003).

The polygraph machine, first constructed in the early 1900s,[126] does not detect lies. Rather, it is an instrument that charts changes in an individual's respiration, heart rate, blood pressure, and sweat gland activity in response to a series of yes-or-no questions. Polygraph examiners determine whether a person's physiological reaction is stronger in responding to certain questions when contrasted with recorded reactions to a series of comparison or "control" questions. It is believed that stronger reactions indicate deception on the part of the individual being tested. It is these physiological responses which are at the heart of the ongoing debate over the validity of polygraph testing.[127]

The polygraph examination attempts to serve two purposes: to detect deception and to reveal truth. The test itself represents an attempt to capture accurate psychophysiological indicators of deception. The "polygraph examination," however, includes both the test and the interrogation surrounding it, and is intended to be a tool for revealing truth.[128]

On balance, the IC maintains that the pros of polygraphing outweigh the cons; polygraph examinations are therefore required throughout the IC. The successful completion of any number of examinations over an individual's period of employment is required to first obtain and then retain a security clearance. IC Policy Guidance (ICPG) 704.6 provides guidance on the "Conduct of Polygraph Examinations for Personnel Security Vetting."[129] There are three types of polygraph examinations: Counterintelligence Scope Polygraph (CSP) examinations, Expanded Scope Polygraph (ESP) examinations, and Specific Issue Polygraph (SIP) examinations. According to ICPG 704.6:

- "CSP examinations shall cover the topics of espionage, sabotage, terrorism, unauthorized disclosure, or removal of classified information (including to the media), or unauthorized or unreported foreign contacts, and deliberate damage to or malicious misuse of U.S. Government information systems or defense systems.
- ESP examinations cover CSP topics plus topics of criminal conduct, drug involvement and falsification of security questionnaires and forms. The ESP examination has also been referred to as a Full Scope Polygraph (FSP) or Expanded Scope Screening (ESS) examination in some IC organizations.
- SIP examinations may be conducted to resolve an individual issue of adjudicative concern such as espionage, sabotage, unauthorized disclosure of classified information, or criminal conduct or to aid in CI investigations. The SIP examination may be used in conjunction with CSP or ESP examinations."[130]

[126] The idea of using psychophysiological recordings to measure deception in laboratory and legal settings can be traced to William Moulton Marston, largely while he was a Harvard University graduate student, 1915-1921. The origins of the modern polygraph, according to polygraph literature, are attributed variously to V.D. Benussi (1914), John A. Larson (1921), or to Leonarde Keeler (1933). See National Research Council, *The Polygraph and Lie Detection* (Washington, DC: National Academies Press, 2003), pp. 291-297.

[127] National Research Council, *The Polygraph and Lie Detection* (Washington, DC: National Academies Press, 2003), p. 13.

[128] National Research Council, *The Polygraph and Lie Detection* (Washington, DC: National Academies Press, 2003), p. 21.

[129] ICPG 704.6, "Conduct of Polygraph Examinations for Personnel Security Vetting," July 3, 2014, at http://www.dni.gov/files/documents/ICPG/ICPG%20704.6.pdf.

[130] ICPG 704.6 (D) (3-5).

The type of examination required varies within agencies and between agencies.[131] Generally speaking, most IC agencies rely on the CSP examination. However, the CIA, FBI, NSA, U.S. Secret Service, and Naval Criminal Investigative Service may require the ESP examination due to the especially sensitive nature of certain information derived from human sources.[132] Polygraphs are required randomly and periodically (generally every five to seven years), although some individuals may go years without one due the large backlog of cases.

While many federal agencies use them, their utility has been called into question. Polygraphs are known to occasionally yield "false-positive" results for a variety of reasons. For example, individuals known as "guilt grabbers" by some polygraph examiners, "feel guilty at the mere thought of having done something wrong."[133] The Supreme Court has determined that "There is simply no consensus that polygraph evidence is reliable…. To this day, the scientific community remains extremely polarized about the reliability of polygraph techniques…. Doubts and uncertainties plague even the best polygraph exams."[134] A 2003 National Academy of Sciences (NAS) report questions the scientific basis for the accuracy of polygraph testing, particularly when used to 'screen' employees.[135]

A decade of reform efforts encouraged by legislation such as the IRTPA of 2004 (P.L. 108-458)[136] and reports such as the one by the NAS, have yielded mixed results. According to a year-long study of the DOD's polygraph programs commissioned by the Principle Deputy, USD(I): "The polygraph has and continues to be a valuable tool in supporting and advancing DoD personnel security and counterintelligence matters, criminal investigation resolution, and mitigating the insider threat."[137] The study found the DOD in full compliance with its own polygraph requirements, to include the appeals process. However, a report published as recently as March 2014 by the NRO IG found "significant shortcomings in the administration and execution" of the NRO's polygraph program. The IG "identified material inconsistencies in examiner approaches

[131] See for example, U.S. Department of Justice, *Use of Polygraph Examinations in the Department of Justice*, September 2006, https://oig.justice.gov/reports/plus/e0608/final.pdf. According to this report, four DOJ components administered their own polygraph programs while seven other DOJ components relied on outside agencies or private contractors to operate polygraph programs. See also Shankar Vedantum, "Polygraph Test Results Vary Among Agencies," *Washington Post*, June 20, 2006, at http://www.washingtonpost.com/wp-dyn/content/article/2006/06/19/AR2006061901415_2.html.

[132] For more on the official use of polygraphs, see 10 USC §1564 "Counterintelligence polygraph program"; the most current version of DOD Instruction 5210.91, "Polygraph and Credibility Assessment (PCA) Procedures"; and the most current version of ODNI, "Security Executive Agent Directive 2."

[133] "The Polygraph Test Strikes—and Strikes Out—Again: The polygraph is an arousal detector, not a lie detector," *Psychology Today*, July 21, 2009, at https://www.psychologytoday.com/blog/the-skeptical-psychologist/200907/the-polygraph-test-strikes-and-strikes-out-again. For those who fail the polygraph for whatever reason, retesting is possible, but the appeals process is slow and often unforgiving. The careers of long-time, outstanding IC professionals may be ruined in the process of trying to clear their name.

[134] See U.S. v. Scheffer, Justice Clarence Thomas, 1998.

[135] National Research Council, The Polygraph and Lie Detection (Washington, DC: National Academies Press, 2003).

[136] Title III of the Act directs the federal government to improve the security clearance process by establishing central oversight and uniform policies for investigating and adjudicating personnel security clearances. The Act states that the federal government must begin developing and implementing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of security clearances and determinations for access to highly sensitive programs, including standardization of security questionnaires, financial disclosure requirements for security clearance applicants, and polygraph policies and procedures.

[137] Northrup Grumman/TASC, Inc./Six3Systems, Inc., "Department of Defense Polygraph Program Process and Compliance Study: Study Report," Office of the USD(I), December 19, 2011, http://www.fas.org/sgp/othergov/polygraph/dod-poly.pdf. The study lasted from May 1, 2010—April 30, 2011.

including examiners improperly raising issues not within the scope of the test."[138] These contradictory findings suggest the need for frequent, independent assessments of the polygraph program across the IC.

Issues to Consider:

1. In light of the IC's use of CE to continually monitor an employee's social and financial activity,
    - Are polygraph ex aminations still necessary?
    - Should they be used only when other warning signs (such as financial improprieties) are evident?
2. Do other foreign intelligence services use polygraph examinations for similar purposes?
    - If so, does the IC share "best practices" with those intelligence services?
3. If polygraphs are necessary,
    - What emerging technologies show the most promise in providing more objective measures to detect lying?
    - Should additional resources be directed toward encouraging such technologies?
    - Are polygraph "best practices" shared across the IC?

Transparency

This issue was selected because the current desire to restore trust through transparency bears many similarities to a period in the mid- to late-1970s when the trust in the IC was shattered by a series of articles in the *New York Times* accusing the CIA, NSA and FBI of "massive" spying and illegal intelligence operations directed against antiwar activists and other American dissidents.[139] The allegations prompted a number of investigations during 1975—a year that became known as the "Year of Intelligence."[140]

Congress convened two investigative select committees (colloquially known as the Church and Pike Committees)[141] that held open hearings and produced multi-volume reports in order to satisfy the public's desire for greater transparency. The Senate and House intelligence committees were established in 1976 and 1977, respectively, to better integrate 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. It was the responsibility of the newly created committees to represent the interests of the American public

[138] Nancy Bloomberg, Office of the Inspector General, *Special Review of the NRO Polygraph Program, Final Report* (*Redacted*), Project Number 2012-006 S, March 31, 2014, p. iv, at http://fas.org/irp/nro/ig-polygraph.pdf. (If there are IG reports related to the administration of polygraph programs in other IC agencies, they are not publicly available.)

[139] Frank J. Smist, *Congress Oversees the Intelligence Community*, Second Edition, (Knoxville: U. of Tennessee Press, 1994), p. 26. See Seymour Hersh, "Huge C.I.A. Operation Reported in U.S. Against Anti-War Forces, Other Dissidents in Nixon Years," *New York Times*, December 22, 1974.

[140] See for example, "New Online Collection of Declassified Documents Chronicles America's 'Year of Intelligence,'" June 18, 2015, at http://www.libraries.wright.edu/noshelfrequired/2015/06/18/new-online-collection-of-declassified-documents-chronicles-americas-year-of-intelligence/.

[141] The Senate "Church Committee" for its chair, Senator Frank Church, and the House "Pike Committee" for its chair, Representative Otis Pike.

by maintaining "vigilant legislative oversight" over the intelligence and intelligence-related activities of the United States.[142]

The current emphasis within the IC on providing greater transparency has a great deal to with its efforts to restore the trust of the American public—much of it lost in 2013 when Edward Snowden, a contractor working inside NSA, released thousands of classified documents to the British newspaper *The Guardian* revealing the extent of government surveillance on American citizens. The Snowden leaks came on the heels of Army Private Bradley Manning's 2010 release of thousands of classified documents to WikiLeaks revealing, among other things, the contents of State Department cables.

Across the IC, leadership champions the idea of transparency but finds implementation difficult—due in large part to an organizational culture long-trained to fear that disclosure of any intelligence-related information will compromise national security. Some suggest that greater "translucency" should be the goal, not "transparency" because translucency allows more light but keeps the details opaque.

Ann Florini, a senior fellow in Foreign Policy at Brookings, writes that those calling for increased transparency do so for many reasons to include fighting perceived corruption, enhancing public policy effectiveness and efficiency, and enforcing democratic principle of 'informed consent.'[143] Florini notes those calling for increased transparency, even those who are in top government positions, "find themselves up against powerful forces: entrenched habits, protection of privilege, and fear of how newly released information might be used, or misused."[144] She points out that there are excellent arguments for and against sharing secrets. For example, she writes: "No country wants its adversaries to have access to details about the design and potential weaknesses of weapons—but soldiers whole lives may be threatened by those weaknesses would benefit greatly from having those weapons subjected to public scrutiny before they are needed."[145]

General Michael Hayden, former director of the CIA and NSA notes the dangers associated with those who want "absolute transparency at all costs."[146] He points to the widespread public expectation of access to government documents particularly among the 'millennial generation'—people born after 1980 and before 2000.'[147] He describes the problems associated with recruiting from "Edward Snowden's generation" this way:

> The problem is that this is a generation of people whose views on secrecy, privacy, transparency, and government accountability are a bit different from the folks supervising them, and certainly different from my generation. We nonetheless need to recruit from this group because they have the skills that … NSA and CIA require to fulfil their lawful mandates. So the challenge is how to recruit this talent while also protecting ourselves

[142] H.Res. 658, *Congressional Record—House*, July 14, 1977, p. 22932.

[143] Ann Florini, "The Battle over Transparency," Introduction to The Right to Know: Transparency for an Open World, Edited by Ann Florini, New York: Columbia University Press, 2007, pp. 2-3.

[144] Ann Florini, "The Battle over Transparency," Introduction to *The Right to Know: Transparency for an Open World*, Edited by Ann Florini, New York: Columbia University Press, 2007, p. 3.

[145] Ann Florini, "The Battle over Transparency," Introduction to The Right to Know: Transparency for an Open World, Edited by Ann Florini, New York: Columbia University Press, 2007, p. 3.

[146] Christopher Joye, Interview with Michael Hayden Regarding Edward Snowden, Cyber Security, and Transparency," *Australian Financial Review*, at http://genius.com/Michael-hayden-interview-regarding-edward-snowden-cyber-security-and-transparency-annotated.

[147] For more on millennials, see for example, Sam Tanenhaus, "Generation Nice," August 15, 2014, at http://www.nytimes.com/2014/08/17/fashion/the-millennials-are-generation-nice.html?_r=0.

> from the very small fraction of that population that has this romantic attachment to absolute transparency at all costs.[148]

Responding to the demands for greater transparency from the millennial generation and others, President Obama announced in 2009 that his Administration was committed to an unprecedented level of openness in Government.[149] President Obama stated:

> Government should be transparent. Transparency promotes accountability and provides information for citizens about what their Government is doing. Information maintained by the Federal Government is a national asset. My Administration will take appropriate action, consistent with law and policy, to disclose information rapidly in forms that the public can readily find and use. Executive departments and agencies should harness new technologies to put information about their operations and decisions online and readily available to the public. Executive departments and agencies should also solicit public feedback to identify information of greatest use to the public.[150]

Gregory Treverton, currently chairman of the National Intelligence Council, has spoken and written on the issue of transparency in the intelligence and policy arena. His remarks highlight the important role of congressional oversight as a way to represent the public's need to know and find the right balance between secrecy and open government:

> Precisely because intelligence tools of the fight against terror cannot be entirely transparent, lest the nation's enemies adapt their operations to circumvent them, the social contract requires some processes of secret oversight. The public doesn't need to know the details of what is being done in its name. It does need to know that somebody independent of an administration does know and does approve. What is critical is process before the fact and oversight afterward, if not before. If, in the famous phrase, the Constitution is not a suicide pact, neither is war a blank check.[151]

In 2015, the DNI published "IC Principles of Transparency" "intended to facilitate IC decisions on making information publicly available in a manner that enhances public understanding of intelligence activities, while continuing to protect information when disclosure would harm national security."[152] (See **Appendix** for a complete list of IC Principles of Transparency.)

A number of journals discuss the issue of transparency in terms of greater accountability to the American public through Congress's investigative arm and its power of the purse.

Transparency and GAO Access

Legislative entities such as the Government Accountability Office (GAO) have broad statutory authority to evaluate and investigate any government activity to include the IC.[153] However, as

[148] Christopher Joye, Interview with Michael Hayden Regarding Edward Snowden, Cyber Security, and Transparency," *Australian Financial Review*.

[149] The White House, "Transparency and Open Government," Memorandum for the Heads of Executive Departments and Agencies, at https://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment/.

[150] The White House, "Transparency and Open Government," Memorandum for the Heads of Executive Departments and Agencies.

[151] Gregory Treverton, "Intelligence Test," *Democracy*, Issue 11, Winter 2009, at http://www.democracyjournal.org/11/6667.php?page=all. See also Gregory Treverton, "Intelligence and Policy in an Era of Transparency," IISS-US Policy Makers Series, Thursday 19 March 2015, video available at https://www.iiss.org/en/events/events/archive/2015-f463/march-3048/intelligence-and-policy-in-an-era-of-tranparency-b0a5.

[152] ODNI, "Principles of Intelligence Transparency for the Intelligence Community," not dated, last accessed on March 1, 2016, at http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.

[153] Statement of David M. Walker, Comptroller of the United States, "Intelligence Reform: GAO Can Assist the (continued...)

mentioned in the section on "Inspectors General (IGs)," congressional oversight committees have traditionally left the bulk of IC-related oversight to independent IC entities such as the agency IGs. The IC has had a long tradition of resisting GAO access beginning with the first Director of the Central Intelligence Agency (DCIA). According to Britt Snider, a former CIA IG, and author of *The CIA and the Hill*, the first DCIA argued that the CIA was exempt from GAO audit because according to the law, the DCIA was the final authority required for the expenditure of agency funds.[154] According to Snider, despite repeated efforts by the GAO and House Armed Services' Committee to negotiate limited access, all of the GAO's audit activities at the CIA were abandoned in 1962, and remained that way for many years.[155]

IC attitudes toward GAO evaluations and investigations appear to be changing. Over the past several decades, the GAO has gradually evaluated a number of intelligence-related programs, particularly in the DOD. The most sensitive activities continue to remain off-limits.[156] In response to a directive in the IAA for FY2010,[157] the IC produced a policy directive directing IC agencies to cooperate with GAO audits or reviews but allowing IC elements to evaluate GAO requests for information on a case-by-case basis:

> Information that falls within the purview of the congressional intelligence oversight committees generally shall not be made available to GAO to support a GAO audit or review of core national intelligence capabilities and activities, which include intelligence collection operations, intelligence analyses and analytical techniques, counterintelligence operations, and intelligence funding. IC elements may on a case-by-case basis provide information in response to any GAO requests not related to GAO audits or reviews of core national intelligence capabilities and activities.[158]

The policy directive prohibits GAO access to any information related to intelligence sources and methods.[159] DNI Clapper has reportedly said that he believes it is the job of congressional oversight staff associated with the congressional intelligence committees to do the most sensitive investigations:

> '[T]he evaluation, review, and audit of intelligence activities, capabilities, programs and operations,' as well as activities involving 'intelligence sources . . . intelligence methods, and the analysis of intelligence funding' should be done by staffs of the congressional intelligence committees. If the intelligence committees wanted GAO assistance, he

(...continued)

Congress and the Intelligence Community on Management Reform Initiatives," February 29, 2008, at http://www.gao.gov/new.items/d08413t.pdf. Walker argues that GAO has the necessary authority, expertise, and security protocols to perform audits and evaluations of IC activities.

[154] Britt Snider, *The Agency and the Hill: CIA's Relationship with Congress, 1946-2004*, (Washington, DC: Center for the Study of Intelligence, 2008), p. 20, at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/agency-and-the-hill/index.html. According to the CIA Act of 1949, P.L. 110, Section 8(b): "The sums made available to the Agency may be expended without regard to the provisions of law and regulations relating to the expenditure of Government funds; and for objects of a confidential, extraordinary, or emergency nature, such expenditures to be accounted for solely on the certificate of the Director and every such certificate shall be deemed a sufficient voucher for the amount therein certified."

[155] Britt Snider, *The Agency and the Hill: CIA's Relationship with Congress, 1946-2004*, (Washington, DC: Center for the Study of Intelligence, 2008), p. 20.

[156] Statement of David M. Walker, Comptroller of the United States, "Intelligence Reform: GAO Can Assist the Congress and the Intelligence Community on Management Reform Initiatives," February 29, 2008.

[157] P.L. 111-259 §348 "Information Access by the Comptroller General of the United States."

[158] Intelligence Community Directive (ICD) 114 (D) (4) (b), "Comptroller General Access to Intelligence Community Information," June 30, 2011, at http://www.dni.gov/files/documents/ICD/ICD_114.pdf.

[159] ICD-114 (D) (4) (c).

> believed 'those people should be loaned to the committees so they would be working under the auspices of the intelligence panel and not under the director of the comptroller general.'[160]

Transparency and Budget Numbers

Most intelligence dollars are embedded in the defense budget for security purposes. All but the topline budget numbers are classified. Disclosure of details associated with the intelligence budget has been debated for many years—proponents arguing for more accountability;[161] IC leadership arguing that disclosure could cause damage to national security.[162]

The Church and Pike Committees, and Senate and House intelligence committees, all held hearings on greater transparency in regards to the IC budget. Congressional documents from the 1970s provide a rich repository of the arguments voiced in favor of, or in opposition to, disclosing the intelligence budget. At that time, the debates typically focused on (1) whether to disclose one NIP top-line number, or (2) whether to disclose all IC agency top-line numbers.[163]

The disclosure debate was rekindled a number of times the years following the creation of the intelligence committees. The *9/11 Commission* agreed with the critics who argued for more transparency but also agreed that disclosure of numbers below the topline could cause damage to national security. It recommended that the amount of money spent on national intelligence be released to the public.[164]

In response to the *9/11 Commission* recommendations, P.L. 110-53 Section 601(a) directs the DNI to disclose the NIP topline number.[165] The first such disclosure was made on October 30, 2007.[166] The IAA for FY2010 (P.L. 111-259) further amended Section 601 to require the President to publicly disclose the amount requested for the NIP for the *next* fiscal year "at the time the President submits to Congress the budget."[167]

At the present time only the NIP topline figure must be disclosed based on a directive in statute. The DNI is not required to disclose any other information concerning the NIP budget, whether the information concerns particular intelligence agencies or particular intelligence programs. In 2010,

---

[160] Walter Pincus, "Clarifying GAO's role in intelligence oversight," *Washington Post*, October 25, 2010, at http://www.washingtonpost.com/wp-dyn/content/article/2010/10/25/AR2010102505278.html.

[161] 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/. See also the discussion of the *Intelligence Budget Transparency Act of 2015* in the final section of this report, "Issues for Congress."

[162] "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.

[163] See for example, U.S. Congress, Senate Select Committee on Intelligence, *Whether Disclosure of Funds for the Intelligence Activities of the United States is in the Public Interest*, 95th Cong., 1st sess., S.Rept. 95-274, June 16, 1977 (Washington, DC: GPO, 1977).

[164] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report, the Attack from Planning to Aftermath* (New York: W.W. Norton, 2011), p. 416.

[165] P.L. 110-53, titled *The Implementing the Recommendations of the 9/11 Commission Act of 2007* and was enacted August 3, 2007.

[166] ODNI, "DNI Releases Budget Figure for National Intelligence Program," *press release*, October 30, 2007, at http://www.dni.gov/files/documents/Newsroom/Press%20Releases/2007%20Press%20Releases/20071030_release.pdf.

[167] P.L. 111-259 §364. See for example, ODNI Releases Requested Budget Figure for FY2016 Appropriations for the National Intelligence Program," ODNI *news release* no. 24-15, February 2, 2015, at http://www.dni.gov/index.php/newsroom/press-releases/210-press-releases-2015/1168-dni-releases-requested-budget-figure-for-fy-2016-appropriations.

the Secretary of Defense began disclosing MIP appropriations figures on an annual basis and in 2011 disclosed those figures back to 2007.[168] These actions have provided public access to previously classified budget numbers for national and military intelligence activities.[169]

In the 114th Congress, legislation has again been introduced to address the issue of transparency and secrecy in the intelligence budgets.[170] H.R. 2272, and an identical bill, S. 1307, both titled the "Intelligence Budget Transparency Act of 2015," were introduced in the House and Senate respectively on May 12, 2015.[171] Both bills require disclosure of:

> [T]he total dollar amount proposed in the budget for intelligence or intelligence related activities of each element of the Government engaged in such activities in the fiscal year for which the budget is submitted and the estimated appropriation required for each of the ensuing four fiscal years.[172]

Issues to Consider:

1. How might the relationship between the IC and GAO be improved in order to promote more transparency into IC activities for congressional overseers?
    - What specific authorities might Congress need to grant GAO to enable greater access?
2. The DNI is currently the final authority if the GAO is denied access to an IC activity. Is it time to reexamine the GAO-IC appeals process?
3. Do the arguments, directives, and statute that currently guides disclosure of numbers associated with intelligence spending need to be reexamined?
4. Are there portions of the IC budget that could be made more transparent to the American public without endangering national security?
5. Are the new principles of transparency sufficient? Can the DNI do more to promote transparency across the IC?

Questions in Common

The issues examined in this report represent only a few of the many cross-cutting issues associated with IC leadership and management. While all eight are different in many ways, they are similar in that they shine a light on important questions in common that can applied to oversight of other IC-wide cross-cutting issues. For example, there are IC-wide hurdles faced by large and small businesses in pursuing IC contracts; negative consequences associated with the ever growing number of intelligence integration centers; IC—law enforcement sharing of intelligence data and its negative impact on public trust of the IC; good organizational change

[168] Department of Defense, "DOD Releases Military Intelligence Program Top Line Budget for Fiscal 2007, 2008, 2009," DOD *news release* no. 199-11, March 11, 2011, available at http://archive.defense.gov/Releases/Release.aspx?ReleaseID=14328. The release of the MIP topline was not directed by statute. According to this news release, it was a decision made by the Secretary of Defense.

[169] For more on transparency and intelligence spending, see CRS Report R44381, *Intelligence Spending: In Brief*, by (name redacted) .

[170] Such legislation is not new. For example, H.R. 3855, "The Intelligence Budget Transparency Act of 2014," was introduced in the 113th Congress.

[171] The bills were referred to the House and Senate Committees on the Budget respectively.

[172] H.R. 2272 §2.

versus "change for the sake of change"—related to issues of structural reform and "reform fatigue"; and lack of integration in the IC's research and development efforts.

In examining any cross-cutting issue, does anything about the issue suggest focusing on:

- **Balance?** Does the issue require attention to how resources (money and manpower) or priorities are balanced (e.g., security versus bringing best new hires on-board quickly)?
- **Best Practices?** Are they being sought and shared?
- **Integration?** What agency specific processes could be better integrated to address a particular cross-cutting issue (e.g., the hiring process, budget)?
- **Privacy and Civil Liberties?** Are existing protections sufficient?
- **Transparency?** Does any given issue need more public scrutiny?
- **Trust?** What are the consequences of any policy option on trust (e.g., trust between individuals, agencies, branches of government, public and government)?

Appendix. Intelligence Community Principles of Transparency

"The Intelligence Community Will:

1. Provide appropriate transparency to enhance public understanding about:
    a. the IC's mission and what the IC does to accomplish it (including its structure and effectiveness);
    b. the laws, directives, authorities, and policies that govern the IC's activities; and
    c. the compliance and oversight framework that ensures intelligence activities are conducted in accordance with applicable rules.
2. Be proactive and clear in making information publicly available through authorized channels, including taking affirmative steps to:
    a. provide timely transparency on matters of public interest;
    b. prepare information with sufficient clarity and context, so that it is readily understandable;
    c. make information accessible to the public through a range of communications channels, such as those enabled by new technology;
    d. engage with stakeholders to better explain information and to understand diverse perspectives; and
    e. in appropriate circumstances, describe why information cannot be made public.
3. In protecting information about intelligence sources, methods, and activities from unauthorized disclosure, ensure that IC professionals consistently and diligently execute their responsibilities to:
    a. classify only that information which, if disclosed without authorization, could be expected to cause identifiable or describable damage to the national security;
    b. never classify information to conceal violations of law, inefficiency, or administrative error, or to prevent embarrassment;
    c. distinguish, through portion marking and similar means, classified and unclassified information; and
    d. consider the public interest to the maximum extent feasible when making classification determinations, while continuing to protect information as necessary to maintain intelligence effectiveness, protect the safety of those who work for or with the IC, or otherwise protect national security.
4. Align IC roles, resources, processes, and policies to support robust implementation of these principles, consistent with applicable laws, executive orders, and directives."[173]

[173] Office of the DNI, "Principles of Intelligence Transparency for the Intelligence Community," not dated, last accessed on March 1, 2016, at http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.

Author Contact Information

(name redacted)
Analyst in Intelligence and National Security Policy
[redacted]@crs.loc.gov, ...