~~SECRET//NOFORN~~

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

(U) Semiannual Report
1 January 2011 – 30 June 2011

LEADING INTELLIGENCE INTEGRATION

6 Aug 2011

[redacted] (b)(1)
(b)(3)

Office of the Inspector General

~~SECRET//NOFORN~~

(U) The Inspector General of the Office of the Director of National Intelligence (ODNI) provides policy direction for, and plans, conducts, supervises, and coordinates inspections, audits, investigations, and other inquiries relating to the programs and operations of the ODNI and the authorities and responsibilities of the Director of National Intelligence (DNI). The Inspector General is charged with detecting fraud, waste, and abuse; evaluating performance; and making recommendations to promote economy, efficiency, and effectiveness in the ODNI and the Intelligence Community.

(U) A Message From the Inspector General

(U) The Office of the Director of National Intelligence (ODNI) Office of the Inspector General (OIG) made significant contributions to the missions of the ODNI and the Intelligence Community during the 1 January 2011 through 30 June 2011 reporting period. During this reporting period the OIG conducted audits, inspections, investigations, and reviews designed to improve the efficiency and effectiveness of ODNI and Intelligence Community programs. These matters are described in detail in the Completed Projects section of this report.

(U) As the ODNI Inspector General, I chair the Intelligence Community Inspectors General Forum. The Forum's audit, inspections, and investigation working groups collaborated on a variety of ongoing and planned projects and shared best practices. On 23 June 2011, the OIG hosted the Third Annual Intelligence Community Inspectors General Professional Awards Ceremony. The ceremony recognized personnel from OIGs throughout the Intelligence Community (IC) who made extraordinary contributions in 2010 to the OIG mission and objectives. Forum Members voted to present the Leadership Award posthumously to Thomas J. Burton for his outstanding service and leadership as the Inspector General of the National Geospatial-Intelligence Agency and his exemplary service to the IC.

(U) We continued to support the DNI and senior ODNI officials in working diligently to implement pending OIG recommendations. During this reporting period ODNI management has taken significant steps to communicate the new executive leadership's mission, vision, goals, and objectives to the ODNI workforce, the broader IC. Members of Congress, the press, and the general public. First and foremost, upon his arrival, Director Clapper clearly articulated that the core mission of the ODNI is to lead intelligence integration and that protecting the Homeland is job #1 for the Intelligence Community. To drive this message and better align the organization to the mission, Director Clapper has "re-set" ODNI's activities and personnel and, together with the ODNI and IC elements' Public Affairs Offices, used ODNI and IC publications, web sites, Town Halls, and speaking engagements by ODNI senior leadership in both classified and unclassified venues to reinforce the integration message. These strategic communication efforts clarify the ODNI's role and mission and communicate its unique value to the intelligence enterprise, which implements a long-standing OIG recommendation. In addition, ODNI management formalized a repeatable process to track implementation of OIG recommendations.

(U) Finally, the OIG began developing a strategic plan to support the eventual stand-up of the Office of the Inspector General of the Intelligence Community, an office established by the FY 2010 Intelligence Authorization Act. These efforts involved benchmarking, identifying possible requirements or gaps in current policy and processes, initiating development of a cost model to support a separate OIG budget, assessment of staffing requirements for variable workloads, and scoping of objectives to support a phased transition.

(U) We appreciate the continued support for our mission from ODNI senior leadership, ODNI management, and Congress. As the OIG prepares to transition to the Office of the Inspector General of the Intelligence Community, I also want to express my appreciation for the talent and dedication of OIG personnel in the ODNI and across the Intelligence Community. We are committed to performing our work in accordance with the highest standards of professionalism, objectivity, independence, and integrity.

Roslyn A. Mazer
Inspector General
29 July 2011

(U) Table of Contents

This Page Left Intentionally Blank

I. (U) Overview

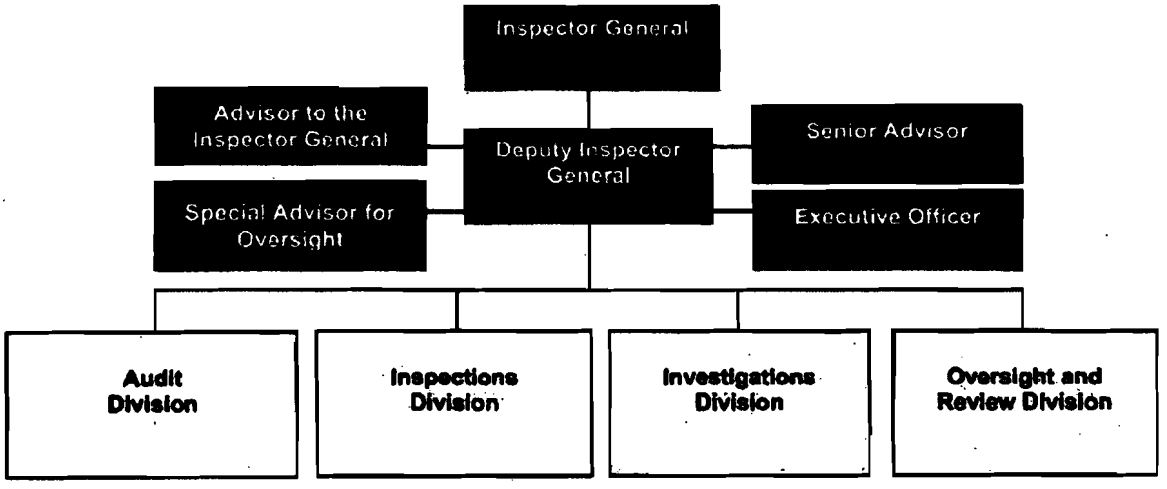
(U) The mission of the Office of the Inspector General (OIG) is to improve Intelligence Community (IC) performance by: 1) overseeing the Office of the Director of National Intelligence (ODNI) and IC programs and operations that fall within the authorities and responsibilities of the Director of National Intelligence (DNI); 2) exercising a unique cross-agency focus; and 3) collaborating with IC Inspector General (IG) partners. The OIG conducts audits, investigations, inspections, and reviews of ODNI and IC performance to detect and deter waste, fraud, and abuse and to promote efficiency, effectiveness, and accountability. Sections IV and V of this report describe the OIG's completed and ongoing projects respectively. In addition, the ODNI OIG facilitates the activities of the IC Inspectors General Forum, which are described in section II of this report.

(U) The OIG recommends performance improvements for ODNI and IC programs and activities to the DNI. Section VII of this report updates the status of ODNI management's implementation of report recommendations since 2008.

(U) OIG Organization

(U) As illustrated in the organization chart below, OIG is comprised of four divisions and a front office staff (See Figure 1).

(U) Figure 1. OIG Organization Chart January 2011



(U) During this reporting period the OIG combined the Oversight and Policy Division and the Management Reviews Division to create the Oversight and Review Division, which better aligned OIG functions and resources (See Figure 2).

(U) Figure 2. OIG Divisions 1 January 2011 – 30 June 2011

Office of the Inspector General Divisions
Audit Division Audits program, compliance, and financial audits and evaluations of ODNI and IC programs, information technology, procurement, acquisitions, internal controls, financial statements, and financial management.
Inspections Division Conducts inspections, reviews, and evaluations to improve ODNI and IC-wide performance; examines information access, collaboration, intelligence collection, analysis, and compliance with laws and regulations.
Investigations Division Investigates allegations of violations of criminal laws and administrative regulations arising from the conduct of ODNI and IC employees and contractors.
Oversight and Review Division Conducts comprehensive evaluations and reviews of systemic issues within the ODNI, national mission centers, and the IC to evaluate efficiency and effectiveness, identify vulnerabilities, and prevent and detect fraud, waste, and abuse. Has a multi-disciplinary staff that complements the traditional audit, inspection, and investigations disciplines to assess ODNI and IC activities and programs.

(U) OIG Personnel

(U//~~FOUO~~) The OIG has a diverse, highly-experienced workforce with a variety of professional and IC experience, including auditors, investigators, attorneys, and inspectors. Complementing these professionals are collectors, analysts, and project managers from military and civilian intelligence organizations.

~~(S//NF)~~

(b)(1)
(b)(3)

II. (U) IC Inspectors General Activities

(U) To achieve its oversight objectives, the ODNI OIG facilitates collaboration, information sharing, and strategic planning among the IC Inspectors General. This section provides highlights of IC Inspector General Activities conducted during this reporting period.

(U) 17th Annual IC Inspectors General Conference

(U) The ODNI OIG hosted the 17th Annual IC Inspectors General (IC IG) Conference on 10 May 2011 at the Defense Intelligence Agency Center on Bolling Air Force Base. Approximately [redacted] personnel from across the IC IG Community attended the conference. (b)(3)

(U) The conference objectives were to enhance collaboration across the IC IG community, improve IC IGs' performance, and facilitate the accomplishment of the IC IGs' mission, duties, and responsibilities. The attendees heard perspectives from distinguished IC leaders, OIG experts, and congressional intelligence oversight committee staff.

(U//FOUO) Highlights of the conference include a keynote address by The Honorable James R. Clapper, Jr., Director of National Intelligence (DNI), who expressed his appreciation for the work of IGs and emphasized their value as "an objective and independent set of eyes and ears." He also endorsed the statutory IC IG, established by the Intelligence Authorization Act (IAA) for FY 2010 in October 2010. [redacted] chaired a plenary session with [redacted], on methodologies and best practices for conducting IG reviews focused on cost-saving initiatives and bolstering efficiencies. [redacted] chaired a plenary session on Intelligence Oversight with congressional staffers [redacted] Majority Staff Director for the Senate Select Committee on Intelligence (SSCI), and [redacted] SSCI Minority Staff Director. The panel discussed topics such as congressional notification of intelligence operations, expectations for the newly-created IC IG position, and how OIGs can better assist the intelligence committees with IC oversight. (b)(3)

(U) Conference participants also engaged in small group discussions on:

- Emerging Standards Related to Financial Statements, led by [redacted] (b)(3)
- Prosecuting IC IG Cases, led by Charles McCullough, ODNI Deputy Inspector General;
- Best Practices for Intelligence Oversight, led by [redacted]
- [redacted]

- Predictive Analysis, led by
- Best Practices for Data Collection, led by (b)(3)

(U) Third Annual IC Inspectors General Awards Ceremony

(U) On 23 June 2011, the IC IG community participated in the Third Annual IC Inspectors General Awards Ceremony. The ceremony recognized personnel from OIGs throughout the IC who made extraordinary contributions in Calendar Year 2010 to the mission and objectives of the OIGs and the *National Intelligence Strategy*. Honorees were presented awards in the following categories:

- Leadership Award
- Lifetime Achievement Award
- Audit Award
- Inspections Award
- Investigations Award

(U) was the keynote speaker for the awards ceremony. noted that IC IGs often are the only individuals – outside of the cleared Members of Congress – who are informed, independent, and have access to the classified information necessary to conduct thorough evaluations of IC activities. also recognized the value of the work performed by awards recipients, as well as the critical role IC OIGs play in addressing waste, fraud, and abuse. (b)(3)

(U) The Leadership Award was presented posthumously t for his outstanding service and leadership as the The Lifetime Achi rd was presented to who was recognized for more than 33 years of service to the IG community. (b)(3)

(U) The IC IGs also presented Audit Awards to the National Security Agency (NSA) OIG auditors who determined the significance of intelligence lost because of certain legal mandates. The Inspections Award was presented to Central Intelligence Agency (CIA) OIG inspectors who evaluated the CIA's performance against the foreign cyber threat. The Investigations Award was presented to NSA investigators in recognition of their work on a case involving contracting improprieties.

(U) IC Inspectors General Forum Meetings

(U) The ODNI IG chairs the IC IG Forum, which meets quarterly to develop cross-agency projects and promote the role of IC IGs. During this reporting period, the IC IG Forum exchanged ideas and work plans, shared best practices, and identified projects affecting

two or more IC OIGs. In addition to these business agenda items, the Forum considered several critical issues facing the IC today. Specifically, Forum members discussed the state of IC intelligence integration and how the IC IGs are positioned to provide management with guidance in this area. The Forum members welcomed the Principal Deputy Director of National Intelligence (PDDNI), The Honorable Stephanie O'Sullivan, to share her views and vision for the IC. PDDNI O'Sullivan expressed her appreciation for the work of the IC IGs and committed to supporting IG independence.

(U//FOUO) Forum members also discussed the audit and oversight roles IC IGs could take with respect to unauthorized disclosures of national security information such as WikiLeaks. [redacted] Staff provided insights on the NSC's approach to the WikiLeaks incident to the Forum members. (b)(3)

(U//FOUO) Financial management was also a key topic of discussion for IC IGs this reporting period. The FY 2010 IAA establishes the Inspectors General of DIA, NGA, National Reconnaissance Office (NRO), and NSA as "Designated Federal Entities (DFE)." Forum members invited the Associate Director of National Intelligence (ADNI) and Chief Financial Officer (CFO), [redacted] to discuss the role of DFE IGs in preparing to become auditable, including auditing financial statements, preparing for the audit process, and working to ensure that congressional expectations are met.

(U) Forum members received a briefing on the creation of an IC IG Community of Interest (COI), which is hosted on an internal classified website. The COI was officially launched during this reporting period. The COI's objectives are to leverage efforts of the IC IG Community to create a platform for sharing information across the community. The IC IGs fully endorsed the creation of the IC IG COI.

(U) IC Deputy Inspectors General Activities

(U) The Deputy Inspectors General Working Group met to exchange ideas on a wide variety of topics. They developed topics and panels for the 17th Annual IC IG Conference held in May 2011, selected recipients of IC IG Awards, and discussed strategies for addressing Congressionally Directed Actions requiring IG reviews of IC matters.

(U) IC Assistant Inspectors General for Audit Activities

(U//FOUO) The Joint Audit Working Group (JAWG) met in March 2011 and discussed IC OIG work plans, provisions of the 2010 IAA regarding the designation of a statutory IC IG and the DFEs, the impact of DFEs on performing financial statement audits, and FY 2011 Federal Information Security Management Act preparation.

(U//FOUO) The Cyber JAWG met in March 2011 to discuss the Wikileaks incident. Topics included: 1) the security problems that enabled the WikiLeaks incident and the major

efforts underway to address those problems; and 2) ODNI's efforts to comply with recent Office of Management and Budget memoranda in regard to safeguarding classified information.

(U) IC Assistant Inspectors General for Inspections Activities

(U//FOUO) The IC AIGs for Inspections Working Group met to discuss best practices for conducting short-cycle inspections. The AIGs for Inspections from CIA and NRO provided presentations. Working group members discussed the use of various methodologies including use of surveys and on-line assessment tools.

(U//FOUO) The ODNI OIG hosted a Forum on promoting efficiencies in June 2011. [redacted] Assistant Director of National Intelligence (ADNI) for Systems and Resource Analysis, and [redacted] briefed Forum participants from Departments of Defense, Justice, and State, as well as CIA, NGA, NRO, and ODNI. [redacted] provided perspectives on Intelligence Planning; the Programming, Planning, Budget and Evaluation (PPBE) process; IC performance and evaluations; and the DNI efficiency studies. (b)(3)

(U) IC Assistant Inspectors General for Investigations Activities

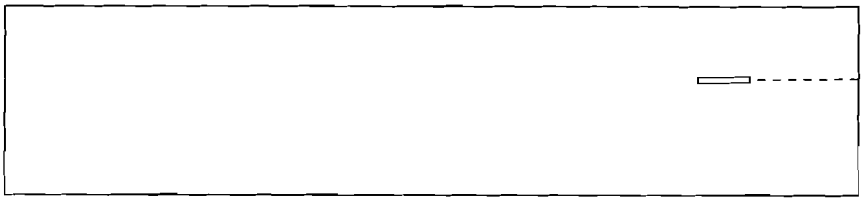
(U) The AIG for Investigations (AIGI) Working Group collaborated to exchange best practices for detecting fraud, waste, and abuse. Working group members also shared the names of working targets to ensure that all IC agencies are aware of any fraudulent schemes or efforts that could affect other IC agencies. The Working Group encouraged the AIGIs to participate in the IC IG Joint Duty Rotational Assignment Program; scheduled future IC Investigation Peer Reviews; and discussed blanket declination policies and prosecutive thresholds for cases within the jurisdiction of the United States Attorney's Office, Eastern District of Virginia. The IC IG Joint Data Mining Working Group, the Department of Defense Contractor Disclosure Program, and the Executive Director for the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Training Institute each briefed the AIGI Working Group during this reporting period.

III. (U) Top Management and Performance Challenges

(U) In accordance with the Reports Consolidation Act of 2000, in November 2010, the OIG created a list of the top management challenges within the ODNI. To identify these challenges, the OIG drew upon [redacted] and reviews performed in the previous two years, challenges discussed in the IC Inspectors General Forum, and issues identified by ODNI senior officials. (b)(3)

(C//NF) The challenges were not presented in priority order because all are critical for the ODNI. This also is not a cumulative list of all ODNI management challenges; rather it is a

snapshot seen through the lens of recent OIG reports, OIG findings, and ODNI activities and focus areas. The management challenges we identified are:



(b)(3)

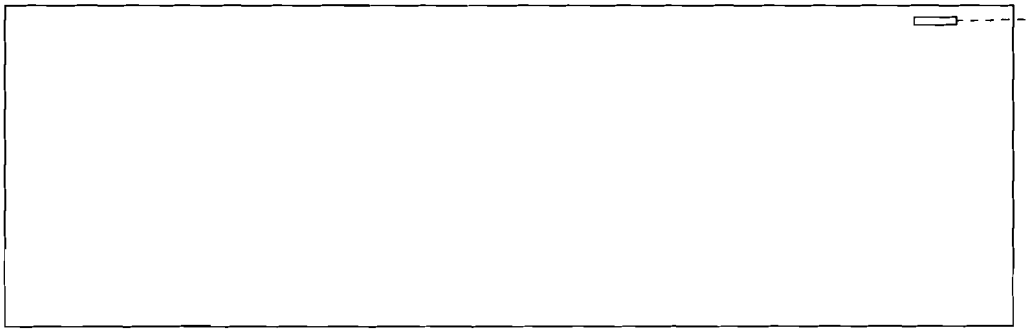
IV. (U) Completed Projects

(U) Audit Division

(U) Audit of the Monitoring and Coordination of the Comprehensive National Cybersecurity Initiative (CNCI) by the Director of National Intelligence (DNI)

(U//FOUO) National Security Presidential Directive 54/Homeland Security Presidential Directive 23, commonly known as Comprehensive National Cybersecurity Initiative (CNCI), assigns to the DNI primary responsibility to "monitor and coordinate CNCI implementation." To discharge this responsibility, the ODNI stood up the Joint Interagency Cyber Task Force and established the Cyberspace Management Office under the Associate Director of National Intelligence/Chief Information Officer. This self-initiated audit provided an independent assessment of the DNI's monitoring and coordination of CNCI implementation. The audit evaluated whether the policies and procedures, roles and responsibilities, and governance structures existed to monitor and coordinate CNCI implementation. The audit also examined the adequacy of ODNI and other federal agency coordination and identified gaps that the ODNI should address. To accomplish this audit, we coordinated with agencies in the IC, agencies responsible for CNCI initiatives and enablers, and senior administration cyber officials.

(U//FOUO) The report provides information and observations that could assist in the development of regulations and protocols for the next phase of CNCI monitoring and coordination. Specifically, OIG identified opportunities for improvements in two areas:

- 

(b)(3)

(U) Inspections Division

(U) Evaluation of the Administration and Management of ODNI Core Contracts Supporting Critical Missions

(U//FOUO) The OIG evaluated the risks associated with the administration and management of core contracts supporting ODNI critical missions. We conducted interviews, reviewed documentation, issued questionnaires, and performed a detailed examination of a judgmental sample of ODNI core contracts. Our review resulted in three findings:

(b)(3)

To address each of these findings, we made specific recommendations designed to ensure that internal controls are in place to improve the ODNI's oversight of core contracts. We also made recommendations designed to improve the ODNI's management of COTRs.

(U) Oversight & Review Division

(U) Status of Integration of the Departmental and Service Intelligence Community Elements

(U//FOUO) In OIG reviews conducted after the standup of the ODNI, senior representatives from the Departmental and Service IC elements stated that their elements' missions, roles, expertise, and capabilities were not fully known, understood, or leveraged by the ODNI and other IC elements. Departmental and Service elements are intelligence components embedded within Federal departments or agencies and focus primarily on serving their respective parent organizations' intelligence needs. During this review, the OIG identified the unique roles, capabilities, expertise, and contributions of the Departmental and Service elements, identified barriers to their integration, and determined how these elements can be more effectively leveraged and integrated in the IC.

(b)(3)

(U//FOUO) The OIG found that the Departmental and Service elements play a significant and expanding role in the IC and make valuable contributions to the IC mission. Additionally, we found the ODNI has made meaningful progress integrating these elements. ODNI officials and other participants identified ODNI initiatives such as strategy alignment and enterprise management activities; participation in governance bodies, other collaborative venues, and mission management initiatives; and access to information sharing tools, as advancing integration and collaboration.

(U//FOUO) However, we found Departmental and Service element integration varies widely due to inconsistent awareness of Departmental and Service elements' capabilities and expertise. While awareness is largely based on mission need, the ways in which the Departmental and Service elements can best support the mission are not always well understood and pose risks of missed collection opportunities and sub-optimal analysis and resource utilization. We found that inconsistent awareness stems from four factors:

-
-
-
-

(b)(3)

(U//FOUO) To address these findings, the report contains two recommendations:

-
-

(b)(3)

(U//FOUO) Implementing these recommendations, in conjunction with Departmental and Service elements' efforts to enhance IC awareness of their unique expertise and capabilities, should improve the level and breadth of Departmental and Service element integration.

(U) Investigations Division

(U//FOUO) During this reporting period, the OIG conducted investigations on a variety of allegations including time and attendance (T&A) fraud, contracting irregularities, ethics violations, misuse of government property, voucher fraud, and abuse of position.

(b)(3)

(U//FOUO) Ethics Violation by Senior Official

(U//FOUO) The OIG investigated an allegation that a senior ODNI official violated administrative and criminal ethics rules by personally and substantially participating in the ODNI acquisition process of a potential acquisition of software services of a former employer. The OIG investigation substantiated the allegation; however, the Department of Justice (DOJ) declined prosecution and referred the matter to ODNI executive management to address administratively.

(U//FOUO) Ethics Violation by Senior Official

(U//FOUO) The OIG investigated an allegation that a senior ODNI official failed to list personally owned stock on two public financial disclosure reports and provided a briefing to a company in which he owned stock. The senior official self-reported the failure to report his stock ownership. The OIG investigation substantiated the allegation; however, the DOJ declined prosecution and referred the matter to ODNI executive management to address administratively.

(U//FOUO) Misuse of Position by ODNI Manager

(U//FOUO) The OIG investigated allegations that senior officials in an ODNI component retaliated against an ODNI employee because the employee filed a formal complaint about the component's management practices. The employee claimed he was given a low performance rating, threatened with a suitability investigation, and given a letter of warning without justification after making his written complaint. During the investigation, ODNI executive management made significant management changes within the component and, with the employee's concurrence, reassigned the employee.

(U//FOUO) Alleged Violation of the Procurement Integrity Act

(U//FOUO) The OIG investigated allegations that an ODNI employee provided sensitive ODNI procurement information to a contractor whose company was bidding on an ODNI contract. The OIG investigation did not substantiate the allegation.

(U//FOUO) Alleged T&A Fraud by an ODNI Employee

(U//FOUO) The OIG investigated allegations that an ODNI employee submitted false T&A records for several months. The employee's managers alleged that the employee repeatedly failed to show up for work and then submitted T&A records indicating s/he was at work. The investigation substantiated the allegation, and a report has been submitted to ODNI executive management to address administratively.

(U//FOUO) Alleged Unauthorized Possession of Government Credentials

(U//FOUO) The OIG investigated allegations that ODNI employees improperly received official government credentials from an ODNI component and other government entities that purportedly authorized the ODNI employees to carry firearms as part of their ODNI employment. The ODNI recovered all of the outstanding ODNI credentials and the credentials issued to ODNI personnel from other government entities.

(U//FOUO) Use of Subpoena Authority

(U//FOUO) The OIG did not exercise subpoena authority under § 7(a)(4) of ODNI Instruction 2005-10 during this reporting period.

V. (U) Ongoing Projects and Activities

(U) Audit Division

(U) Audit of the Use of Reciprocity by the ODNI for Personnel Security Clearance and Hiring Purposes

(U) The OIG initiated this audit to examine security clearance reciprocity with respect to eligibility. The OIG believes the findings of this audit will facilitate and increase the efficiency and effectiveness of security clearance and access determination reciprocity among IC agencies.

(U) This audit also will respond in part to the FY 2010 Intelligence Authorization Act (IAA) requirement for the Inspector General of the Intelligence Community to audit security clearance reciprocity throughout the IC. Due to resource constraints, the ODNI OIG will focus solely on reciprocity for ODNI personnel as related to the three security clearance reciprocity scenarios specified in the IAA requirement: 1) an employee of an element of the IC detailed to another element of the IC; 2) an employee of an element of the IC seeking permanent employment with another element of the IC; and 3) a contractor seeking permanent employment with an element of the IC.

(U//FOUO) Joint Audit of the Status of the Sharing of Cyber-Threat Information

(U//FOUO) This audit addresses a statutory requirement in the FY 2010 IAA requiring the IG of the Department of Homeland Security (DHS) and the Inspector General of the Intelligence Community to jointly submit to Congress and the President a report on the status of sharing cyber-threat information. The IAA specifies the following four objectives:

1. a description of how cyber-threat intelligence information, including classified information, is shared among the agencies and departments of the United States and with persons responsible for critical infrastructure;

2. a description of the mechanisms by which classified cyber-threat information is distributed;
3. an assessment of the effectiveness of cyber-threat information sharing and distribution; and
4. any other matters identified by either IG that would help to fully inform Congress or the President regarding the effectiveness and legality of cybersecurity programs.

(U//FOUO) We initiated this audit in coordination with the DHS OIG. Our review addresses the four objectives for both the unclassified and classified information environments. Our focus is primarily on the sharing of classified cyber-threat information. We are coordinating with the DHS OIG on other aspects of the audit where appropriate.

(U) FY 2011 Federal Information Security Management Act (FISMA) Review

(U) FISMA requires that an annual independent evaluation be performed by an agency OIG or a third party to assess the security measures for information systems that support operations. The objective of the review is to determine the adequacy of the information security program for the ODNI's internal operations and the information security strategic plans for the IC's information systems. In addition, we will follow up on steps the ODNI has taken to address recommendations made in our FISMA Reports for Fiscal Years 2008, 2009, and 2010.

(U) Inspections Division

(U) Evaluation of the President's Daily Briefing (PDB): Sources, Resources, Processes and Outcomes

(S//NF) In August 2009, the ODNI OIG began an evaluation of the PDB. The evaluation's objectives were to: [redacted] (b)(3)

In August 2010, after completion of our field work, The Honorable James R. Clapper, Jr., became the Director of National Intelligence. After assuming office, Director Clapper engaged the President and senior Presidential advisors on how to continue tailoring the PDB to meet the President's needs and was subsequently briefed on the draft PDB evaluation recommendations and findings. Director Clapper thereafter reorganized the PDB book and briefing, modified PDB art forms, and expanded the use of expert briefings.

(U//FOUO) In light of these developments and to ensure that the final OIG report captures and evaluates the current PDB enterprise, in February 2011 we temporarily suspended our evaluation and issuance of a final report to allow these and other changes to mature. We identified additional issues meriting management's attention, which are important for

management to address before we resume our evaluation. We asked stakeholders to document their decisions and progress in these issue areas to expedite the evaluation when it resumes. We also requested stakeholders' cooperation in maintaining situational awareness of the PDB enterprise.

(U) Investigations Division

(U//FOUO) Alleged Unauthorized Contract Commitments

(U//FOUO) The OIG is investigating allegations that a senior official and a subordinate made several unauthorized ODNI financial commitments in violation of ODNI policy and government acquisition regulations.

(U//FOUO) OIG Complaint Intake System

(U//FOUO) The OIG receives allegations of misconduct from IC employees and the general public on a variety of violations. During this reporting period, the OIG received 28 complaints, which included allegations of ethics violations, contract fraud, and misuse of position. The OIG has investigated or referred each of these cases to the appropriate IC investigative element.

(U) Intelligence Oversight Activities

(U) Assistance to President's Intelligence Oversight Board

(U) Executive Order (E.O.) 13462 established the Intelligence Oversight Board (IOB) as a subcommittee of the President's Intelligence Advisory Board (PIAB). Under E.O. 13462, the DNI analyzes IC component intelligence oversight reporting submitted jointly to the IOB and DNI and reports results of investigations and intelligence activities. The ODNI oversight team is staffed with experienced officers from ODNI OIG, ODNI Office of the General Counsel (OGC), and ODNI Civil Liberties and Privacy Office (CLPO).

(U//FOUO) The ODNI oversight team worked closely with IOB staff to review and assess incoming intelligence oversight reporting. Pursuant to the September 2010 *Intelligence Oversight Board's Concept of Operations,* the ODNI oversight team and IOB staff reached out to IC oversight personnel from each IC element. Individual meetings with oversight personnel from each IC element allowed the ODNI oversight team and IOB staff to address the impact of the policy changes for that IC element, to reinforce IOB reporting requirements, and to stress the importance of timely reporting and feedback on IOB matters.

(U) Oversight of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008

(U//FOUO) The OIG is a member of the joint ODNI and Department of Justice oversight team, which assesses IC compliance with procedures and guidelines issued pursuant to § 702 of the FISA, 50 U.S.C. § 1801 *et seq.*, as amended by the FISA Amendments Act of 2008 (FAA), 50 U.S.C. § 1881a. The OIG participated in a number of reviews. The results of these FISA FAA compliance reviews are summarized by the DNI and the Attorney General in joint semiannual reports submitted to the Senate Select Committee on Intelligence, House Permanent Select Committee on Intelligence (HPSCI), Senate Judiciary Committee, House Judiciary Committee, and the Foreign Intelligence Surveillance Court.

(U) Strategic Planning to Support Transition to Office of the Inspector General of the Intelligence Community

(U) The OIG began developing a strategic plan to support the eventual stand-up of the Office of the Inspector General of the Intelligence Community, an office established by the FY 2010 Intelligence Authorization Act. These efforts involved benchmarking, identifying possible requirements or gaps in current policy and processes, initiating development of a cost-model to support a separate OIG budget, assessment of staffing requirements for variable workloads, and scoping of objectives to support a phased transition. Our benchmarking efforts included interviews with both standing and newly created statutory OIGs, including the Special Inspector General Troubled Asset Relief Program, Special Inspector General for Afghanistan Reconstruction, Special Inspector General for Iraq, Federal Housing Finance Agency OIG, and Export/Import OIG, as well as the [redacted] The information developed from our benchmarking – including flexibility considerations, resources, professional staff recruitment and retention, and identification of best practices – informed the development of a cost model, staffing options, and a phased transition for varied levels of maturity. (b)(3)

VI. (U) Congressional Engagements

(U//FOUO) The OIG briefed House Permanent Select Committee on Intelligence (HPSCI) and Senate Select Committee on Intelligence (SSCI) congressional staffers on congressionally-directed actions (CDAs) assigned to the Inspector General of the Intelligence Community (IC IG) in the FY 2010 Intelligence Authorization Act (IAA). Even though these CDAs are assigned to the IC IG, the ODNI IG, after consultation with the IC IG Forum members, decided to engage with the congressional oversight staffs on the scope, objectives, and timeline for each of these reporting requirements as they will impact the resources of all the IC OIGs.

(U//FOUO) OIG staff engaged with congressional staff on CDAs regarding the IC's ability to share cyber-threat information; IC security clearance reciprocity; Electronic-waste; and other classified congressional reporting requirements. These engagements have prepared the

OIG staff to meet the statutory congressional reporting requirements following confirmation of the IC IG.

VII. (U) Status of OIG Recommendations

(U) At the close of previous reporting period (ending 31 December 2010), there were 13 OIG reports, which contained a total of 183 recommendations, of which 151 recommendations were closed (82 percent) and 32 recommendations remained open (17 percent). At the end of this reporting period, 75 percent of the recommendations in the reports listed in the table below are closed (designated in green), and 25 percent remain open (no color designation).[1] As illustrated in Appendix A, recommendations are "closed" if they have been fully implemented and "open" if they have not been fully implemented.[2]

(U) In the past 6 months, 18 recommendations in 9 different OIG reports have been closed. Significantly, during this reporting period, the ODNI developed and executed a formal ODNI process for timely responding to OIG recommendations and for tracking implementation of recommendations.

(C//NF)

(b)(3)

First and foremost, upon his arrival, Director Clapper clearly articulated that the core mission of the ODNI is to lead intelligence integration and that protecting the Homeland is job #1 for the Intelligence Community. To drive this message and better align the organization to the mission, Director Clapper has "re-set" ODNI's activities and personnel and, together with the ODNI and IC elements' Public Affairs Offices, used ODNI and IC publications, web sites, Town Halls, and speaking engagements by ODNI senior leadership in both classified and unclassified venues to reinforce the integration message. These messages also have been reinforced on the official ODNI Facebook page, open to the general public. These strategic communication efforts clarify the ODNI's role and mission, communicate its unique value to the intelligence enterprise, and close a recommendation in the OIG's 2008 IC-Wide Integration and Collaboration Diagnostic.

[1] (U) The increase in the percentage of open recommendations at the close of this reporting period is the result of the inclusion of open recommendations that were not previously counted because the deadline for implementation had not expired.

[2] (U) In previous semiannual reports, the OIG has reported on all recommendations made in OIG reports completed since 2007, even when all recommendations have been closed in some of those reports. Starting with this semiannual report, the OIG will include in its table only those reports that either have open recommendations or recommendations that closed during this reporting period. As a result, we are not including in this report table approximately 126 recommendations that have been previously closed. For a cumulative list of the number of all OIG report recommendations issued in reports since 2007, see Appendix B.

(U//FOUO) The ODNI also implemented several recommendations from the OIG's Review of IC-Wide Dissemination of Sensitive Reporting, including executing new processes for managing access and dissemination and developing technical capabilities that provide for a common architecture to deliver sensitive reporting. As a result, the ODNI has made significant progress in developing a common framework for managing access and dissemination of sensitive reporting. Moreover, in addressing recommendations from the OIG's Inspection of IC Acquisition Oversight Strategies Policies and Processes, the ODNI established a process to track and address instances of IC agency non-compliance with IC acquisition policy, which strengthens the ODNI's oversight of IC acquisitions and closes one of the five remaining recommendations in the report.

(U//FOUO) In addition, the ODNI has closed a total of 8 recommendations from our FY 2009 and FY 2010 FISMA reports. These recommendations were designed to reduce the vulnerability of ODNI systems to attack and compromise of critical information. Implementation of these recommendations has improved the accuracy of the ODNI's system inventories, clarified responsibilities for IT security, strengthened the ODNI's incident response and reporting program, and facilitated the planning and performance of contingency plan tests on IT systems. The ODNI has continued to make significant progress toward ensuring that it has an effective information security program.

Appendices

This Page Left Intentionally Blank

(U) Appendix A: ODNI OIG Open Recommendations and Recommendations Closed This Reporting Period.

(U) In previous semiannual reports, the OIG has reported on all recommendations made in OIG reports completed since 2007, even when all recommendations have been closed in some of those reports. Starting with this semiannual report, the OIG will include in the table only those reports which have either open recommendations or recommendations closed during the current reporting period. As a result, we are not including in this report table approximately 126 recommendations which have been previously closed. For a cumulative list of all OIG report recommendations issued in reports since 2007, see Appendix A.

(b)(3)

(U) EVALUATION OF THE ADMINISTRATION AND MANAGEMENT OF ODNI CORE CONTRACTS SUPPORTING CRITICAL MISSIONS (Issued July 2011)

Report Total: 5 Recommendations; 5 Open; 0 Closed

Summary of Open Recommendations

Recommendation	Responsible Office	Corrective Action
(U//FOUO) 1.1: Within 180 days of the issuance of this report, the Chief Management Officer should publish an ODNI Strategic Plan that includes ODNI-specific missions, goals, and objectives to facilitate decisions related to contractor support.	CMO	(U) New recommendation. No action yet taken.

Recommendation	Responsible Office	Corrective Action
(U//FOUO) 1.2: Within 180 days after publishing the ODNI-specific Strategic Plan, the Chief Management Officer should develop and publish an ODNI Strategic Human Capital Plan, based on the necessary workforce analysis, which includes clearly defined core functions and core competencies for ODNI government personnel; mission-critical occupations; and guidance for ODNI offices to determine the optimal balance of government and contractor personnel.	CMO	(U) New recommendation. No action yet taken.
(U//FOUO) 2.1: Within 180 days of the issuance of this report, the Chief Management Officer and the Director, Mission Support Division should: a. Modify the Service Level Agreement between the ODNI and the CIA to include performance measures or other mechanisms to ensure that the contracting services being provided under the interagency acquisition agreement are meeting ODNI needs and comply with federal authorities. b. Amend the Service Level Agreement with the CIA to include a meaningful dispute resolution procedure and authorize ODNI to access, upon request, copies of relevant ODNI contract information in accordance with the ODNI's fiscal and management responsibilities. c. Issue instructions for the development of quality verification procedures and for implementing enhanced controls when contractors perform tasks closely supporting inherently governmental functions. d. Ensure Letters of Delegation are issued by contracting officers in a timely manner to each ODNI COTR.	CMO, MSD	(U) New recommendation. No action yet taken.
(U//FOUO) 3.1: Within 270 days of this report, or 90 days following the completion of the ODNI Strategic Plan, the Chief Management Officer and the Director, Mission Support Division should: a. Identify COTRs as a critical skill and mission-critical occupation in the Strategic Human Capital Plan recommended in Recommendation 2. b. Develop and disseminate guidance on criteria for the selection and assignment of COTRs; a COTR performance reward program; and, appropriate recognition of COTR duties in performance appraisals. c. Develop procedures to formally manage Government Points of Contact (GPOCs) who assist COTRs in overseeing contractor activities. d. Include a detailed block of instruction on service contracts in the ODNI COTR training program.	CMO, MSD	(U) New recommendation. No action yet taken.
(U//FOUO) Within 270 days of this report, or 90 days following the completion of the ODNI Strategic Plan, the Assistant Director of National Intelligence for Policy & Strategy should: a. Modify Annex D to ICD 610 to identify the supervision of COTRs by IC senior officials as a core competency under "Business Acumen."	P&S	(U) New recommendation. No action yet taken.

(U) FISCAL YEAR 2010 INDEPENDENT EVALUATION OF ODNI COMPLIANCE WITH FISMA (Issued Sept. 2010)

Report Contains 23 Recommendations: 20 Open; 3 Closed in this Reporting Period; 7 Previously

Summary of Recommendations Closed During this Reporting Period

Recommendation	Responsible Office	Corrective Action
(U//~~FOUO~~) 1.1 a: Assign responsibility for timely updating and reconciling D/MSC and IC IT Registry system inventories.	MSC	[redacted]
(U//~~FOUO~~) 4.1.b: Revise its Service Agreement (SA) with ISG to clarify ISG and MSC responsibilities for security.	MSC	[redacted]
(U//~~FOUO~~) 5.1.a: Revise and update the incident response and reporting program to include OMB's expectations for comprehensive analysis, validation, documentation, and resolution of incidents in a timely manner and timely reporting of incident data to appropriate authorities.	MSC	[redacted]
(U//~~FOUO~~) 5.1. b: Amend the Service Agreement with ISG to explicitly include requirements delineating specific roles and responsibilities that ISG will perform in assisting with the incident response and reporting functions; alternatively, MSC should institute measures that address incident response and reporting functions required by OMB.	MSC	[redacted]
(U//~~FOUO~~) 8.1.b: Complete contingency plans for all systems with availability level of concern ratings of medium or greater.	MSC	[redacted]

(b)(5)

Summary of Open Recommendations		
Recommendation	Responsible Office	Corrective Action
(U//FOUO) I.1. b: Reconcile MSC internal inventories with the IC IT Registry and make system additions, deletions, or adjustments to the IC IT Registry at a minimum on a quarterly basis. *(U//FOUO) Repeats 2009 Recommendations 1.1 and 1.2, due to be completed in January 2010.*	MSC	[redacted]
(U//FOUO) 1.2 b: Reconcile IECC internal inventories with the IC IT Registry and make system additions, deletions, or adjustments to the IC IT Registry at a minimum on a quarterly basis. *(U//FOUO) Repeats 2009 Recommendations 1.1 and 1.2, due to be completed in January 2010.*	CIO	[redacted]

(b)(5)

Recommendation	Responsible Office	Corrective Action
(U//~~FOUO~~) 2.3: We recommend that within 180 days of this report (14 March 2011), the D/MSC should formalize and document the process as well as perform security tests on the systems that currently have security tests that are greater than 1-year old.	MSC	
(U//~~FOUO~~) 2.4 a: Perform security tests on systems that currently have security tests that are greater than 1-year old.	CIO	
(U//~~FOUO~~) 2.4. b: Perform annual security tests on systems with a PL greater than 1 within 12 months of their accreditation date or the date of last testing.	CIO	
(U//~~FOUO~~) 3.3: We recommend that within 60 days of this report, the IC CIO should develop a certification and accreditation strategy including a schedule for accrediting its systems (systems should be certified and accredited within 12 months and the IC IT Registry updated accordingly). *(U//FOUO) Repeats 2009 Recommendation 2.0, due to be completed in Jan. 2010.*	CIO	
(U//~~FOUO~~) 4.1. a: Revise the security configuration management oversight program for its systems that includes OMB's FY 2010 FISMA requirements.	MSC	

(b)(5)

Recommendation	Responsible Office	Corrective Action
(U//FOUO) 4.1.c: Establish responsibility for those CM functions that MSC will not include in the Service Agreement with ISG.	MSC	[redacted]
(U//FOUO) 4.1.d: Ensure the proper implementation of FDCC standards according to the milestones established for intelligence agencies and document deviations from those standards when appropriate.	MSC	[redacted]
(U//FOUO) 4.2.a: Establish a security configuration management program for its systems that meets OMB's FY 2010 FISMA requirements.	CIO	[redacted]
(U//FOUO) 4.2.b: Ensure the proper implementation of FDCC standards according to the milestones established for intelligence agencies and document deviations from those standards when appropriate.	CIO	[redacted]
(U//FOUO) 5.2. a: Finalize its draft Intelink Incident Response Plan and ensure that it meets or exceeds all requirements established by OMB and FISMA.	CIO	[redacted] requirements.

(b)(5)

Recommendation	Responsible Office	Corrective Action
(U//~~FOUO~~) 5.2b: Establish an incident response and reporting program that meets OMB's expectations for comprehensive analysis, validation, documentation, and resolution of incidents in a timely manner timely reporting of incident data to appropriate authorities.	CIO	
(U//~~FOUO~~): 6.2: We recommend that within 60 days of this report, the IC CIO should develop a written Plan of Action and Milestones (POA&M) program for the IECC. *Repeats 2009 Recommendation 5 a, b, c. due to be completed in Nov. 2009.*	CIO	
(U//~~FOUO~~) 7.1: We recommend that within 180 days of this report, the D/MSC should establish and document a continuous monitoring program incorporating all of OMB's requirements.	MSC	
(U//~~FOUO~~) 7.2: Within 90 days of this report, the IC CIO should establish and document a continuous monitoring program incorporating all of the OMB requirements.	CIO	
(U//~~FOUO~~) 8.2a: Establish a contingency plan program including, at a minimum, the areas outlined in the OMB FY 2010 FISMA metrics.	CIO	
(U//~~FOUO~~) 8.2.b: Establish a plan for performing contingency plan tests on systems whose contingency plans are greater than 1-year	CIO	
(U//~~FOUO~~) 8.2.c: Perform contingency plan tests on all systems with availability ratings of high.	CIO	
(U//~~FOUO~~) 8.2.d: Establish contingency plans for all systems with availability ratings of medium or greater.	CIO	

(b)(5)

(U) INCREASING THE VALUE OF INTELLIGENCE COMMUNITY FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) REPORTS (Issued June 2010)

Report Total: 4 Recommendations; 0 Open; 4 Closed; 4 Closed this Reporting Period; 3 Previously

Summary of Recommendations Closed During This Reporting Period

Recommendation	Responsible Office	Corrective Action
(U) Recommendation 2-2. Within 120 days of this report date, the IC CIO should establish a detailed plan of action and milestones necessary for developing and implementing a classified version of Cyberscope for purposes of FY 2011 FISMA reporting.	CIO	(U) 28 Dec. 2010: IC CIO provided a detailed project plan for implementing CyberScope. OIG's review shows that it meets the requirements for this recommendation.

(U) THE INTELLIGENCE COMMUNITY CIVILIAN JOINT DUTY PROGRAM: IMPLEMENTATION STATUS REPORT (Issued Nov. 2009)

Report Total: 20 Recommendations; 1 Open; 19 Closed; 1 Closed this Reporting Period; 18 Previously

Summary of Recommendations Closed During This Reporting Period

Recommendation	Responsible Office	Corrective Action
(U) 17: We recommend that the ADNI/CHCO collect data from each IC element annually to track bonus data, comparing Joint Duty Program participants with their non-participant peers.	CHCO	(U) 23 June 2011: Recommendation closed: Many factors beyond Joint Duty assignment impact a bonus decision - job performance, job responsibilities, agency policies/practices, resource availability/priorities, etc. - making it a questionable metric as to whether a participant is disadvantaged when measured against a non-participant peers. Furthermore, in our current austere fiscal environment, JDA bonus receipt as a metric may be even less applicable.

(U) FISCAL YEAR 2009 INDEPENDENT EVALUATION OF ODNI COMPLIANCE WITH FISMA (Issued July 2009)

Report Total: 53 Recommendations; 1 Open; 52 Closed; 3 Closed this Reporting Period; 49 Previously

Summary of Recommendations Closed During This Reporting Period

Recommendation	Responsible Office	Corrective Action
(U//FOUO) 1.1.a.2. Develop and maintain an accurate inventory of systems.	MSC	(U//FOUO) 24 March 2011: Closed based on OIG review of existing inventory provided on 21 March 2011.
(U//FOUO) 1.2. b. The ADNI/CIO and the Director of MSC should reconcile the ADNI/CIO and MSC inventories with the IC Registry, at a minimum, on a quarterly basis.	MSC	(U//FOUO) 24 March 2011: Closed based on OIG review of existing inventory and evidence of system additions and deletions for 2011.
(U//FOUO) 1.1.c.2: Make system additions deletions or adjustments to the Intelligence Community's (IC) Registry in a timely manner.	MSC	(U//FOUO) 23 June 2011: IC CIO will maintain registry for IC.

Summary of Open Recommendations		
Recommendation	Responsible Office	Corrective Action
(U//FOUO) I.1.a.1: Develop and maintain an accurate inventory of systems	CIO	
(U//FOUO) I.1.c.1: Make system additions deletions or adjustments to the Intelligence Community's (IC) Registry in a timely manner.	CIO	
(U//FOUO) I.2.a: The ADNI/CIO and the Director of MSC should reconcile the ADNI/CIO and MSC inventories with the IC Registry, at a minimum, on a quarterly basis.	CIO	
(U//FOUO) I.2.b: The ADNI/CIO and the Director of MSC should reconcile the ADNI/CIO and MSC inventories with the IC Registry, at a minimum, on a quarterly basis.	MSD	

(b)(5)

Recommendation	Responsible Office	Corrective Action
(U//~~FOUO~~) 2.0.a: The ADNI/CIO and the Director of MSC, within 180 days of this report (24 Jan. 2010), ADNI/CIO will develop a certification and accreditation strategy including a schedule (plan of action and milestones) for reaccrediting the cited systems and update this information in the IC Registry and the Director of the Mission Support Center will establish current certifications and accreditations for all systems identified under their ownership and update this information in the IC Registry.	CIO	
(U//~~FOUO~~) 3.0.a.1: Perform security tests on the systems that currently have security tests that are greater than a year old.	CIO	
(U//~~FOUO~~) 3.0.b.1: Perform annual security tests on systems with Protection level greater than protection level 1.	CIO	
(U//~~FOUO~~) 4.a.1: Establish a plan for performing contingency plan tests on systems whose contingency plan tests are greater than a year old and establish a designated period for future contingency plan tests.	CIO	
(U//~~FOUO~~) 4.b.1: Perform contingency plan tests on all systems with an availability rating of high.	CIO	
(U//~~FOUO~~) 5.a.1: Develop a uniform written plan of action and milestone process for the ODNI.	CIO	
(U//~~FOUO~~) 6.2.a: Adopt and implement Federal Desktop Core Configuration standard configurations and document deviations and security control deficiencies on desktops directly controlled by ODNI.	MSD	
(U//~~FOUO~~) 6.2.b: Implement Federal Desktop Core Configuration security settings into all Windows XP™ and Vista™ desktops directly controlled by the ODNI.	MSD	

(b)(5)

(b)(5)

INSPECTION OF IC ACQUISITION OVERSIGHT STRATEGIES, POLICIES, AND PROCESSES (Issued June 2009)		
Report Total: 11 Recommendations: 4 Open 7 Close (1 Closed this Reporting Period, 6 Previously)		
Summary of Recommendations Closed During This Reporting Period		
Recommendation	Responsible Office	Corrective Action
(U//FOUO) j: Establish a process to track and address instances of IC agency noncompliance with IC acquisition policy and process discipline breakdowns no later than 120 days after signature. An option the DNI may wish to consider is to establish ODNI staff liaison positions at the IC agencies to act as the forward-deployed focal points for all actions and information requests transmitted from the ODNI staff to an agency.		**(U//FOUO) This recommendation is closed. However, the OIG is concerned that the implementation of recommendations continues to ensure timely and effective reporting, compliance and accountability. Given this concern, and despite closure of this recommendation, the OIG plans to initiate a follow-on inspection during FY 2012.**
Summary of Open Recommendations		
Recommendation	Responsible Office	Corrective Action
(U//FOUO) b: Publish IC policy no later than 120 days after signature, identifying a governance model for the ODNI AO workforce relative to the IC acquisition community, including: **A. Revising ICD 1 to account for current distributions of authorities and decision rights.** **B. Standardizing levels of official interface and protocol between ODNI officials and IC counterparts.** **C. Clarifying the role of the PDDNI relative to the codified authorities of the DNI's Milestone Decision Authority (MDA) (DDNI/FC), the DDNIs, the ADNIs, and DNI Policy for the IC.**	**MSC; P&S; CMO**	[redacted]
(U//FOUO) d: DDNI/FC enforces accountability for IC agencies to have validated requirements documents as a prerequisite for MDA delegation, and permanently add such language to DDNI/FC performance objectives no later than 360 days after signature. Additionally, when the DDNI/FC delegates MDA for a program without a validated requirements document, formal justification to the DNI shall be identified in an Acquisition Decision Memorandum.	**AT&F**	[redacted]

Recommendation	Responsible Office	Corrective Action
(U//FOUO) f: DDNI/FC, the CIO, and the Office of General Counsel to collaborate and codify statutorily compliant areas of oversight jurisdiction no later than 120 days after signature. We also recommend that the DNI and the CIO codify processes for oversight of IT programs under CIO jurisdiction no later than 120 days after signature, and maintain sufficient numbers of experienced IT professionals to execute the processes.	CIO	
(U//FOUO) i: DDNI/FC and DDNI/PPR to revise the Acquisition cross-cutting emphasis areas (ACCEA) no later than 150 days after signature, with the following objectives: A. Align goals with stated strategy elements: Policy Guidance, Monitoring, and Corrective Action. B. Update ACCEA Immediate Actions to address corrective action as a priority. C. Elevate workforce qualification and certification goals.	P&S; AT&F, OGC	

(b)(5)

(U) CRITICAL IC MANAGEMENT CHALLENGES (Issued Nov. 2008)		
Report Total: [illegible] Recommendations, [illegible] Open, [illegible] to Close, [illegible] Closed this Reporting Period, [illegible] Previously		
Summary of Recommendations Closed During This Reporting Period		
Recommendation	Responsible Office	Corrective Action
(U//FOUO) i: Develop a formal ODNI process for timely response to OIG recommendations and for tracking implementation of recommendations that are accepted by management.	CMO	(U//FOUO) OIG and ODNI Front Office finalized a joint protocol for handling OIG matters. The protocol became effective 25 Feb. 2011.

Recommendation	Responsible Office	Corrective Action
(U//FOUO) k: Revise the auditability strategy with target dates for achieving auditability based on standard financial systems and ICBT initiatives and monitor progress towards auditability.	CIO; CFO; BTO	(U//FOUO) Closed. Superceded by FY 2010 IAA. (U//FOUO) Draft document, based on COA final provided. BTO has not developed architecture system. (U//FOUO) 8 Dec. 2010: Sent email to FMO and CFO for update. (U//FOUO) The FIG (now FMO) will provide an updated auditability strategy to the SSCI within 4 months following the BTO's identification of an IC systems architecture. BTO has not identified an architecture, and there is no target date. Therefore, the FMO will not provide an auditability strategy to the SSCI in the foreseeable future. The FY 2010 Intel Auth Act also mandates ODNI develop an auditability strategy. (U//FOUO) Recommendation can be closed upon receipt of an FMO auditability strategy with target dates.

(U) FISCAL YEAR 2008 FISMA REVIEW (Issued Aug 2008)

Report Total: 10 Recommendations, 1 Open, 9 Considered Closed this Reporting Period, 9 Previously

Summary of Open Recommendations

Recommendation	Responsible Office	Corrective Action
(U) 1.a: CIO complete a documented comprehensive information security program consistent with FISMA requirements that includes the following elements: 1) periodic risk assessments; 2) policies and procedures based on risk assessments; 3) plans for providing appropriate information security; 4) Periodic testing and evaluation of the information security policies and procedures; 5) A process for developing a plan of action; and 6) Plans and procedures for developing continuity of operations for information systems.	CIO	[redacted] (b)(5)

(U) IC-WIDE INTEGRATION AND COLLABORATION DIAGNOSTIC AND RECOMMENDATIONS (Issued Aug 2008)

Report Total: 29 Recommendations, 2 Open, 27 Closed or Closed this Reporting Period, 26 Previously

Summary of Recommendations Closed During This Reporting Period

Recommendation	Responsible Office	Corrective Action
(U) q: Create a clear and succinct mission and vision statement for the ODNI. Publish and communicate the ODNI mission and vision to the ODNI and IC elements.	PAO; DIS	(U) 25 May 2011: The PAO published a new ODNI Mission and Vision Statement and launched a strategic communication strategy to drive these messages.

Summary of Open Recommendations		
Recommendation	Responsible Office	Corrective Action
(U) p: Identify, compile, maintain, and distribute to the IC a list of the expertise of all IC elements.	CHCO	[redacted]
(U) t: Establish an "Ask the DNI" link on the DNI homepage to solicit questions and comments from the IC workforce.	PAO	[redacted]

(b)(5)

(U) REVIEW OF IC-WIDE DISSEMINATION OF SENSITIVE REPORTING
(Issued Nov. 2007)

Report Total: [illegible] Recommendations, 0 Open, [illegible] Closed [illegible] Recommendations Identified in Reassessment

Summary of Recommendations Closed During This Reporting Period		
Recommendation	Responsible Office	Corrective Action
(U) c.1: Establish and promulgate IC standards and a process for the dissemination of sensitive intelligence reporting to ensure that customer requirements are better met. Standards should include or provide for a common definition of sensitive intelligence.	CIO; P&S	(U) The Chair of the Senior Review Group, also serving as the IC-ISE, has implemented new processes intended to address this recommendation. This recommendation is closed in order to allow implementation of the new processes with a specific proviso that the OIG plans to initiate a follow-up inspection in approximately 120 days to assess the new processes and review the definition of sensitive intelligence and related criteria.
(U) c.3: A common architecture that horizontally integrates the delivery of IC sensitive reporting while ensuring that adequate safeguards are in place.	CIO	(U) This recommendation is closed. The ADNI CIO continues to progress towards implementing and documenting a pilot capability and repeatable architecture for a Level 6 COI. The closure of this recommendation comes with the proviso that ADNI CIO will demonstrate a pilot capability for the Intelligence Community Compartmented Collaboration Environment (IC3E) Enterprise Phase 1 (EP1) to OIG and provide a copy of said architecture and related standards documentation to the OIG by the end of FY 2011.

Recommendation	Responsible Office	Corrective Action
(U) c.5.a: Based upon the results of our Phase Two review, we believe that the CIA joint review board or the dissemination office concept should be adopted by all major IC collection agencies. Agencies should participate in an IC-wide policy board with support and oversight provided by the ADNI/Dissemination. This would maximize Community integration, enhance information sharing, and make best use of available resources. Functions to be accomplished by the dissemination offices/review boards would include, but not be limited to: b. Reviewing all sensitive reporting for appropriateness of dissemination, unless the reporting is specifically exempted by the DNI or his designated representative. c. Overseeing requests for expanded dissemination and providing an appeals process for consumers to dispute collectors' dissemination decisions. In rare cases when an impasse occurs, the final decision authority will be the DNI or his designated representative. d. Coordinating reading requirements or developing alternatives to ensure consumer agencies and analytic components receive the intelligence they need. e. Developing training to ensure the proper handling and use of sensitive reporting by collection agencies, consumer agencies, and analytic components.	ISE	(U) The Chair of the Senior Review Group, also serving as the IC-ISE, has implemented new processes intended to address this recommendation. This recommendation is closed to allow implementation of the new processes with a specific proviso that the OIG plans to initiate a follow up inspection in approximately 120 days to assess the new processes and review the definition of sensitive intelligence related criteria.

(U) OIG Reports 2007 – 2011
Status of Recommendations (Active Reports)

Number of Recommendations*	Number Closed	Percent of Total	Number Open	Percent of Total
[redacted]				

(b)(3)

*(U) Does not include the two OIG recommendations from the June 2011 report, *Status of Integration of the Departmental and Service Intelligence Community Elements* and the five OIG recommendations from the July 2011 report, *Evaluation of the Administration and Management of ODNI Core Contracts Supporting Critical Missions*, for which the implementation deadline has not yet passed.

(U) Appendix B: Comprehensive Summary of ODNI OIG Report Recommendations Since 2007

ODNI OIG REPORTS ISSUED (2007 – 2011)	Total Recs Made	Total Open	Total Closed
(U) Evaluation of the Administration and Management of ODNI Core Contracts Supporting Critical Missions (Issued July 2011)	5	5	–
(U) Status of Integration of The Departmental and Service Intelligence Community Elements (Issued June 2011)	2	2	–
(U) Audit of the Monitoring and Coordination of the Comprehensive National Cybersecurity Initiative by the DNI (Issued April 2011)	–	–	–
(U) Fiscal Year 2010 Independent Evaluation of ODNI Compliance with FISMA (Issued Sept. 2010)	32	20	12
(U) Increasing the Value of Intelligence Community Federal Information Security Management Act Reports (Issued June 2010)	4	–	4
(U) Internal Controls Over Fund Balance with Treasury (Issued Jan. 2010)	5	–	5
(U) The Intelligence Community Civilian Joint Duty Program: Implementation Status Report (Issued Nov. 2009)	20	–	20
(U) Department of Homeland Security Office of Intelligence and Analysis Audit (Issued Sept. 2009)	2	–	2
(U) Fiscal Year 2009 Independent Evaluation of ODNI Compliance with FISMA (Issued July 2009)	34	12	22
(U) Inspection of IC Acquisition Oversight Strategies, Policies, and Processes (Issued June 2009)	11	4	7
(U) Critical IC Management Challenges (Issued Nov. 2008)	16	–	16
(U) IC-Wide Integration and Collaboration Diagnostic and Recommendations (Issued Aug. 2008)	29	2	27
(U) FY 2008 Federal Information Security Management Act Review (Issued Aug. 2008)	10	1	9
(U) IC -Wide Review of the Terrorist Watchlist Nomination Process (Issued Feb. 2008)	9	–	9
(U) Review of IC-Wide Dissemination of Sensitive Reporting (Issued Nov. 2007)	9	–	9
RECOMMENDATIONS SUMMARY AS OF 30 JUNE 2011	190	46	144

(b)(1)
(b)(3)

* Active Reports in Bold

(U) Report Waste, Fraud, Abuse, or Misconduct

(U) To report allegations of waste, fraud, abuse, or misconduct in the ODNI or IC agencies, contact:

Office of the Inspector General
Office of the Director of National Intelligence
Investigations Division
Washington, DC 20511

Commercial: (703) 482-1300
[redacted]
or
OIG_Complaints@dni.gov

(b)(3)

(U) For additional copies of this or other ODNI OIG reports, contact:

Office of the Inspector General
Office of the Director of National Intelligence
Washington, DC 20511

Commercial: (703) 482-4955
[redacted]

[redacted]

(b)(1)
(b)(3)

[redacted]

(b)(3)

(U//FOUO) To provide an on-line, classified venue for members of the IC OIGs to collaborate and share best practices, the ODNI OIG launched the IC OIG Community of Interest. OIG personnel from across the IC are working together in planning conferences, IC IG Forum meetings, and posting OIG reports and articles and events of interest.

~~SECRET//NOFORN~~

(U) Office of the Director of National Intelligence

(U) Semiannual Report

1 January 2011 – 30 June 2011

~~SECRET//NOFORN~~