

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

OFFICE OF THE INSPECTOR GENERAL



**(U) CRITICAL INTELLIGENCE COMMUNITY MANAGEMENT
CHALLENGES**

November 12, 2008

**EDWARD MAGUIRE
INSPECTOR GENERAL**

UNCLASSIFIED

(U) Introduction

(U) This paper identifies the critical leadership and management challenges currently facing the Director of National Intelligence (DNI) as leader of the Intelligence Community (IC) and as head of the Office of the Director of National Intelligence (ODNI).

(U) The DNI's most critical management challenges are the following:

- 1. Strengthening leadership and governance.**
- 2. Accelerating progress in driving IC information sharing.**
- 3. Removing impediments to IC collaboration and integration.**
- 4. Improving financial management and acquisition oversight.**
- 5. Resolving major legal issues.**

(U) The ODNI Office of Inspector General (OIG) conducts oversight of IC programs and operations related to the authorities and responsibilities of the DNI. The ODNI Inspector General (IG), furthermore, chairs the IC Inspector General Forum, an organization comprised of IGs from all IC agencies, which undertakes joint reviews of important issues affecting the IC. In identifying the management challenges facing the DNI, we have drawn on inspections, audits, and reviews performed by our office and by IGs of other IC entities.

(U) We also have reviewed the current Management Challenges reports of the OIGs of most IC entities. While each IC entity has its own particular management challenges, many of them are common to and interconnected with challenges encountered throughout the IC. The perspective of this paper will be those challenges that fall within the DNI's responsibility under the Intelligence Reform and Terrorism Protection Act of 2004 (IRTPA) to lead and integrate the IC.

1. (U) Strengthening Leadership and Governance

(U) IRTPA charged the DNI with leading and transforming the IC, as well as serving as the principal intelligence advisor to the President and the National Security Council. IRTPA made the DNI responsible for improving intelligence information sharing; planning and monitoring the expenditure of funds; overseeing acquisitions; improving analysis; implementing a program of joint duty for IC professionals; and leading the National Counterterrorism Center (NCTC), the National Counterintelligence Executive (NCIX), the National Counterproliferation Center (NCPC), and other special centers.

(U) In its March 31, 2005, Report to the President, the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission) issued an important admonition concerning the DNI's management responsibilities:

The DNI's management responsibilities will be both critically important and exceedingly difficult, and there is a real risk that the obligation to provide current intelligence support to the President and senior policymakers will reduce or eliminate the attention the DNI can devote to the painstaking, long-term work of integrating and managing the community.¹

(U) Since inception of the ODNI in April 2005, the DNI has had to devote much of his time to providing intelligence support to the President and senior policymakers. IG reports have identified the need for the DNI to place stronger emphasis on management – defining and executing DNI authorities; imposing accountability for compliance with DNI directives; and communicating a clear statement of the respective roles, responsibilities, and authorities of ODNI staff and the IC agencies. IG findings regarding governance and communication challenges have been previously provided to ODNI senior leadership. Full engagement by the DNI in the management of the ODNI and the IC is a fundamental precondition to fulfilling the DNI's mission.

(U) The ODNI OIG has over the past 18 months performed two “diagnostic” studies: the first on the internal ODNI organization (2007), and the second on the state of integration and collaboration across the IC (2008).² Both reviews were carried out at the request of the DNI.

(U) Noteworthy findings include the following:

- The majority of the ODNI and IC employees (including many senior officials) whom we interviewed were unable to articulate a clear understanding of the ODNI's mission, roles, and responsibilities with respect to the IC.
- Many ODNI employees understand the objectives of IRTPA but do not know how the ODNI is implementing those objectives.
- ODNI employees voiced confusion about the lines of authority within the ODNI and criticized poor internal communications and lack of transparency.
- Employees in other IC agencies criticized the lack of information flowing from the ODNI to the IC.
- IC agencies complained that the ODNI sends duplicative taskings and conflicting messages to the IC, thereby undermining the ODNI's credibility and fueling assertions that the ODNI is just an “additional layer of bureaucracy.”
- The lack of clear communication to the IC of the ODNI staff's authorities has encouraged some agencies to go their own way, to the detriment of the unified and integrated intelligence enterprise envisioned by IRTPA.
- In many cases, the authorities of different agencies overlap or are thought to overlap, creating “lanes in the road” disputes, many of which continue to be unresolved.

¹ WMD Commission, *Report to the President of the United States*, p. 361 (March 31, 2005).

² *Organizational and Cultural Diagnostic* (September 2007); *IC-Wide Integration and Collaboration Diagnostic and Recommendations* (August 2008).

(U) Contributing to the confusion about ODNI responsibilities and authorities are the delays in issuing guidance to the IC. For example, over 20 draft IC Directives (ICD) (the major IC policy instrument used by the DNI) are still in the ODNI review process, some having been there for more than two years. In addition, the need to issue a large volume of guidance implementing new Executive Order (EO) 12333 will increase the backlog. The timely issuance of directives to the community is a core function and responsibility of the ODNI. This is a critical management task that the DNI must address.

(U) The DNI should establish and implement a process to respond to and track OIG recommendations. The Central Intelligence Agency (CIA) and other IC agencies, for example, have established formal processes for responding to IG recommendations and for tracking the implementation of those accepted.

(U) The OIG also identified several management/governance issues during its inspection of Advanced Geospatial Intelligence (AGI) capabilities and programs across the IC.³ These issues raise fundamental questions concerning decision making in the IC that require affirmative engagement by the DNI:

- The DNI must support the National Geospatial-Intelligence Agency (NGA) in its capacity as the Geospatial Intelligence (GEOINT) functional manager for the IC.⁴
- The DNI must provide guidance to NGA regarding GEOINT and AGI analytic tradecraft.
- The DNI must provide an effective mechanism for improving analytic access to sensitive programs and data.

(U) The ODNI OIG's ongoing inspection of ODNI acquisition oversight has identified similar challenges in the effective execution of the DNI's acquisition oversight authority.

(U) In addition to ODNI OIG reviews, the 2007 ODNI Employee Climate Survey, conducted by the IC Chief Human Capital Officer, identified declining employee confidence in ODNI leadership. Comparing the results for 2007 with those of 2006:

- The number of ODNI employees reporting "satisfaction with the policies and practices of ODNI senior leaders" declined 13%.
- The number of ODNI employees reporting a "high level of respect for ODNI senior leaders" declined 10%.

³ *Review of IC-Wide Application of Advanced Geospatial Intelligence (Draft).*

⁴ With the issuance of amended EO 12333 in July 2008, the roles and responsibilities of the functional managers for the IC are now more clearly defined. Further improvement will come from future issuance of internal policies and practices at IC elements implementing the guidance in EO 12333.

(U) The DNI should proceed without delay to:

- Create a clear and succinct mission statement for the ODNI and disseminate it throughout the IC.
- Communicate a transparent governance model to the IC identifying the roles, responsibilities, and authorities of the ODNI staff relative to the IC agencies.
- Define the relative internal authorities of the DNI, Principal Deputy Director for National Intelligence (PDDNI), and other ODNI senior staff.
- Finalize and publish critical ICDs, including:
 - ICD 101 - “Policy System”
 - ICD 303 - “MASINT Collection”
 - ICD 306 - “GEOINT Collection”
 - ICD 501 - “Access to and Dissemination of Intelligence”
- Develop a formal process for timely responding to OIG recommendations and for tracking implementation of recommendations that are accepted by management.

2. (U) Accelerating Progress in Driving IC Information Sharing

(U) The WMD Commission Report stated that “No shortcoming of the Intelligence Community has received more attention since the September 11 attacks than the failure to share information.”⁵

(U) Inadequate information sharing is a major impediment to effective IC performance. IRTPA requires the DNI to ensure maximum availability of and access to intelligence information and to establish policies and procedures to resolve conflicts between the need to share intelligence information and the need to protect intelligence sources and methods. Additionally, EO 12333 requires the DNI to establish common security and access standards across the IC.

(U) IG inspections, audits, and reviews from across the IC indicate that the ODNI has not fully implemented the policies and procedures needed to achieve the level of information sharing contemplated by IRTPA and EO 12333. For example, in our 2007 report on the dissemination of sensitive intelligence,⁶ we found:

- Most analysts still rely on personal relationships with counterparts to acquire much of their intelligence data, especially if that data is from compartmented programs.
- Agencies responsible for developing collection systems continue to control and limit access to data and products essential for analysis across the IC.

⁵ WMD Commission, *Report to the President of the United States*, p. 320.

⁶ *Review of IC-Wide Dissemination of Sensitive Reporting: Findings and Recommendations* (November 2007).

- Analysts have no avenue for review or adjudication when they are denied access to information.

(U) We made several recommendations for corrective action in a draft of the dissemination report provided to the DNI in early 2007. In March 2007, the DNI directed that all of the recommendations be implemented by July 2007. To date, none of the recommendations has been fully implemented. The ODNI, for example, has not finalized ICD 501, "Access to and Dissemination of Intelligence." In addition, the ODNI proposal for creating sensitive reporting review boards remains in draft form. Other IC-wide policies for information sharing also have not been issued.

(U) Reviews and inspections by the ODNI OIG and IC IGs revealed that the following additional impediments to information sharing within the IC that can only be resolved through the leadership and oversight of the DNI:

- IC information technology (IT) systems are largely disconnected and incompatible.
- The IC continues to operate on multiple networks that lack interoperability.
- The IC has no standard architecture supporting the storage and retrieval of sensitive intelligence.
- Intelligence information and reports are frequently not being disseminated in a timely manner.
- IT systems remain vulnerable.
- The ODNI has not fully implemented recommendations from the ODNI OIG's Fiscal Year (FY) 2007 Federal Information Security Management Act (FISMA) review.

(U) However, the IC has made some significant improvements in information sharing, some of which we note below:

- In 2003, the CIA developed a system, which allows the secure, electronic dissemination of sensitive human intelligence (HUMINT) reporting to IC analysts at their desktop in a way that protects sources and methods.
- The Deputy Director for National Intelligence (DDNI) for Analysis has developed a virtual work environment that provides IC analysts with a common platform to conduct research and connect more easily with colleagues working the same or similar issues.
- IC IGs have noted significant advances in the areas of dissemination and security, such as implementation of the IC-wide badge initiative.

(U) Despite these improvements, the IC's information sharing problems will persist as long as the ODNI fails to implement and enforce critical IC-level policies and processes for information sharing.

(U) Driving IC information sharing will require the DNI to:

- Publish ICD 501 and supporting directives providing IC-level policies that expand and improve information access for the analytic community.
- Implement all of the recommendations in the OIG's dissemination of sensitive intelligence report and FISMA audit.
- Implement the ODNI proposal for creating sensitive reporting review boards.
- Develop and implement an IC plan for standardizing communication systems and streamlining the IC data sharing and storage architecture to reduce redundancy and simplify data access and retrieval.

3. (U) Removing Impediments to IC Collaboration and Integration

(U) The DNI is responsible for building an interactive and integrated IC that can successfully identify and assess the threats of the 21st century. With 17 separate organizations in the IC, including several entities new to the IC, integration and collaboration present a persistent and daunting challenge.

(U) IC IG audits, inspections, and reviews have found that IC elements do not consistently and effectively collaborate and integrate their program efforts, resources, and talents. This impairs the IC's ability to develop intelligence collection and analysis capabilities and deliver actionable intelligence to consumers.

(U) Our 2007 diagnostic revealed that within the ODNI poor collaboration has resulted in "turf battles" among some of the ODNI offices, causing information and activities to be "stove piped." This remains a persistent management challenge.

(U) In addition to the diagnostic, ODNI and IC OIG inspections and reviews have found that:

- Collaboration has not been sufficiently defined, promoted, and incentivized across the IC. While the leadership of some IC elements support IC collaboration in principle, the culture of protecting "turf" remains a problem, and there are few, if any, consequences for failure to collaborate. Moreover, some IC agencies have interpreted the DNI's support for collaboration to mean that the IC is managed only by the consent of the major IC agencies, which is inconsistent with the DNI's authorities under IRTPA.
- The effectiveness of the IC Joint Duty Program (Joint Duty) is at risk because of inconsistent participation in the program, lack of support from IC leaders, and limited understanding of Joint Duty opportunities.
- There is no overall IC strategy or leadership structure to drive collaboration among national intelligence agency and law enforcement organizations. No agency or official has taken up the important task of establishing resource

allocation authorities, providing intelligence training, and developing processes required to establish and prioritize joint requirements, strategies, and missions.⁷

- IC elements do not effectively collaborate in defining requirements for systems and acquisitions. When conducting two inspections, we found that several IC agencies have not consistently engaged with each other in order to define and develop collection and complimentary exploitation and analysis capabilities.
- FBI collaboration with the IC is hampered by frequent turnover within FBI senior management ranks and by outdated IT systems. This has adversely affected the FBI's ability to forge effective relationships within the IC.
- The Terrorist Screening Center's (TSC) watch list is a critical collaboration tool for the IC, but management of the consolidated federal terrorist watch list continues to have weaknesses and lacks important safeguards for ensuring data integrity.⁸

(U) The DNI should take the following steps to advance IC collaboration and integration:

- Require collaboration among the national agencies on programs, systems, and acquisitions in accordance with functional management authorities and responsibilities.
- Define "collaboration" for the IC to include agency compliance with DNI decisions.
- Appoint a senior ODNI official responsible for improving collaboration and integration between and among 'traditional' intelligence agencies (those focused exclusively on intelligence gathering and analysis, such as CIA, National Security Agency (NSA), Defense Intelligence Agency (DIA) and NGA) and IC entities that have dual law enforcement and intelligence missions, such as the FBI and DHS.

4. (U) Improving Financial Management and Acquisition Oversight

(U) Financial Management

(U) Under IRTPA, the DNI is the primary authority for managing and directing the financial resources and funding of IC activities, systems, and capabilities. The DNI is also responsible for developing and applying financial management policies and strategies that ensure optimal use of National Intelligence Program (NIP) funding. Financial accountability is critical to the DNI's effective exercise of fiscal responsibilities throughout the IC.

⁷ The absence of IC leadership is illustrated by the fact that, in January of 2006, the PDDNI requested that the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) draft and sign a Memorandum of Understanding (MOU) to clarify roles and responsibilities of each regarding Fusion Centers. The DHS was responsible for drafting of the MOU, which has yet to be signed.

⁸ See the Department of Justice OIG *Follow-Up Audit of the Terrorist Screening Center, Audit Report 07-41* (September 2007).

(U) Financial statements are the method used for reporting to stakeholders on agencies' stewardship of resources provided by Congress. In contrast to many other Federal agencies, most of the IC is struggling to achieve auditable financial statements. Congress has expressed significant interest in the IC's plans and progress in achieving auditability, and has called on the IC to modernize and consolidate its financial and business systems.

(U) The Senate Select Committee on Intelligence (SSCI) had originally required IC financial statement audits to be performed by March 2005, and later required the DNI to submit a Business Enterprise Architecture, an Enterprise Transition Plan, a Financial Audit Plan, and a Human Resources Financial Professional Improvement Plan by April 2007.

(U) In February 2007, the DNI issued a Financial Statement Auditability Plan (Plan) to Congress, which outlined actions necessary for six IC components – NSA, CIA, DIA, NRO, NGA, and ODNI to achieve auditability by 2012. The Plan states that the ODNI will lead and manage the auditability effort by establishing milestones and metrics, putting capable leaders in charge and providing them the resources and support to do the job, and holding leaders accountable for results.

(U) In 2007, the ODNI established a Financial Improvement Group (FIG) under the ODNI Chief Financial Officer (CFO) to facilitate, coordinate, and oversee IC-wide fiscal accountability and to achieve auditability by the year 2012. The ODNI also established the Financial Management Governance Structure, which is supported by a CFO Council composed of CFOs from all IC elements, to oversee financial management improvements outlined in the IC's 2007 Financial Statement Auditability Plan. Moreover, the ODNI has developed IC corporate metrics and milestones for the President's Management Agenda's financial management scorecard that are focused on removing barriers to auditability.

(U) In addition, in late 2007, the ODNI CFO and OIG established a Joint CFO/IG Council to review IC-specific accounting issues. The Joint CFO/IG Council is developing a process for IC components to submit IC-unique accounting issues to the Federal Accounting Standards Advisory Board.

(U) Subsequently, the ODNI conducted a comprehensive assessment of IC financial and business systems, and in March 2008, informed Congress that the IC will consolidate the CIA, NRO, NSA, DIA, NGA, and ODNI core financial management systems into two systems, with the goal of eventually consolidating them into one.

(U) In October 2008, the IC agreed on a phased approach to transform IC business systems around the two core financial management system environments and to establish a business transformation office to oversee these efforts. Recognizing that financial systems support not only auditability but overall mission performance, the ODNI CFO and Chief Information Officer (CIO) expanded the FIG effort and jointly

initiated the IC Business Transformation (ICBT) effort to standardize and consolidate core business systems. Congress approved the ICBT initiative and funded the Business Transformation Office (BTO) in October 2008.

(U) Congress and the BTO recognize that while the ICBT initiative will delay auditability, it will update and consolidate IC business practices and processes, identify systems inventories, eliminate redundancy, address data standardization, and thereby move the IC closer to sound financial management. The BTO also acknowledges that for ICBT to succeed, it must receive substantial senior level support across the IC and across functional components beyond the CFOs.

(U) Neither the ODNI OIG nor the other IC OIGs have yet conducted a review or audit of the new ICBT initiative. However, several of the IC OIGs and CFOs have expressed concern about the impact on financial auditability from the shift to business transformation. One intelligence agency anticipated receiving an unqualified audit opinion by FY 2011, but stated that ICBT-related funding restrictions for systems development may delay that date. Similarly, another OIG worried that the push from Congress and ODNI to align financial systems throughout the IC could potentially derail progress toward achieving an unqualified audit opinion and divert resources that should be used to achieve auditability and sound financial management practices.

(U) In addition to these concerns, IC OIGs' audits have identified the following major impediments to producing auditable financial statements:

- Internal control weaknesses.
- Ineffective processes, inadequate procedures, insufficient documentation, incorrect accounting models, and inaccurate balances.
- Lack of a comprehensive financial management strategy and system that addresses organizational resources and capabilities.
- Unreliable, disparate, and antiquated financial systems.

(U) The ODNI CFO also identified the lack of consistent definition of "systems." The CFO stated that until the IC clearly defines what constitutes a "system," the identification of systems inventories, systems consolidation, and elimination of system redundancies will not occur.

(U) In addition to financial auditability, management and oversight of NIP funds is a critical challenge for the DNI. Some IC elements have not yet implemented financial management recommendations made in prior IC IG audits. According to several IC CFOs, their agencies have failed to take corrective action to remedy internal control weaknesses. Furthermore, several IC elements are accountable to another government agency (Department of Defense (DOD), Department of Justice (DOJ), and DHS) as well as to the ODNI, which leads to contradictory guidance; differing systems, policies, and procedures; and duplicative work for those agencies.

(U) In order for the business transformation, financial management, and auditability initiatives to succeed, the DNI must:

- Revise the auditability strategy with target dates for achieving auditability based on standard financial systems and ICBT initiatives, monitor progress towards auditability.
- Complete and submit to Congress the remaining financial plans and architectures that were due to SSCI in 2005.
- Lead the effort to define what constitutes a “system” for consistent IC application for both auditability and business transformation.
- Develop MOUs for IC elements that are accountable to both ODNI and another government agency to delineate financial-related roles and responsibilities.

(U) Acquisition Oversight

(U) Under IRTPA, the DNI is responsible for managing the NIP and serving as the milestone decision authority for Major Systems Acquisitions (MSAs) funded in the NIP. To fulfill this responsibility and improve IC acquisition policies and execution, the DNI re-organized the ODNI to establish a DDNI for Acquisition.⁹ The DNI also has published IC policies governing IC acquisitions and establishing the ODNI acquisition oversight process. However, the DNI continues to face significant challenges in this area.

(U) Preliminary findings from our ongoing review of acquisition oversight indicate that ODNI acquisition oversight efforts:

- Lack formal policies and processes for IC requirements validation and its role in IC acquisitions.
- Lack an IC governance model, which perpetuates internal and external impediments to efficiency.
- Suffer from instances of noncompliance, cost and schedule overruns, and poor process discipline.
- Are impeded by a perceived lack of trust, communication, and accountability in the IC acquisition community.
- Need senior ODNI leadership’s empowerment and support.

(U) The DNI must actively address these issues in order to carry out key IRTPA acquisition oversight and financial management responsibilities.

(U) In addition, audits and inspections conducted by several IC OIGs further demonstrate the need for greater acquisition oversight. IC OIGs have found that:

⁹ This division was recently renamed “Future Capabilities,” reflecting the DNI’s plan to consolidate the responsibility for the IC’s overseeing future capabilities. The directorate will execute the programming committee functions of IC-Strategic Enterprise Management (IC-SEM) – the new planning, programming and budgeting process for the IC.

- The risk of waste and abuse has increased with a surge in government spending and a growing trend toward establishing large, complex contracts to support mission requirements throughout the IC; yet many procurements receive limited oversight because they fall below the threshold for mandatory oversight.¹⁰
- IC elements need to improve the number, experience, and oversight of contracting officer's technical representatives.
- IC elements have awarded contracts without clearly defining requirements and statements of work, independent cost estimates or evaluations of contractor proposals, effective process for validating user requirements, or market research to identify feasible, alternative acquisition resources.
- Some IC elements lack strong program and procurement offices; clearly defined program requirements, performance measures, and acceptance terms; and program management systems to support the acquisition decision-making process.

(U) In sum, the IC OIGs have identified a widespread need for improved management oversight in the acquisition process and have concluded that several IC elements do not have adequate acquisition management and execution controls in place.

(U) To achieve effective acquisition oversight, we recommend that the DNI:

- Build on recent successes and positive trends by expanding policies and processes to address critical acquisition oversight functions.
- Codify and normalize an IC governance model to mitigate internal and external constraints to efficiency.
- Reverse negative trends in compliance and cost and schedule overruns by enforcing process discipline.
- Foster trust through accountability in the IC acquisition community.

5. (U) Resolving Major Legal Issues

(U) Legal issues and confusion about what the law actually requires can pose some of the greatest impediments to the IC's national security mission. While the ODNI has made progress with respect to addressing legal issues that impede the IC (Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008 and revised EO 12333), it must increase its efforts in this area.

(U) It is significant that the WMD Commission addressed legal issues at some length. We quote from the WMD Commission Report in order to drive home the need

¹⁰ Systems are "Major Systems" if the total expenditures for research, development, test and evaluation for the system are estimated to be more than \$640 million if developed by DOD agencies or \$160 million if developed by non-DOD agencies (based on FY 2006 dollars). However, the OIG has identified instances where these thresholds have not been strictly applied by the ODNI when determining whether systems are "Major Systems."

for the DNI to consolidate these matters in the hands of the DNI's legal team and to move them forward without further delay.

Throughout our work we came across Intelligence Community leaders, operators, and analysts who claimed that they couldn't do their jobs because of a "legal issue." These "legal issues" arose in a variety of contexts, ranging from the Intelligence Community's dealings with U.S. persons to the legality of certain covert actions. And although there are, of course, very real (and necessary) legal restrictions on the Intelligence Community, quite often the cited legal impediments ended up being either myths that overcautious lawyers had never debunked or policy choices swathed in pseudo-legal justifications. Needless to say such confusion about what the law actually requires can seriously hinder the Intelligence Community's ability to be proactive and innovative. . . .

The recent creation of a DNI General Counsel's office will increase the probability that community legal issues are addressed more seriously. But the existence of the office alone does not guarantee an ongoing and systematic examination of the rules and regulations that govern the Intelligence Community. We therefore recommend that the DNI General Counsel establish an internal office consisting of a small group of lawyers expressly charged with taking a forward-leaning look at legal issues that affect the Intelligence Community as a whole. By creating such an office, the DNI will help ensure that the Intelligence Community is fully able to confront the many real – and imaginary – legal issues that will arise.¹¹

(U) U.S. Persons

(U) The WMD Commission also recommended specifically that the DNI review "U.S. persons" rules and procedures across the IC because:

- The legal, policy, and cultural rules governing collection and retention of information on "U.S. persons" often act as a barrier to information sharing in the IC.
- U.S. persons rules are complicated, differ substantially between agencies, and pose significant impediments to analysts accessing intelligence possessed by other agencies.

(U) Working with the Department of Justice (DOJ) and attorneys from throughout the IC, the ODNI established a Working Group in 2005 with the task of crafting clear, consistent, and effective U.S. persons rules across the IC. However, more than three years after the issuance of the WMD Commission's recommendations, the Working Group has still not finalized or issued any common U.S. persons rules, principles, or presumptions.¹²

¹¹ WMD Commission, *Report to the President of the United States*, p. 383.

¹² ICD 102 addresses the subject but simply authorizes the Working Group to establish common principles and does not promulgate any common principles.

(U) At the request of the Working Group, the ODNI OIG's surveyed the interpretation and application of U.S. persons rules throughout the IC in March 2006. Some of the issues identified in the OIG's report included:

- Limited ability to conduct analysis of U.S. persons information.
- Inability to retain and search U.S. persons information.
- Difficulty obtaining unmasked U.S. persons information.
- Insufficient training on the handling of U.S. persons information.
- Varying interpretations of U.S. persons rules.

(U) We urge the DNI to move forward to:

- Expedite the finalization and issuance of common U.S. persons rules, principles, or presumptions.

(U) FISA

(U) Over the past 2 years, the ODNI has made substantial efforts to improve the FISA process and to strengthen the FBI's national intelligence authorities. However, in a recent review of issues affecting the FBI's intelligence efforts, we encountered a widespread belief that the FISA *process* and non-FISA areas of the FBI's national security program still need improvement. Despite legislative, policy, and restructuring accomplishments, FBI field agents and other IC officials told us that they see little improvement in their ability to conduct intelligence activities.

(U) Several of the FISA-related issues identified by interviewees during our review were identical to those identified by the DNI-created FISA Panel during its FISA Enterprise Review.¹³ Our review reinforces those findings and lends urgency to the timely implementation of the FISA Panel's recommendations. The tasks, which were largely not addressed by the FISA Amendments Act, include:

- Improving the timeliness of the FISA process.
- Improving the quality of FISA requests.
- Enhancing training on FISA and national security issues.
- Determining how to handle information gathered in national security investigations on U.S. persons that lack predication.
- Resolving issues regarding the inclusion of FISA-derived identifiers in the National Crime Information Center.
- Evaluating the FBI's non-FISA resources for national security investigations.

¹³ The DNI created the FISA Panel in July 2006 to examine issues related to the FISA process and to make recommendations for improvement. The FISA Panel conducted a FISA Enterprise Review and recommended that the DNI and AG form a "FISA Working Group" to implement the Panel's recommendations. In 2007, the DNI and Attorney General directed implementation of all of the recommendations from the Panel, including establishment of the FISA Working Group.

(U) The DNI should move quickly to:

- Ensure prompt implementation of the recommendations of the FISA Panel.

(U) Role of the DOJ

(U) The DOJ, although not a member of the IC, has and will continue to have a major impact on how intelligence activities are carried out in the United States. For example, the DOJ must approve ODNI guidelines implementing EO 12333 within the ODNI. These guidelines are essential for setting forth clear, comprehensive U.S. persons rules and other critical legal guidance for the ODNI. The ODNI Office of General Counsel (OGC) made significant progress in developing these guidelines in late 2007, but the finalization and implementation of the guidelines was postponed until after EO 12333 was amended. Now that those amendments have taken effect, OGC is working with Civil Liberties and Privacy Office and the DOJ to implement these, in the context of other IC element guidelines the DOJ is receiving. Other agencies also are working with the DOJ to issue EO 12333 guidelines. Implementation of these guidelines is overdue, and the DNI must work with the DOJ to finalize these guidelines as quickly as possible.

(U) The DNI should work closely with the DOJ to ensure that the criminal and prosecutorial responsibilities and policies of the DOJ take into account U.S. national security considerations. In addition, the DNI should team with DOJ to develop more effective approaches to stopping the proliferation of unauthorized disclosures of classified information. Some of these unauthorized disclosures have been extremely harmful to conducting intelligence operations and protecting sources and methods. We believe that it is essential that the DNI, on behalf of the IC, engage regularly with the Attorney General and relevant elements of the DOJ to address these and other national security and intelligence matters.

(U) We recommend that the DNI take the following actions:

- Engage the DOJ at its highest levels in order to communicate national intelligence interests to the DOJ and to implement appropriate legal and policy changes throughout the IC.
- Focus efforts on finalizing the ODNI's guidelines implementing EO 12333.

(U) Oversight Role

(U) Finally, IRTPA specifies that the DNI shall “ensure compliance with the constitution and laws of the United States by the Central Intelligence Agency and shall ensure such compliance by other elements of the intelligence community through the host executive departments that manage the programs and activities that are part of the National Intelligence Program.” (IRTPA, section 102A(f)(4)). In addition, the FISA Amendments

Act of 2008 imposes requirements on the DNI and the Attorney General to certify compliance with specific provisions in that statute.

(U) Ensuring that the IC is complying with the laws relating to intelligence activities is a significant challenge for the DNI. In addition to the DNI and the DOJ, the President's Intelligence Oversight Board (IOB), which is part of the President's Intelligence Advisory Board, has the responsibility to monitor and report on compliance and non-compliance with applicable intelligence laws and directives.¹⁴ The DNI, through the reporting offices of the ODNI OIG and ODNI OGC, assists the IOB in performing its oversight role. The DNI is now playing a key role in intelligence oversight and should continue to work closely with the IOB and the DOJ in monitoring compliance with laws relating to intelligence.

(U) Conclusion

(U) The DNI should act promptly to address the management challenges described above. Such action is necessary for the DNI to succeed in the overriding responsibility to effectively lead and manage the IC and the ODNI.

¹⁴ See EO 13462.