# Inspector General

## United States
## Department of Defense

**Additional Information and Copies**

To request copies of this report, contact Mr. James Graham (703) 604-8841 (DSN 664-8841).

**Suggestions for Future Audits and Evaluations**

To suggest ideas for, or to request future audits and evaluations of Defense intelligence issues, contact the Office of the Deputy Inspector General for Intelligence at (703) 604-8800 (DSN 664-8800) or fax (703) 604-0045. Ideas and requests can also be mailed to:

Office of the Deputy Inspector General for Intelligence
ODIG-INTEL (ATTN: Audit/Evaluation Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 703)
Arlington, VA 22202-4704

DEPARTMENT OF DEFENSE
hotline

**To report fraud, waste, mismanagement, and abuse of authority.**

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900
Phone: 800.424.9098 e-mail: hotline@dodig.mil www.dodig.mil/hotline

## Acronyms

| | |
|---|---|
| ATSD(IO) | Assistant to the Secretary of Defense for Intelligence Oversight |
| CI | Counterintelligence |
| CIFA | Counterintelligence Field Activity |
| DCIIS | Defense Counterintelligence Information System |
| DIA | Defense Intelligence Agency |
| DIMA | Defense Intelligence Mission Area |
| TALON | Threat and Local Observation Notice |
| USD(I) | Under Secretary of Defense for Intelligence |

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

May 11, 2009

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
ASSISTANT TO THE SECRETARY OF DEFENSE
FOR INTELLIGENCE OVERSIGHT

SUBJECT: Report on Audit of Information Technology Portfolio for DoD Intelligence Databases (Report No. 09-INTEL-07)

We are providing this report for review and comment.

Comments from the Under Secretary of Defense for Intelligence were not received on the December 10, 2008, draft of this report. We request that management provide comments that conform to the requirements of DoD Directive 7650.3. Please provide comments by June 8, 2009.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to Averel.Gregg@dodig.mil or iggreae@dodig.ic.gov. Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, they must be sent over the Joint Worldwide Intelligence Communications System (JWICS).

Management comments should indicate concurrence or nonconcurrence with each applicable finding and recommendation. Comments should describe actions taken or planned in response to agreed-upon recommendations and provide the completion dates of the actions. State specific reasons for any nonconcurrence and propose alternative actions, if appropriate.

We appreciate the courtesies extended to the staff. Questions should be directed to Mr. Sean Mitchell at (703) 604-8815 (DSN 664-8815) or Mr. Averel E. Gregg at (703) 604-8965 (DSN 664-8965).

Patricia A. Brannin

Patricia A. Brannin
Deputy Inspector General
for Intelligence

Department of Defense Office of Inspector General

**Report No. 09-Intel-07** **May 11, 2009**
(Project No. D2008-DINT02-0055)

# Audit of Information Technology Portfolio for DoD Intelligence Databases

## Executive Summary

**Who Should Read This Report and Why?** All DoD officials and intelligence and counterintelligence personnel who manage DoD databases should read this report.

**Background.** This report discusses DoD criteria and compliance with internal controls related to portfolio management for intelligence databases.

During the briefing of DoD Inspector General Report No. 07-INTEL-09, "The Threat and Local Observation Notice Report Program," June 27, 2007, the House Permanent Select Committee on Intelligence suggested that the DoD Inspector General audit additional intelligence databases.

**Results.** Office of the Under Secretary of Defense for Intelligence officials had not fully established the control mechanisms to effectively manage and oversee DoD databases for intelligence components in accordance with DoD regulations. Office of the Under Secretary of Defense for Intelligence officials had not established an intelligence technology portfolio; therefore, they did not have visibility into issues such as duplication of systems, facilities, and services; and system interoperability. As a result, officials were unaware of the quantity and capabilities of intelligence databases maintained by agencies within the intelligence community responsible for data collection and dissemination. Under Secretary of Defense for Intelligence officials did not have:

- the capability to guarantee that the information collected, stored, and disseminated by subordinate agencies were maintained in accordance with applicable intelligence laws and DoD regulations;
- the information needed to identify gaps and opportunities for technology insertions to enhance intelligence, counterintelligence, and security responsibilities**;** and
- all the information needed to provide advice concerning acquisition programs that significantly affected the Defense intelligence community.

Recommendation 2 in the December 10, 2008, draft report was deleted because the Office of the Under Secretary of Defense for Intelligence removed the Defense Intelligence Mission Area Portfolio Management Office from the Defense Intelligence Agency and incorporated that function into their Deputy Under Secretaries of Defense for Portfolio, Programs, and Resources office.

**Recommendations.** We recommend that the Under Secretary of Defense for Intelligence:

- develop an intelligence information technology portfolio,

- assess all systems in the information technology portfolio to enhance the management of those systems.

**Client Comments.** Under Secretary of Defense for Intelligence did not provide comments to the draft of this report issued December 10, 2008.

**Our Response.** We request that the Under Secretary of Defense for Intelligence comment on this report by June 8, 2009.

# Table of Contents

**Executive Summary** i

**Background** 1

**Objectives** 3

**Finding**

USD(I) Intelligence Database Oversight 4

**Appendixes**

A. Scope and Methodology 10
B. Mitre report 12

# Background

This report discusses DoD criteria and compliance with internal controls related to information technology portfolio management for Intelligence Community databases.

During the briefing of DoD Office of the Inspector General, (Report No. 07-INTEL-09), "The Threat and Local Observation Notice (TALON) Report Program," June 27, 2007, the House Permanent Select Committee on Intelligence suggested that the DoD Inspector General audit additional intelligence databases. The DoD Inspector General conducted the TALON audit in response to a congressional request on media reports that DoD developed and maintained a database for information on U.S. persons conducting domestic anti-war and counter military protests and demonstrations. The audit found that the Counterintelligence Field Activity (CIFA) and the U.S. Northern Command had legally gathered and maintained TALON data for law enforcement and force protection purposes; however, they did not comply with the information retention criteria specified in DoD directives. The Deputy Secretary of Defense directed the termination of the TALON reporting system effective September 17, 2007.

**DoD Criteria**. DoD Regulation, 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect U.S. Persons," dated December 1982, established procedures for collecting, retaining, and disseminating information on U.S. persons. Specifically, DoD Regulation 5240.1-R defines collected information as follows:

> Information shall be considered as "collected" only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties. Thus, information volunteered to a DoD intelligence component by a cooperating source would be "collected" under this procedure when an employee of such component officially accepts, in some manner, such information for use within that component. Data acquired by electronic means is "collected" only when it has been processed into intelligible form.

DoD Directive 8115.02, "Information Technology Portfolio Management Implementation," dated October 30, 2006, establishes policy and assigns responsibilities for the management of DoD information technology investments as portfolios that focus on improving DoD capabilities and mission outcomes.

DoD Directive 5148.11, "Assistant to the Secretary of Defense for Intelligence Oversight (ATSD[IO])," May 21, 2004, updates the responsibilities, functions, relationships, and authorities of the Assistant to the Secretary of Defense for Intelligence Oversight:

> In the exercise of assigned responsibilities, the ATSD(IO) shall develop intelligence oversight policy and, in coordination with the General Counsel of the Department of Defense, issue intelligence oversight guidance to the DoD Components, including regulatory guidance

implementing intelligence oversight aspects of Executive Order (E.O.) 12333 United States Intelligence Activities, dated December 4, 1981.

DoD Manual 8115.01, "Information Technology Portfolio Management," October 30, 2006, requires information technology investments be managed as portfolios to ensure investments support the Department's vision, mission, and goals; ensure efficient and effective delivery of capabilities to the warfighter; and maximize return on investment to the enterprise. Each portfolio shall be managed using the Global Infrastructure Grid, plans, risk management techniques, capability goals and objectives, and performance measures. Portfolios shall be nested and integrated at the Enterprise, Mission, and Component levels. The Enterprise portfolio shall be divided into Mission Area portfolios, which includes the DoD portion of intelligence. Portfolios shall be used as a management tool in each of the Department's decision support systems including: the Joint Capabilities Integration and Development System; the Planning, Programming, Budgeting, and Execution System; and the Defense Acquisition System. The Under Secretary of Defense for Intelligence (USD[I]) is the Mission Area lead for the DoD portion of the Intelligence Portfolio. The USD(I) shall establish the Defense Intelligence Mission Area (DIMA) portfolio and issue guidance for managing the DIMA portfolio and designate responsibilities for DIMA portfolio management.

## Definitions

**Data Repository.** A specialized database containing information about data, such as meaning, relationships to other data, origin, usage, and format, including the information resources needed by an organization. (DoD 8320.1-M)

**Database.** A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; the data are stored so that other programs without concern for the data structure or organization can use them. A common approach is used to add new data, and modify and retrieve existing data. (DoD 8320.1-M-1)

**Information Technology.** The term with respect to an executive agency means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, and reception of data or information. The term "information technology" includes computers, ancillary equipment, software, firmware, and any similar procedures, services, and related resources. (Chairman of the Joint Chief of Staff Instruction 8410.01)

**Information Technology Portfolio.** A grouping of information technology investments by capability to accomplish a specific functional goal, objective, or mission outcome. (DoDD 8115.01)

**Information Technology Portfolio Management.** The management of selected groupings of information technology investments using strategic planning, architectures, and outcome-based scoring criteria to achieve mission capability. (Chairman of the Joint Chief of Staff Instruction 8410.01)

**Portfolio.** The collection of capabilities, resources and related investments that are required to accomplish a mission-related or administrative outcome. A portfolio includes outcomes, performance measures (mission, functional, or administrative measures), and an expected return on investment. Resources include people, money, facilities, weapons, information technology, other equipment, logistics support, services, and information. Management activities for the portfolio include strategic planning, capital planning, governance, process improvements, performance metrics/measures, requirements generation, acquisition/development, and operations (DoD 8115.02).

**Schema.** A definition of data structure. (FIPS 184)

**Internal Schema.** A schema of the American National Standards Institute's Standard Planning and Requirements Committee's Three Schema Architecture, in which views of information are represented in a form specific to the database management system used to store the information; a description of the physical structure of data. (FIPS 184)

## Objective

Our overall audit objective was to determine the extent that DoD intelligence and counterintelligence (CI) components maintain databases that contain U.S. person information. This report discusses control mechanisms for effective management and oversight. See Appendix A for a discussion of the scope and methodology, and prior audit coverage related to the objectives.

# USD(I) Intelligence Database Oversight

OUSD(I) officials had not fully established the control mechanisms to effectively manage and oversee DoD databases for intelligence components in accordance with DoD regulations. OUSD(I) officials had not established an intelligence technology portfolio; therefore, they did not have visibility into issues such as duplication of systems, facilities, and services; and system interoperability. As a result, OUSD(I) officials were unaware of the quantity and capabilities of intelligence databases maintained by agencies within the intelligence community responsible for data collection and dissemination. In addition, OUSD(I) officials did not have:

- the capability to guarantee that the information collected, stored, and disseminated by subordinate agencies were maintained in accordance with applicable intelligence laws and DoD regulations;
- the information needed to identify gaps and opportunities for technology insertions to enhance intelligence, counterintelligence, and security responsibilities**;** and
- all the information needed to provide advice concerning acquisition programs that significantly affected the Defense intelligence community.

## USD(I) Program Oversight and Responsibilities

On April 18, 2003, the Secretary of Defense established the office of the Under Secretary of Defense for Intelligence. The primary functions of the USD(I) are to act as the principal assistant to the Secretary of Defense regarding intelligence; exercise the authority, direction, and control over intelligence and intelligence-related activities within the DoD; and serve as the single point of contact within the DoD for other government agencies on intelligence matters.

**USD(I) Program Oversight.** DoD Directive 5143.01, "Under Secretary of Defense for Intelligence," November 23, 2005, states that the USD(I) exercises the Secretary of Defense's authority, direction, and control over the Defense Agencies and DoD Field Activities that are Defense intelligence, CI, or security components[1] and exercises planning, policy, and strategic oversight over all DoD intelligence, CI, and security policy, plans, and programs. In the performance of this policy, the USD(I) shall:

- oversee DoD Intelligence Community policy, plans, programs, required capabilities, and resource allocations, which includes exercising responsibilities for DoD Components within the National Intelligence Program and the Military Intelligence Program;

[1] DoD Directive 5143.01 states that the Under Secretary of Defense for Intelligence shall exercise the Secretary of Defense's authority, direct, direction, and control over the Defense Security Service, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Security Agency/Central Security Service, and the National Reconnaissance Office and other positions and organizations as may be established by the USD(I).

- develop and oversee DoD policy regarding the sharing of information consistent with applicable laws, regulations, and policies;
- serve as the focal point for all policy and oversight matters relating to intelligence information sharing and interoperability of Defense intelligence systems and processes;
- use existing systems, facilities, and services of DoD and other Federal Agencies to avoid duplication and to achieve maximum readiness, sustainability, economy, and efficiency; and
- identify gaps and opportunities for technology insertion to enhance intelligence, CI, and security capabilities.

DoD Directive 5143.01 states that for planning, programming, budgeting, and execution matters, USD(I) shall support the Assistant Secretary of Defense for Legislative Affairs and the Under Secretary of Defense (Comptroller) in presenting, justifying, and defending intelligence, CI, and security programs and budgets before the Congress as well as evaluating and assessing Congressional activity for impact on all assigned areas of responsibility. That Directive further states that, for acquisition matters, the USD(I) shall provide advice and assistance to officials and entities within the U.S. Government concerning acquisition programs that significantly affect Defense intelligence, CI, and security components as well as intelligence, CI, and security programs.

**USD(I) Program Responsibilities.** DoD Directive 8115.01, "Information Technology Portfolio Management," October 10, 2005, states that the USD(I) shall serve as the mission area lead for the DoD portion of the intelligence portfolio.[2] The Directive tasked USD(I) with establishing the DIMA Portfolio as well as issuing guidance and designating responsibilities for managing the DIMA portfolio. DoD Instruction 8115.02, "Information Technology Portfolio Management Implementation," October 30, 2006, states that USD(I) has delegated responsibility for managing the DIMA portfolio to the Director, Defense Intelligence Agency (DIA), but USD(I) retains final signature authority. DIA established the DIMA Portfolio Management Office to manage the DIMA portfolio.

## List of DoD Intelligence Databases

OUSD(I) did not have a list of DoD intelligence databases; therefore, OUSD(I) officials were unaware of the quantity and content of the large repository/library type of intelligence databases that contain source information maintained by DoD intelligence components. On November 13, 2007, the USD(I) issued a memorandum to the DoD intelligence components requesting that they provide a point of contact by November 26, 2007. Each point of contact was responsible for assembling a list and description of the database(s) that contain U.S. person

[2] According to DoDD 8115.01, an Information Technology Portfolio is a grouping of information technology investments by capability to accomplish a specific functional goal, objective, or mission outcome. DoDD 8115.01 does not provide an official definition for the phrase "Intelligence Portfolio;" however, the specific functional goal described in this section relates to the collection of intelligence data required for an Information Technology Portfolio.

information maintained for intelligence, CI, law enforcement, or force protection purposes; and identifying the organization that maintained each database. As of October 22, 2008, OUSD(I) personnel had not located any responses to the November 13, 2007, memorandum.

OUSD(I) officials and officials within the Intelligence Agencies requested clarification on how the DoD IG defined the word “database.” On January 8, 2008, DoD IG made a distinction for this audit between the large repository/library type databases and the databases created by analysts from querying the large repository/library type database pertaining to a specific threat category or topic. We view the databases created by analysts pertaining to a specific threat category or topic as their “work projects.”

The DIA’s DIMA Portfolio Management Office was requested to provide a list of existing DoD intelligence databases, a description of each database, the name of the organization responsible for maintaining the database, and a database point of contact maintained for intelligence, CI, law enforcement, or force protection purposes. On December 20, 2007, the DIA’s DIMA Portfolio Management Office officials stated that a list of the universe of DoD intelligence and CI databases containing U.S. person information was unavailable because the organization had only been in existence since October 2006 and they had not received a listing from OUSD(I). DoD Directive 5143.01 states that the USD(I) shall provide support for presentations, justifications, and the defense of intelligence budgets before Congress. Therefore, the DIA’s DIMA Portfolio Management Office personnel did not have the information needed to fulfill their mission of managing the intelligence information technology portfolio.

## Management and Oversight

OUSD(I) officials had not fully established the control mechanisms to effectively manage and oversee DoD databases for intelligence components in accordance with DoD regulations. Although DoD Directive 8115.01, October 10, 2005, required the USD(I) to establish an intelligence information technology portfolio and provide that portfolio to the DIA’s DIMA Portfolio Management Office, OUSD(I) officials did not establish an intelligence information technology portfolio to enhance intelligence, CI, and security responsibilities. Therefore, OUSD(I) officials did not have visibility into issues such as duplication of systems, services, and facilities; system interoperability; and opportunities for technology insertion. The development and effective management of a joint intelligence operating system begins with the knowledge of available intelligence databases owned and maintained by each member of the intelligence community followed by an understanding of each database’s capabilities.

Maintaining a directory of databases allows intelligence administrators to make informed decisions regarding database acquisition and database consolidation where applicable. Because USD(I) did not have a directory of databases, they) could not:

- guarantee that the information collected, stored, and disseminated by subordinate agencies were maintained in accordance with applicable intelligence laws and DoD regulations;

- identify gaps and opportunities for technology insertions to enhance intelligence, CI, and security responsibilities; and

- provide fully informed advice concerning acquisition programs that significantly affect the Defense intelligence community.

There were no indications that the OUSD(I) ever considered identifying the universe of primary databases/repositories maintained by the intelligence community. The creation of an intelligence information technology portfolio that includes database/repositories for each intelligence component is necessary when considering intelligence community management and oversight, agency interoperability, and financial intelligence community resource spending. The OUSD(I) could also use the information technology portfolio to conduct a review of intelligence systems similar to the one completed by CIFA.

## Information Systems Assessment

A complete information technology portfolio of the DoD Intelligence Community's intelligence systems and an assessment of those systems would provide the OUSD(I) with the information needed to:

- improve management and oversight of the Defense intelligence community, and
- provide fully informed decisions on budgeting, systems acquisitions, systems interoperability, systems duplication, and systems data standards.

A review would help OUSD(I) identify gaps and opportunities for technology insertions to enhance intelligence, CI, and security responsibilities. A review would also help OUSD(I) develop data standards; a shared data architecture, multi-tiered intelligence data architecture; and standards for a federated application architecture framework to facilitate and foster the future sharing of applications within the intelligence community. CIFA used such an assessment to improve the management of the CI Community information technology portfolio.

On June 22, 2007, the MITRE Corporation (MITRE) issued a report in response to a contract from the Director, CIFA, to complete two tasks:

- assess and review DoD systems providing automated support to the CI community, and

- recommend a way ahead for the Defense Counterintelligence Information System (DCIIS) program, specifically for the multitude of automation systems currently in use to support the CI processes.

The MITRE review identified three issues within the CI community:

- a lack of standardization, not only at the information level, but also in data and information exchange formats;

- insufficient interoperability and access because of disjointed CI data across the community; and

- duplication of effort across the CI community as CIFA, the Services, and DIA build and improve on information systems that provide overlapping functionality.

DoD Directive O-5240.02, "Counterintelligence," December 20, 2007, addressed the MITRE findings. The Directive stated that DoD Components will use USD(I)-approved CI information systems and architectures for DoD CI management and reporting. The Directive also states that the USD(I) shall "designate and approve all CI information systems and architectures to be used for DoD CI management and reporting purposes." See Appendix B for additional information on the MITRE report.

## Summary

OUSD(I) officials need to improve control mechanisms so that they have better visibility of the quantity and capabilities of intelligence databases/repositories maintained by agencies within the intelligence community responsible for data collection and dissemination. They also need to improve control mechanisms that provide the information needed to (1) determine whether duplication of systems, facilities, and services existed; (2) provide fully informed advice concerning acquisition of information technology programs and systems; and (3) identify gaps and opportunities for technology insertions to enhance intelligence, CI, and security responsibilities. OUSD(I) officials need to establish an intelligence information technology portfolio and use that portfolio to improver management of intelligence information systems..

## Recommendation, Management Comments, and Our Response

We recommend that the Under Secretary of Defense for Intelligence:

1. Develop an intelligence information technology portfolio to include a list of all systems currently used and systems in development, a description of the mission and capabilities of each system, and a point-of-contact.

2. Assess all systems in the intelligence information technology portfolio to:

- determine whether duplication of systems, facilities, and services exist;
- identify gaps and opportunities for technology insertions;
- develop data standards,
- develop a shared data architecture,
- develop a multi-tiered intelligence data architecture, and
- develop standards for a federated application architecture framework to facilitate and foster the future sharing of applications within the intelligence community.

# Appendix A. Scope and Methodology

We conducted this performance audit from October 16, 2007, through October 17, 2008, in accordance with generally accepted government auditing standards. Those standards require that we perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions.

We reviewed the management and oversight of DoD OUSD(I) provided for intelligence databases. During December 2007 through September 2008, we conducted multiple site visits to obtain a better understanding of intelligence databases. We interviewed officials within the Office of Assistant to the Secretary of Defense for Intelligence and Oversight; Joint Staff; Defense Intelligence Agency; National Security Agency; National Geospatial-Intelligence Agency; Naval Criminal Investigative Services; Office of Naval Intelligence; U.S. Army Intelligence Security Command; National Reconnaissance Office; Air Force Office of Special Investigations; and the Air Force Intelligence, Surveillance, and Reconnaissance Agency. We requested that OUSD(I) and the DIA's DIMA Portfolio Management Office provide a copy of the Intelligence Information Technology Portfolio; however, they had not developed a portfolio. We requested each member of the DoD Intelligence Community to provide a list of databases they maintained or used to store intelligence, CI, and law enforcement data.

During the audit, we applied relevant criteria, such as DoD Directive 5143.01, DoD Directive 5240.1-R, DoD Directive 5240.02, DoD Directive 5148.11, and DoD Instruction 8115.02.

**Scope Limitation.** On September 17, 2007, we issued a memorandum to the USD(I) requesting a list of intelligence databases. Because USD(I) could not provide a list, we announced the audit, on October 16, 2007, to the DoD intelligence components with the intention of developing the universe list of intelligence databases from which to select a sample. On November 13, 2007, USD(I) issued a memorandum, "Audit of Department of Defense Intelligence Database(s)," to the DoD intelligence components requiring a point of contact to be provided by November 26, 2007. The memorandum required each point of contact to be responsible for assembling a list and description of the database(s) that contain U.S. person information maintained for intelligence, counterintelligence, law enforcement, or force protection purposes; and identifying the organization that maintains each database. As of October 7, 2008, OUSD(I) still had not received a list of databases from the Intelligence Community.

The difficulties encountered in trying to generate the universe list of DoD intelligence databases from which to select the sample for the audit was not completely settled. There was confusion on what type of databases we wanted included in the request; therefore, on January 8, 2008, we made a distinction between the large repositories/library type databases that would be the source data for analysts' queries and databases created by analysts for their specific tasks. Meeting with the DoD intelligence components, specifying the large repository/library type databases, obtaining lists, and reviewing their policy and procedures pertaining to U.S. person information have been a time consuming endeavor.  For that reason, we have chosen to issue this report addressing the current management control condition.

**Use of Computer-Processed Data.**  We did not use computer-processed data to perform this audit.

## Prior Coverage

During the last 5 years, the Department of Defense Office of the Inspector General (DoD OIG) issued two report discussing DoD databases that contain U.S. person information.

### DoD OIG

DoD IG Report No. 07-INTEL-09, "The Threat and Local Observation Notice (TALON) Report Program," June 27, 2007

DoD OIG Report No. 07-INTEL-14, "Review of Access to U.S. Persons Data by the Space and Naval Warfare Systems Command," September 28, 2007

# Appendix B. MITRE Report

In June 2007, the CIFA initiated an assessment of the CI environment with the objective of cataloging and potentially consolidating CI databases. The following assessment demonstrates a successful attempt at reaching uniformity throughout the intelligence community.

On June 22, 2007, the MITRE Corporation (MITRE) issued a report in response to a request from the Director, CIFA, to complete two tasks:

- assess and review DoD systems providing automated support to the CI community, and
- recommend a way ahead for the DCIIS program, specifically for the multitude of automation systems currently in use to support the CI processes.

The goal of the DCIIS assessment was to provide an independent, objective evaluation on the capabilities of automated tools currently in use or in development for use across the CI community. The assessment also included a high-level gap analysis to highlight the capabilities that existed at the time to meet the needs of the CI community and identify shortfalls in current automated capabilities. For the DCIIS assessment, CIFA asked each CI community organization to identify current or near-current systems that are in use to support CI processes and that satisfy all or a portion of the requirements identified as evaluation factors in the review. CIFA asked MITRE to include available capabilities or capabilities projected to be available through testing by December 2007.

The MITRE assessment team reviewed 14 CI systems owned by 5 intelligence community members.[3] MITRE representatives met with representatives from each CI agency to discuss and further refine the evaluation factors and then prepared a report documenting the assessment criteria, assumptions about specific criteria, the scoring guidance, and the approach used to collect the evidence to score each system. Based on their discussions, issues within the CI community included:

- a lack of standardization, not only at the information level, but in data and information exchange formats;
- insufficient interoperability and access as a result of disjointed CI data across the community; and
- duplication of effort across the CI community as CIFA, the Services, and DIA build and improve on information systems that provide overlapping functionality.

[3] The five intelligence community member organizations included in the MITRE DCIIS assessment included the Air Force Office of Special Investigations (four CI systems), CIFA (three systems), DIA (one system), Naval Criminal Investigative Service (five systems), and United States Army (one system).

The MITRE assessment team collected information about each of the 14 systems and generated five assessment reports, one for each system or suite of systems. The assessment team then conducted a functional and a technical assessment of each system. During the functional assessment, MITRE analyzed the information contained within the five assessment reports and compared the systems based on the following categories:

- counterintelligence collections,
- counterintelligence investigations,
- offensive counterintelligence operations,
- counterintelligence analysis and production,
- counterintelligence functional services, and
- non-offensive counterintelligence operations.

The technical assessment of each system was based on the following categories:

- general system and performance requirements,
- human factors requirements,
- information technology requirements,
- DoD information technology compliance,
- operations and maintenance of the system, and
- training.

According to the MITRE assessment, although CIFA had developed and deployed its program as the intelligence community's CI information system, the Army, Navy, Air Force, and DIA had concurrently developed and deployed information systems that supported their individual CI missions and responsibilities. After considering both the functional and technical assessments of each of the 14 information systems, MITRE could not identify a definitive winner among the information systems assessed. According to their evaluation, different systems excelled in providing different user capabilities, more robust architectures, or more intuitive user interfaces. The MITRE assessment team recognized that some duplication of effort was expected due to the existence of centers of excellence in the CI community for various tools, services, or architectures. The MITRE assessment team observed that a regular process to identify and connect the information systems that supported the Defense CI community did not exist.

MITRE's recommendations focused on system standardization (developing standards across the CI community); promoting a shared data architecture (improving CI data access across the CI community, security domains, and the DoD); and creating a federated application architecture (one that would improve ease of use, improve system functionality, and develop future capabilities, i.e., technology and tool enhancement). The MITRE presentation contained the following conclusions:

- a community of semi-autonomous, dynamic CI entities will persist;
- CIFA should not attempt to build and operate a central CI information system that all CI users are expected to use exclusively to perform their mission; and

- facilitate and foster the future sharing of applications within the CI community, CIFA should focus on developing data standards, a shared, multi-tiered CI data architecture, and standards for a federated application architecture framework.

On December 20, 2007, DoD Directive O-5240.02, “Counterintelligence,” stated that DoD Components will use USD(I)-approved CI information systems and architectures for DoD CI management and reporting. In addition, the USD(I) shall, “designate and approve all CI information systems and architectures to be used for DoD CI management and reporting purposes.” The directive also states that the Director, CIFA, shall, “develop, manage, and maintain the DoD CI management and reporting information systems and architectures;” as well as, “exercising CI mission tasking authority to ensure the effective integration and synchronization of the DoD CI community.” On January 31, 2008, USD(I) issued a memorandum stating that in accordance with DoD Directive O-5240.02, Portico (the CIFA/Defense Intelligence Agency CI information system) will be the DoD information system for all CI reporting within the DoD no later than June 1, 2008.

Inspector General
Department of Defense