

September 2011

# DATA MINING

## DHS Needs to Improve Executive Oversight of Systems Supporting Counterterrorism

U.S. Government Accountability Office

GAO 90

YEARS

1921-2011

ACCOUNTABILITY ★ INTEGRITY ★ RELIABILITY

## Why GAO Did This Study

Data mining—a technique for extracting useful information from large volumes of data—is one type of analysis that the Department of Homeland Security (DHS) uses to help detect and prevent terrorist threats. While data-mining systems offer a number of promising benefits, their use also raises privacy concerns.

GAO was asked to (1) assess DHS policies for evaluating the effectiveness and privacy protections of data-mining systems used for counterterrorism, (2) assess DHS agencies' efforts to evaluate the effectiveness and privacy protections of their data-mining systems, and (3) describe the challenges facing DHS in implementing an effective evaluation framework.

To do so, GAO developed a systematic evaluation framework based on recommendations and best practices outlined by the National Research Council, industry practices, and prior GAO reports. GAO compared its evaluation framework to DHS's and three component agencies' policies and to six systems' practices, and interviewed agency officials about gaps in their evaluations and challenges.

## What GAO Recommends

GAO is recommending that DHS executives address gaps in agency evaluation policies and that component agency officials address shortfalls in their system evaluations. DHS concurred with GAO's recommendations and identified steps it is taking to address selected recommendations. The department also offered technical comments, which GAO incorporated as appropriate.

View [GAO-11-742](#) or key components. For more information, contact Dave Powner at (202) 512-9286 or [pownerd@gao.gov](mailto:pownerd@gao.gov).

## DATA MINING

### DHS Needs to Improve Executive Oversight of Systems Supporting Counterterrorism

## What GAO Found

As part of a systematic evaluation framework, agency policies should ensure organizational competence, evaluations of a system's effectiveness and privacy protections, executive review, and appropriate transparency throughout the system's life cycle. While DHS and three of its component agencies—U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and the U.S. Citizenship and Immigration Services—have established policies that address most of these key policy elements, the policies are not comprehensive. For example, DHS policies do not fully ensure executive review and transparency, and the component agencies' policies do not sufficiently require evaluating system effectiveness. DHS's Chief Information Officer reported that the agency is planning to improve its executive review process by conducting more intensive reviews of IT investments, including the data-mining systems reviewed in this report. Until such reforms are in place, DHS and its component agencies may not be able to ensure that critical data mining systems used in support of counterterrorism are both effective and that they protect personal privacy.

Another aspect of a systematic evaluation framework involves ensuring that agencies implement sound practices for organizational competence, evaluations of a system's effectiveness and privacy protections, executive review, and appropriate transparency and oversight throughout a system's life cycle. Evaluations of six data mining systems from a mix of DHS component agencies showed that all six program offices took steps to evaluate their system's effectiveness and privacy protections. However, none performed all of the key activities associated with an effective evaluation framework. For example, four of the program offices executed most of the activities for evaluating program privacy impacts, but only one program office performed most of the activities related to obtaining executive review and approval. By not consistently performing necessary evaluations and reviews of these systems, DHS and its component agencies risk developing and acquiring systems that do not effectively support their agencies' missions and do not adequately ensure the protection of privacy-related information.

DHS faces key challenges in implementing a framework to ensure systems are effective and provide privacy protections. These include reviewing and overseeing systems once they are in operation, stabilizing and implementing acquisition policies throughout the department, and ensuring that privacy-sensitive systems have timely and up-to-date privacy reviews. The shortfalls GAO noted in agency policies and practices provide insight into these challenges. Until DHS addresses these challenges, it will be limited in its ability to ensure that its systems have been adequately reviewed, are operating as intended, and are appropriately protecting individual privacy and assuring transparency to the public.

---

# Contents

---

Letter		1
	Background	2
	Agency Policies Address Most Elements of a Systematic Framework for Evaluating Effectiveness and Privacy, but Are Not Comprehensive	15
	Program Offices Are Evaluating System Effectiveness and Privacy Protections, but Have Not Consistently Implemented Key Activities	21
	DHS Faces Challenges in Implementing a Framework to Ensure System Effectiveness and Privacy Protections	28
	Conclusions	32
	Recommendations for Executive Action	32
	Agency Comments and Our Evaluation	33
Appendix I	Objectives, Scope, and Methodology	37
Appendix II	Fair Information Practices	40
Appendix III	Detailed Assessment of DHS and Selected Agencies' Policies	42
Appendix IV	Detailed Assessments of Selected Data-Mining Systems	44
Appendix V	Comments from the Department of Homeland Security	61
Appendix VI	GAO Contact and Staff Acknowledgments	69
Tables		
	Table 1: DHS Component Agencies	4
	Table 2: Selected DHS Data-Mining Systems	7

---

Table 3: Overview of a Systematic Framework for Evaluating Agency Policies and Practices for System Effectiveness and Privacy Impacts	13
Table 4: Key Elements of an Effective Policy for Evaluating System Effectiveness and Privacy Impacts	16
Table 5: Assessment of DHS and Selected Component Agencies' Policies	17
Table 6: Key Elements and Activities for Evaluating System Effectiveness and Privacy Protections	21
Table 7: Assessment of System Practices	23
Table 8: Status of Privacy Impact Assessments	31
Table 9: Fair Information Practices	41
Table 10: Detailed Assessment of DHS and Selected Agencies' Policies	42
Table 11: Detailed Assessment of AFI	45
Table 12: Detailed Assessment of ATS-P	48
Table 13: Detailed Assessment of CIDR	50
Table 14: Detailed Assessment of DARTTS	53
Table 15: Detailed Assessment of ICEPIC	55
Table 16: Detailed Assessment of CBP's TECS-Mod	58

---

Figure

Figure 1: DHS Organizational Structure	3
--	---

---

---

## Abbreviations

AFI	Analytical Framework for Intelligence
ATS	Automated Targeting System
ATS-P	ATS-Passenger module
CBP	Customs and Border Protection
CIDR	Citizen and Immigration Data Repository
CIO	Chief Information Officer
DARTTS	Data Analysis and Research for Trade Transparency System
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act of 2002
ICE	Immigration and Customs Enforcement
ICEPIC	ICE Pattern Analysis and Information Collection
NRC	National Research Council
OECD	Organization for Economic Cooperation and Development
OMB	Office of Management and Budget
PIA	privacy impact assessment
TECS-Mod	TECS Modernization
USCIS	U.S. Citizenship and Immigration Services

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



**G A O**

Accountability \* Integrity \* Reliability

**United States Government Accountability Office**  
Washington, DC 20548

---

September 7, 2011

The Honorable Donna F. Edwards  
Ranking Member  
Subcommittee on Investigations and Oversight  
Committee on Science, Space, and Technology  
House of Representatives

The Honorable Brad Miller  
Ranking Member  
Subcommittee on Energy and Environment  
Committee on Science, Space, and Technology  
House of Representatives

Established in the aftermath of the terrorist attacks that took place on September 11, 2001, the Department of Homeland Security (DHS) is, among other things, responsible for preventing terrorist attacks within the United States, reducing the nation's vulnerability to terrorism, minimizing damages from attacks that occur, and helping the nation recover from such attacks. Since its formation, DHS has increasingly focused on the prevention and detection of terrorist threats through technological means. Data mining—a technique for extracting useful information from large volumes of data—is one type of analysis that DHS uses to help detect terrorist threats. While data mining offers a number of promising benefits, its use also raises privacy concerns when the data being mined include personal information.

Given the challenge of balancing DHS's counterterrorism mission with the need to protect individuals' personal information, you requested that we evaluate DHS policies and practices for ensuring that its data-mining systems are both effective and that they protect personal privacy. Our objectives were to (1) assess DHS policies for evaluating the effectiveness and privacy protections of data-mining systems used for counterterrorism, (2) assess DHS agencies' efforts to evaluate the effectiveness and privacy protections of their counterterrorism-related data-mining systems throughout the systems' life cycles, and (3) describe the challenges facing DHS in implementing an effective framework for evaluating its counterterrorism-related data-mining systems.

To address our objectives, we developed an assessment framework based on recommendations and best practices outlined by the National Research Council, industry practices, and prior GAO reports. We

---

compared DHS policies for evaluating the effectiveness and privacy protections of its data-mining systems to this framework and identified gaps. We also selected a nonrandom sample of six systems that perform data mining in support of counterterrorism, seeking systems from a mix of component agencies and in different life-cycle stages. We compared the practices used to evaluate these systems to the assessment framework and identified gaps. Because we reviewed a nonrandom sample of systems, our results cannot be generalized to the agency as a whole or to other agency systems that we did not review. We identified the causes of any gaps in DHS's policies and practices to determine challenges the department faces in implementing an effective framework for evaluating its data-mining systems. We also interviewed agency and program officials on their policies, practices, and challenges.

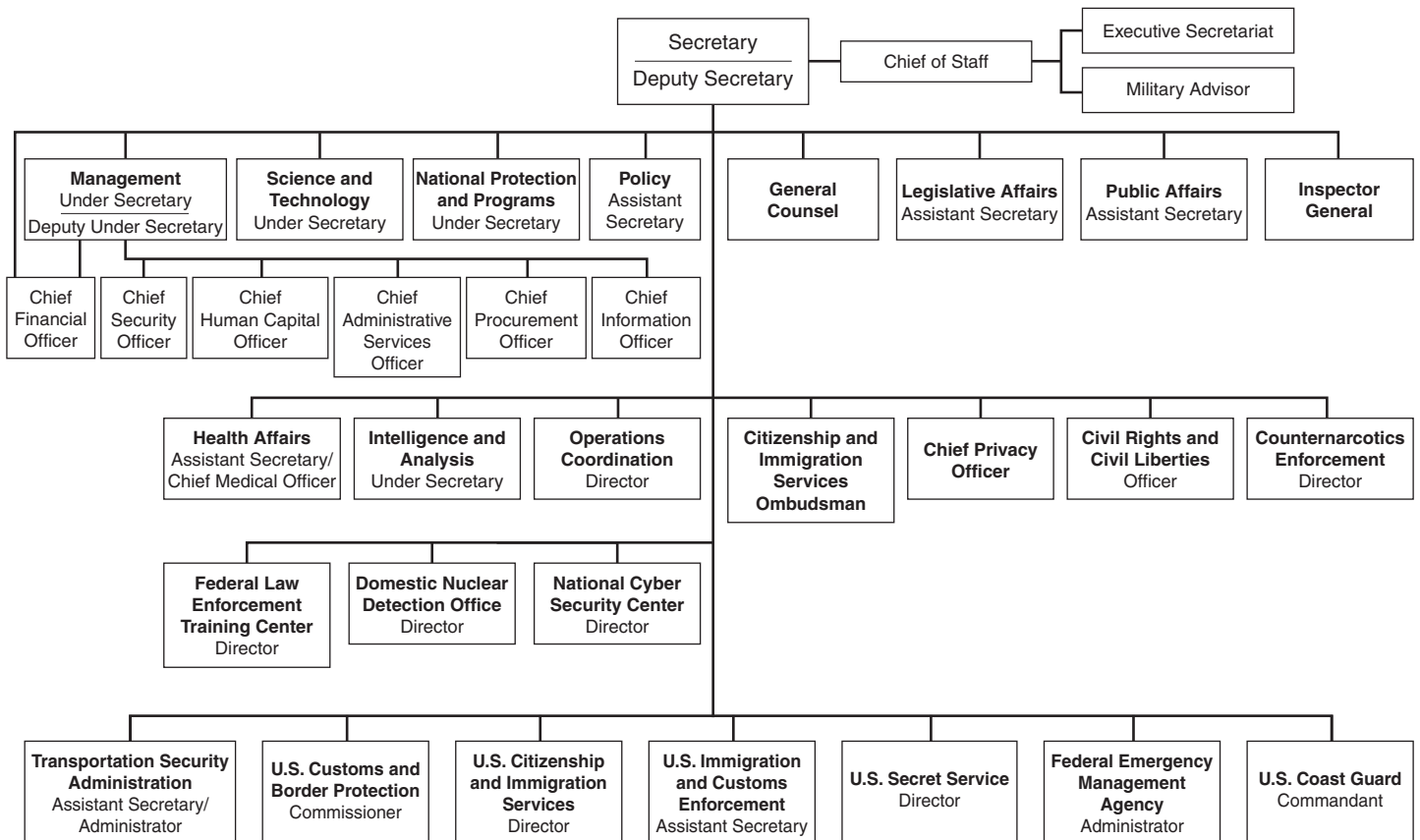
We conducted this performance audit from August 2010 to September 2011, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Additional details on our objectives, scope, and methodology are provided in appendix I.

---

## Background

DHS is charged with preventing and deterring terrorist attacks and protecting against and responding to threats and hazards to the United States. Originally formed in 2003 with the combination and reorganization of functions from 22 different agencies, the department currently consists of 7 component agencies, including U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and the U.S. Citizenship and Immigration Services (USCIS). In addition to the component agencies, centralized management functions are handled by offices including the Privacy Office, the Office of the Chief Procurement Officer, and the Office of the Chief Information Officer. Figure 1 provides an overview of the DHS organizational structure, while table 1 summarizes the responsibilities of the seven component agencies.

**Figure 1: DHS Organizational Structure**



Source: DHS.



---

---

**Table 1: DHS Component Agencies**

<b>Component agency</b>	<b>Mission</b>
Customs and Border Protection	Protects the nation's borders to prevent terrorists and terrorist weapons from entering the United States, while facilitating the flow of legitimate trade and travel.
Federal Emergency Management Agency	Prepares the nation for hazards, manages federal response and recovery efforts following any national incident, and administers the National Flood Insurance Program.
U.S. Immigration and Customs Enforcement	Protects the nation's borders by identifying and shutting down vulnerabilities in the nation's border, economic, transportation, and infrastructure security.
Transportation Security Administration	Protects the nation's transportation systems to ensure freedom of movement for people and commerce.
U.S. Citizenship and Immigration Services	Administers immigration and naturalization adjudication functions and establishes immigration services, policies, and priorities.
U.S. Coast Guard	Protects the public, the environment, and economic interests in the nation's ports and waterways, along the coast, on international waters, and in any maritime region as required to support national security.
U.S. Secret Service	Protects the President and other high-level officials and investigates counterfeiting and other financial crimes, including financial institution fraud, identity theft, computer fraud, and computer-based attacks on our nation's financial, banking, and telecommunications infrastructure.

Source: GAO analysis of DHS data.

---

## DHS IT Acquisition Management

DHS spends billions of dollars each year to develop and acquire IT systems that perform both mission-critical and support functions. In fiscal year 2011, DHS expects to spend approximately \$6.27 billion on over 300 IT-related programs, including 45 major IT acquisition programs.<sup>1</sup>

In order to manage these acquisitions, the department established the Management Directorate, which includes the Chief Information Officer (CIO), the Chief Procurement Officer, and the Acquisition Review Board. In addition, the Chief Privacy Officer plays a key role in developing and deploying IT systems. Specific roles and responsibilities for these entities are described below:

- The CIO's responsibilities include setting IT policies, processes and standards, and ensuring departmental information technology

---

<sup>1</sup>DHS defines major IT acquisitions as those with total life-cycle costs over \$300 million or programs that warrant special attention due to their importance to the department's strategic and performance plans, effect on multiple components, or program and policy implications, among other factors.

---

acquisitions comply with its management processes, technical requirements, and approved enterprise architecture, among other things. Additionally, the CIO chairs the department's Chief Information Officer Council, which is responsible for ensuring the development of IT resource management policies, processes, best practices, performance measures, and decision criteria for managing the delivery of services and investments, while controlling costs and mitigating risks.

- The Chief Procurement Officer is the department's senior procurement executive, who has leadership and authority over DHS acquisition and contracting, including major investments. The officer's responsibilities include issuing acquisition policies and implementation instructions, overseeing acquisition and contracting functions, and ensuring that a given acquisition's contracting strategy and plans align with the intent of the department's Acquisition Review Board.
- The Acquisition Review Board<sup>2</sup> is the department's highest-level investment review board, responsible for reviewing major programs at key acquisition decision points and determining a program's readiness to proceed to the next life-cycle phase.<sup>3</sup> The board's chairperson is responsible for approving the key acquisition documents critical to establishing a program's business case, operational requirements, acquisition baseline, and testing and support plans. Also, the board's chairperson is responsible for assessing breaches of the acquisition plan's cost and schedule estimates and directing corrective actions.
- The Chief Privacy Officer heads DHS's Privacy Office and is responsible for ensuring that the department is in compliance with federal laws and guidance that govern the use of personal information by the federal government, as well as ensuring compliance with

---

<sup>2</sup>Key members of the Acquisition Review Board include the Undersecretary of Management, the Chief Procurement Officer, CIO, and General Counsel.

<sup>3</sup>A system's life cycle normally begins with initial concept development and continues through requirements definition to design, development, various phases of testing, implementation, and maintenance phases.

---

departmental policy.<sup>4</sup> One of the office's key roles is the review and approval of privacy impact assessments (PIA), which are analyses of how personal information is collected, used, disseminated, and maintained within a system.

DHS's component agencies also share responsibility for IT management and acquisition activities. For example, the departmental CIO shares control of IT management functions with the CIOs of the major component agencies. Similarly, DHS's Chief Procurement Officer and the component agencies' senior acquisition officials share responsibility for managing and overseeing component acquisitions. Further, the Privacy Office coordinates with privacy officers for each major component agency to ensure that system PIAs are completed.

---

## DHS Collects and Analyzes Personal Data to Fulfill Its Mission

In fulfilling its mission, DHS and its component agencies collect and analyze data, including data about individuals. Data-mining systems provide a means to analyze this information. These systems apply database technology and associated techniques—such as queries, statistical analysis, and modeling—in order to discover information in massive databases, uncover hidden patterns, find subtle relationships in existing data, and predict future results.

The two most common types of data mining are pattern-based queries and subject-based queries. Pattern-based queries search for data elements that match or depart from a pre-determined pattern, such as unusual travel patterns that might indicate a terrorist threat. Subject-based queries search for any available information on a predetermined subject using a specific identifier. This identifier could be linked to an individual (such as a person's name or Social Security number) or an object (such as a bar code or registration number). For example, one could initiate a search for information related to an automobile license plate number. In practice, many data-mining systems use a combination of pattern-based and subject-based queries.

---

<sup>4</sup>For purposes of this report, the term personal information encompasses all information associated with an individual, including both *identifying* and *nonidentifying* information. Personally identifying information, which can be used to locate or identify an individual, includes things such as names, aliases, and agency-assigned case numbers. Nonidentifying personal information includes such things as age, education, finances, criminal history, physical attributes, and gender.

By law, DHS is required to report to Congress annually on its pattern-based data-mining systems that are used to indicate terrorist or criminal activity.<sup>5</sup> In its most recent report, DHS identified three such systems. For example, CBP's Automated Targeting System (ATS) compares intelligence and law enforcement data with traveler and cargo data to detect and prevent terrorists and terrorist weapons from entering the United States.

DHS's subject-based data-mining systems are more common. These include any information system that uses analytical tools to retrieve information from large volumes of data or multiple sources of information. For example, the ICE Pattern Analysis and Information Collection (ICEPIC) system allows analysts to search for information about individuals who are the subject of investigation across multiple data sources. Table 2 describes the six DHS data-mining systems (and, where applicable, key components of the systems) evaluated in this report.

**Table 2: Selected DHS Data-Mining Systems**

System/component	Description
Analytical Framework for Intelligence (AFI)	CBP is developing this system to enable intelligence analysts to perform data queries and searches of multiple CBP data sources from a single platform/interface, the results of which are presented in the single platform. In addition, AFI is to provide access and federated search functions to other data sources and systems via interconnections. It is to provide automated tools and capabilities to support different kinds of analysis and visualization by CBP intelligence analysts, including link analysis, anomaly detection, change detection analysis, temporal analysis, pattern analysis, and predictive modeling of the data, and will assist with production management and work flow of intelligence products and reports.
Automated Targeting System (ATS)/ ATS-Passenger (ATS-P)	CBP uses the pattern-based ATS system to collect, analyze, and disseminate information that is gathered for the primary purpose of targeting, identifying, and preventing potential terrorists and terrorist weapons from entering the United States. ATS-P is one of three data-mining components of this system. It uses data mining to evaluate travelers prior to their arrival at U.S. ports of entry. The other two components (Inbound and Outbound) primarily analyze cargo, not individuals.
Citizen and Immigration Data Repository (CIDR)	USCIS is developing this system to allow classified queries of USCIS benefits administration data systems in order to vet USCIS application information for indications of possible immigration fraud and national security concerns (when a classified environment is required), detect possible fraud and misuse of immigration information or position by USCIS employees, and respond to requests for information from the DHS Office of Intelligence and Analysis and the federal intelligence and law enforcement community that are based on classified criteria.

<sup>5</sup>The Federal Agency Data Mining Reporting Act of 2007, 42 U.S.C. 2000ee-3.

System/component	Description
Data Analysis and Research for Trade Transparency System (DARTTS)	ICE uses this pattern-based system to help carry out its responsibility to investigate import-export crimes including trade-based money laundering, contraband smuggling, and trafficking of counterfeit goods. ICE agents and analysts use the system to mine trade and financial data in order to identify possible illegal activity based on anomalies they find in certain trade activities.
ICEPIC	ICE uses this system to search disparate sources of information for previously unknown relationship data about individuals who are the subject of investigations. It is one of five projects in ICE's Enforcement Information Sharing program. One feature of this system is the Law Enforcement Information Sharing Service, a Web service that links federal, state, and local law enforcement information sharing partners to ICEPIC's searchable data sets.
TECS <sup>a</sup> /TECS Modernization (TECS-Mod)	<p>CBP operates the TECS system, and it is used by more than 20 federal agencies for border enforcement needs and the sharing of border enforcement and traveler entry/exit information. The primary mission of the system is to support the agency in the prevention of terrorist entry into the United States and the enforcement of U.S. laws related to trade and travel. The system processes over 2 million transactions daily.</p> <p>TECS-Mod is an ongoing initiative to modernize legacy TECS capabilities with modules focused on the primary and secondary inspection of travelers and cargo entering and exiting the United States. The modernized TECS will perform data queries in support of those inspections that are to compare traveler's information with things such as watch-lists, and is also to process travel documentation.</p>

Source: GAO analysis of DHS data.

<sup>a</sup>TECS was originally called the Treasury Enforcement Communications System, but it lost that name when the system was transferred to DHS. Currently, TECS is not considered an acronym for anything.

## Federal Laws Define Steps to Protect the Privacy of Personal Information

Multiple federal laws provide privacy protections for personal information used by federal agencies. The major requirements for the protection of personal privacy by federal agencies come from two laws, the Privacy Act of 1974 and the E-Government Act of 2002. In addition, the Federal Information Security Management Act of 2002 (FISMA) addresses the protection of personal information in the context of securing federal agency information and information systems, and the Homeland Security Act specifies additional roles for DHS's Chief Privacy Officer. Further, the Federal Agency Data Mining Reporting Act of 2007 requires federal agencies to report to Congress on the use of certain data-mining systems, including their potential impact on personal privacy. These laws are discussed in more detail below.

- 
- *The Privacy Act*<sup>6</sup>—This act places limitations on agencies’ collection, disclosure, and use of personal information maintained in systems of records.<sup>7</sup> The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public through a system of records notice in the Federal Register. This notice should identify, among other things, the categories of data collected, the categories of individuals about whom information is collected, the purposes for which the information is used (including, for example, intended sharing of the information), and procedures that individuals can use to review and correct personal information.
  - *The E-Government Act of 2002*—This act strives, among other things, to enhance protection for personal information in government information systems and information collections by requiring that agencies conduct privacy impact assessments (PIA). A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. According to Office of Management and Budget (OMB) guidance, a PIA is to (1) ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.<sup>8</sup> Agencies are required to conduct PIAs before developing or procuring information technology that collects, maintains, or disseminates information that is in a personally identifiable form, and before initiating any new data collections involving personal information that will be collected, maintained, or disseminated using information technology if the same questions are asked of 10 or more people. To the extent that PIAs are made publicly available, they provide explanations to the public about such things as the information that will be collected, why it is being collected, how it is

---

<sup>6</sup>5 U.S.C. § 552a.

<sup>7</sup>The act describes a “record” as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. It also defines “system of records” as a group of records under the control of any agency from which information is retrieved by the name of the individual or other individual identifier.

<sup>8</sup>Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Sept. 26, 2003).

---

to be used, and how the system and data will be maintained and protected.<sup>9</sup>

- *FISMA*—This act defines federal requirements for securing information and information systems that support federal agency operations and assets. It requires agencies to develop agencywide information security programs that extend to contractors and other providers of federal data and systems.<sup>10</sup> Under FISMA, information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, including controls necessary to preserve authorized restrictions on access and disclosure to protect personal privacy.
- *The Homeland Security Act of 2002*<sup>11</sup>—This act requires DHS to establish a Chief Privacy Officer to oversee its implementation of privacy protections. According to the act, the Chief Privacy Officer is responsible for, among other things, providing assurance that the agency's use of technologies sustains privacy protections relating to the use, collection, and disclosure of personal information and that personal information within systems of records is handled in compliance with fair information practices as set out in the Privacy Act.<sup>12</sup>
- *The Federal Agency Data Mining Reporting Act of 2007*—The act requires federal agencies to report annually to Congress on pattern-based analyses of electronic databases used to identify predictive patterns or anomalies that indicate terrorist or criminal activity. The act excludes analyses that are subject-based, that use personal identifiers or inputs associated with individuals, and those that are

---

<sup>9</sup>The E-Government Act requires agencies, if practicable, to make privacy impact assessments publicly available through agency Web sites, by publication in the *Federal Register*, or by other means. Pub. L. 107-347, § 208(b)(1)(B)(iii).

<sup>10</sup>FISMA, Title III, E-Government Act of 2002, Pub. L. 107-347 (Dec. 17, 2002), 44 U.S.C. § 3541, et seq.

<sup>11</sup>Pub. L. No. 107-296, § 222 (Nov. 25, 2002).

<sup>12</sup>For more information on the Fair Information Practices, see appendix II.

---

solely to detect fraud, waste, and abuse in government agencies or programs, or for government computer security.<sup>13</sup>

---

### Assessment Framework Provides Guidance for Evaluating System Effectiveness and Privacy Impacts

In 2008, the National Research Council (NRC)<sup>14</sup> issued a report outlining ways to evaluate the effectiveness and privacy protections of data-mining systems at agencies with counterterrorism responsibilities, including DHS.<sup>15</sup> In its report, NRC recommends that agencies establish a systematic process—such as the framework that it proposes—to evaluate their policies and programs. NRC’s proposed framework addresses five key elements: (1) ensuring organizational competence, (2) evaluating the effectiveness of systems throughout their life cycles, (3) evaluating the privacy protections of systems throughout their life cycles, (4) obtaining executive review and authorization, and (5) providing appropriate transparency and external oversight throughout a system’s life cycle.

Supplementing NRC’s recommended framework, GAO and others have recommended specific policies and practices to ensure that IT investments receive appropriate executive oversight throughout their life cycles, that IT acquisitions are adequately managed, and that individuals’ personal information is adequately protected. Key sources include:

- *Investment management*—In 2004, we issued a framework for assessing federal agencies’ IT investment management practices.<sup>16</sup> Investment management involves executive oversight of a system or project throughout its life cycle. Investment management processes and practices are used to select, control, and evaluate investments in

---

<sup>13</sup>As previously noted, in its most recent report, DHS identified three pattern-based data mining systems. These include DARTTS, ATS, and the Freight Assessment System, which does not focus on personal information.

<sup>14</sup>The NRC is the principal operating agency of the National Academies of Sciences and Engineering, which are private, nonprofit societies of distinguished scholars engaged in scientific and engineering research. The NRC’s purpose is to provide services to the federal government, the public, and the scientific and engineering communities.

<sup>15</sup>National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment* (Washington, D.C.: 2008).

<sup>16</sup>GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* (Version 1.1), [GAO-04-394G](#) (Washington, D.C.: March 2004).



---

order to help ensure that they increase business value and mission performance.

- *System acquisition management*—In 2007, the Software Engineering Institute established a model for organizations to use to assess and improve system management capabilities in different process areas, such as project planning, project monitoring and control, requirements management, configuration management, and risk management.<sup>17</sup> These processes help agencies reduce the risk of cost overruns, schedule delays, and performance shortfalls.
- *Personal privacy protection*—Originally developed in 1972, revised in 1980, and reinforced in 1998 and 2006, the Fair Information Practices provide a framework of principles for balancing the need for privacy with other public policy interests, such as national security, law enforcement, and administrative efficiency. These practices underlie the provisions of multiple national and international laws and policies affecting personal privacy, including the Privacy Act. See appendix II for more information on the Fair Information Practices.

Supplementing NRC's proposed framework with the policies and practices discussed above, we developed a systematic framework to evaluate agencies' policies and practices. This evaluation framework is organized into five key elements and includes two components. One component of the framework focuses on agency policies and the other component focuses on system management practices. Table 3 provides an overview of this evaluation framework.

---

<sup>17</sup>Software Engineering Institute, *Capability Maturity Model® Integration (CMMI®) for Acquisition*, Version 1.2, CMU/SEI-2007-TR-017 (Pittsburgh, Pa.: November 2007).

**Table 3: Overview of a Systematic Framework for Evaluating Agency Policies and Practices for System Effectiveness and Privacy Impacts**

Key element	Policy evaluation component	Practice evaluation component
Organizational competence	Ensure that agency policies establish key authorities and require that appropriate staffing is in place and trained.	Ensure that appropriate authorities and staffing are in place and that they perform required functions.
Evaluating system effectiveness	Ensure that agency policies require assessments and testing of the system while it is being developed, before deployment, and once operational.	Ensure that required assessments and testing have taken place.
Evaluating privacy impacts	Ensure that agency policies require assessments of system privacy impacts, before developing, operating, or making major changes to systems, as well as evaluations once operational.	Ensure that privacy impact assessments and required independent reviews have taken place.
Obtaining executive review and authorization of investments	Ensure that agency policies establish executive investment review boards and require that they conduct appropriate reviews.	Ensure that the system has undergone reviews by investment review boards, as appropriate.
Providing transparency and external oversight	Ensure that agency policies require regular reviews by non-system owners, and transparency to external overseers.	Ensure that the program office has obtained regular reviews of the system and provided appropriate transparency.

Source: GAO analysis of NRC recommendations, the Software Engineering Institute's Capability Maturity Model® Integration for Acquisition, federal law and guidance, and GAO guidance.

This evaluation framework is consistent with many aspects of a recent plan established by the Administration to reform IT.<sup>18</sup> The reform plan identifies steps and time frames for achieving operational efficiencies and effectively managing large-scale IT programs. Further, most reviews required under this framework are not new; rather they are required by law or guidance, or suggested by best practices. The benefit of using such a framework is that it provides an integrated approach to ensuring system effectiveness and privacy protections from both a policy and practice perspective. DHS's CIO commented that the framework appears to provide a reasonable approach to ensuring data-mining systems are effective and provide adequate privacy protections.

<sup>18</sup>The White House, *25-Point Implementation Plan to Reform Federal Information Technology Management* (Washington, D.C.: Dec. 9, 2010).

---

## Prior Reviews of DHS Have Identified Concerns

In recent years, we have reported on acquisition management challenges, data-mining systems, and privacy concerns at DHS.<sup>19</sup> For example, in September 2009, we testified that since its creation, DHS had faced challenges in acquiring large-scale IT systems, leading to cost and schedule overruns on multiple programs.<sup>20</sup> We reiterated recommendations that DHS improve its acquisition management process and implement better acquisition management reviews. In June of 2010, we reported that DHS had made progress in its efforts to effectively and efficiently acquire large-scale IT programs—for instance by providing more guidance on acquisitions at the departmental and component levels—but that its implementation of acquisition management policies and practices was inconsistent.<sup>21</sup> Moreover, we reported that many major IT system acquisitions were not receiving effective oversight. DHS acknowledged these shortfalls, and the department’s CIO is developing suggestions for improving DHS’s governance process.

Regarding DHS data-mining systems and privacy protections, in 2007 we reported that DHS’s Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement data-mining tool raised a number of privacy concerns, such as the potential for erroneously associating individuals with crime or terrorism and the misidentification of individuals with similar names.<sup>22</sup> The system was subsequently canceled. We also repeatedly reviewed the Transportation Security Administration’s (TSA) Secure Flight

---

<sup>19</sup>See, for example, GAO, *Department of Homeland Security: Assessments of Selected Complex Acquisitions*, [GAO-10-588SP](#) (Washington, D.C.: July 30, 2010); *Secure Border Initiative: DHS Needs to Follow Through on Plans to Reassess and Better Manage Key Technology Program*, [GAO-10-840T](#) (Washington, D.C.: June 17, 2010); *Homeland Security: Better Use of Terrorist Watchlist Information and Improvements in Deployment of Passenger Checkpoint Technologies Could Further Strengthen Security*, [GAO-10-401T](#) (Washington, D.C.: Jan. 27, 2010); *Homeland Security: Despite Progress, DHS Continues to Be Challenged in Managing Its Multi-Billion Dollar Annual Investment in Large-Scale Information Technology Systems*, [GAO-09-1002T](#) (Washington, D.C.: Sept. 15, 2009); *Department of Homeland Security: Billions Invested in Major Programs Lack Appropriate Oversight*, [GAO-09-29](#) (Washington, D.C.: Nov. 18, 2008); *Homeland Security: Continuing Attention to Privacy Concerns is Needed as Programs Are Developed*, [GAO-07-630T](#) (Washington, D.C.: Mar. 21, 2007); and *Data Mining: Early Attention to Privacy in Developing a Key DHS Program Could Reduce Risks*, [GAO-07-293](#) (Washington, D.C.: Feb. 28, 2007).

<sup>20</sup>[GAO-09-1002T](#).

<sup>21</sup>[GAO-10-588SP](#).

<sup>22</sup>[GAO-07-293](#).

---

program, and reported on the agency's progress and challenges in developing the program, including protecting privacy. Most recently, in April 2010, we reported that TSA had generally achieved all of the conditions for the program's development, including ensuring that there were no specific privacy concerns with the technology.<sup>23</sup>

Additionally, in 2007, we reported that DHS's Privacy Office had addressed its mandate to ensure that technologies sustain, and do not erode, privacy protections through a variety of actions, including implementing its PIA compliance framework and raising awareness of privacy issues through a series of public workshops. However, we noted that the office had made little progress in updating notices for legacy systems of records—older systems of records that were originally developed by other agencies prior to the creation of DHS. We recommended that DHS designate full-time privacy officers at key DHS components and establish a schedule for the timely issuance of Privacy Office reports, among other things.<sup>24</sup> DHS's Privacy Office has since implemented these recommendations.

---

## Agency Policies Address Most Elements of a Systematic Framework for Evaluating Effectiveness and Privacy, but Are Not Comprehensive

While DHS and the three component agencies we reviewed have established policies that address most elements of a systematic framework for evaluating a system's effectiveness and privacy impacts, the policies are not comprehensive. Table 4 identifies the key elements and corresponding attributes of an effective policy for evaluating system effectiveness and privacy impacts.

---

<sup>23</sup>GAO, *GAO Review of the Department of Homeland Security's Certification of the Secure Flight Program—Cost and Schedule Estimates*, [GAO-10-535R](#) (Washington, D.C.: Apr. 5, 2010).

<sup>24</sup>GAO, *DHS Privacy Office: Progress Made but Challenges Remain in Notifying and Reporting to the Public*, [GAO-07-522](#) (Washington, D.C., Apr. 27, 2007).

**Table 4: Key Elements of an Effective Policy for Evaluating System Effectiveness and Privacy Impacts**

Element	Policy attributes
Ensuring organizational competence	<ul style="list-style-type: none"> <li>• Establish acquisition decision authorities responsible for approving acquisitions as they progress through their life cycle.</li> <li>• Establish a policy-level chief privacy officer responsible for ensuring compliance with privacy laws, policies, and guidance, and as appropriate, component privacy officials responsible for assisting in this process.</li> <li>• Require agencies to develop staffing plans that include staff responsible for ensuring a system's effectiveness and privacy protections.</li> <li>• Require agencies to train those responsible for the system's privacy and security requirements.</li> </ul>
Evaluating system effectiveness	<ul style="list-style-type: none"> <li>• Require evaluations of systems while they are being developed or when they have major changes to ensure consistency with their stated purpose.</li> <li>• Require evaluations of system effectiveness (including adequate testing and data quality assessments).</li> <li>• Require an independent assessment of the system's effectiveness (by an entity outside of the program office).</li> <li>• Require routine re-evaluations of systems once deployed to ensure their continued effectiveness and consistency of purpose.</li> </ul>
Evaluating privacy impacts	<ul style="list-style-type: none"> <li>• Require program offices to conduct privacy impact assessments before developing, operating, or making major changes to information systems that process personal information.</li> <li>• Require privacy assessments to include an evaluation of privacy risks and mitigation strategies, the manner in which data are collected and are to be used, security safeguards, procedures for an individual to access and request corrections to their personal information, transparency, and accountability.</li> <li>• Require an independent assessment of a system's privacy impacts and protections (by an entity outside of the program office).</li> <li>• Require periodic re-evaluations of a system's privacy and security protections once the system is deployed.</li> </ul>
Obtaining executive review and authorization of investments	<ul style="list-style-type: none"> <li>• Establish investment review boards that provide executive review and authorization to proceed at regular intervals throughout a system's life cycle—including design, development, and operation.</li> <li>• Require investment reviews to               <ul style="list-style-type: none"> <li>• assess the system's alignment with the agency's goals and mission.</li> <li>• ensure that the system is operating as intended.</li> <li>• ensure that the system has adequate privacy and security protections in place.</li> </ul> </li> </ul>
Providing transparency and external oversight	<ul style="list-style-type: none"> <li>• Require regular reviews of operational information systems by non-system owners (such as the CIO and privacy office) to ensure compliance with privacy and effectiveness requirements.</li> <li>• Ensure that programs report on a system's effectiveness and privacy protections to external overseers, as required.</li> <li>• Require that information is provided to external overseers (such as a congressionally-sponsored oversight board) to allow more intensive scrutiny of a system's privacy protections in cases where public reporting is not required.</li> </ul>

Source: GAO analysis of NRC recommendations, the Software Engineering Institute's Capability Maturity Model® Integration for Acquisition, federal law and guidance, and GAO guidance.

DHS and selected component agencies (CBP, ICE, and USCIS) have established acquisition, investment, and privacy-related policies that address many of the elements and attributes; however, these policies are not comprehensive. At the corporate level, DHS has incorporated most of the critical elements into its policies, but the policies do not fully ensure executive review and transparency. The component agencies' policies partially address most of the elements, but are lacking several important attributes. For example, none of the three component agencies' policies sufficiently address requirements for evaluating system effectiveness or transparency and external oversight. Table 5 provides an assessment of policy areas by agency; a discussion of the agencies' policies follows the table. A detailed assessment of our results can be found in appendix III.

**Table 5: Assessment of DHS and Selected Component Agencies' Policies**

Element	DHS (corporate)	CBP	ICE	USCIS
Ensuring organizational competence	●	●	●	●
Evaluating system effectiveness	●	●	●	○
Evaluating privacy impacts	●	●	●	●
Obtaining executive review and authorization	●	●	●	●
Providing transparency and external oversight	●	●	●	●

Source: GAO analysis of agency data.

**Key**

- = The agency's policies address all of the attributes of this element.
- = The agency's policies address most of the attributes of this element.
- = The agency's policies address about half of the attributes of this element.
- = The agency's policies address a few of the attributes of this element.
- = The agency's policies address none of the attributes of this element.

- *Ensuring organizational competence:* DHS and the component agencies' policies address all or most of the key attributes needed to ensure organizational competence. Specifically, DHS and the three component agencies' policies establish key authorities, including acquisition decision authorities for information-based systems; a policy-level chief privacy officer responsible for ensuring compliance with privacy laws, policies, and guidance; and senior privacy officials for all three component agencies to assist with privacy compliance. In addition, DHS, ICE, and USCIS policies require that program managers assess staff qualifications and resources during system development.

---

Further, DHS policies guide the component agencies in requiring that all staff receive training on security and privacy requirements.

However, CBP policies do not require planning to ensure adequate staff resources. Agency officials stated that they are in the process of revising their acquisition guidance, and anticipate having it completed by September 2011. Until CBP updates its policy to ensure staff qualifications and resources, the agency may be limited in its ability to ensure that program offices have the staff they need to evaluate a system's effectiveness and privacy protections.

- *Evaluating system effectiveness:* DHS, CBP, and ICE policies address all or most of the key attributes for evaluating the effectiveness of systems throughout their life cycles; however, USCIS's policies only address about half of the attributes. DHS's department-level policies require agencies to evaluate systems in development to ensure consistency with their stated purpose, adequately test and conduct data quality assessments for systems before they are deployed, conduct an independent assessment of system effectiveness, and re-evaluate systems once they are operational to ensure that they are still effective and consistent with their stated purpose.

However, component agency policies that supplement the department's policies are not consistent in evaluating system effectiveness. Specifically, none of the three component agencies' policies require data quality assessments for systems before they are deployed. Moreover, the agencies' policies do not require routine re-evaluations of systems once they are operational to ensure continued effectiveness and consistency of purpose. One reason for this disconnect is that DHS recently updated its system acquisition policy, and the component agencies have not yet fully updated their implementing policies. Until the component agencies update their policies to require data quality assessments and re-evaluations of systems once they are operational, DHS and its component agencies may not be able to ensure that systems are operating as effectively as desired or as originally intended.

- *Evaluating privacy impacts:* DHS and the selected component agencies' policies address all of the key attributes for evaluating privacy impacts. The DHS Privacy Office has established policies that require program offices to develop PIAs before developing, operating, or making major changes to information systems that process personal information. The

---

department requires that these PIAs include an evaluation of privacy risks and mitigation strategies, the manner in which data are collected and used, security safeguards, and procedures for individuals to access and request corrections to their personal information. In addition, the DHS Privacy Office—which is independent of program offices and operates under its own authority—reviews and approves all PIAs. The office has several mechanisms for periodically re-evaluating a system’s privacy and security protections. For example, according to DHS policy, the office is to review and approve a program’s assessment of whether or not a new PIA is needed at least every 3 years (or when there are major system changes).

While the DHS Privacy Office has primary responsibility for establishing and ensuring compliance with privacy policies throughout the department, the component agencies’ privacy officers are to oversee their respective agencies’ implementation of guidance from the DHS Chief Privacy Officer. This includes facilitating the completion of required privacy compliance documents by system managers.

- *Obtaining executive review and authorization of investments:* USCIS policies address all of the key attributes of executive review and authorization; however, DHS, ICE, and CBP policies do not address all of the attributes. The department’s acquisition policies establish review boards and other review mechanisms for information-based systems throughout their life cycles, including design, development, and operations. These executive reviews are to include assessments of a system’s alignment with the agency’s goals and mission, whether a system is operating as intended, and privacy and security protections that are in place. Further, component agencies are responsible for providing executive review and authorization for systems with less than \$300 million in life-cycle costs and are to have policies that supplement the department’s policies. All three component agency policies generally require reviews to include assessments of a system’s alignment with the agency’s goals and mission, whether a system is operating as intended, and privacy and security protections that are in place.

However, we previously reported that DHS does not perform executive reviews for many of its major IT investments. Specifically, in September 2009 and again in June of 2010<sup>25</sup> we reported on the

---

<sup>25</sup>[GAO-09-1002T](#) and [GAO-10-588SP](#).



---

status of DHS's acquisition improvement efforts. Despite some progress, we found that many of DHS's major acquisitions were still not receiving effective oversight. Among other things, we noted that the ARB had begun to meet more frequently than in the past, but more than 40 programs had not been reviewed. Further, ICE and CBP policies do not adequately establish investment review boards or define how the boards are to provide oversight throughout a system's life cycle. As of May 2011, the department's CIO and ICE were in the process of reorganizing their governance structures for IT investments, and the CIO reported plans to improve the executive review process by conducting more intensive reviews. In addition, while CBP policies identify requirements for an investment review board to conduct periodic evaluations of IT investments, the policies do not describe how or when the board conducts its reviews or for which systems. CBP officials stated that they are currently updating their acquisition policy and plan to more clearly define their governance process in the next iteration of the policy. Until DHS performs intensive reviews of all of its major IT investments and ICE and CBP establish review boards and define how they are to provide oversight throughout a system's life cycle, the department and component agencies may be unable to ensure that systems receive adequate executive review and approval, including reviews of systems' effectiveness and privacy protections.

- *Providing transparency and external oversight:* While DHS and the selected component agencies' policies address most of the key attributes for providing transparency and oversight, they do not address all of them. DHS and the selected component agencies' policies require regular reviews and documentation of a system's effectiveness and privacy protections once they are in operation, and require reporting to internal and external overseers on a system's effectiveness and privacy protections. For example, DHS policies require programs to report on system effectiveness and privacy protections to DHS, component agency oversight offices, the Office of Management and Budget, and Congress. In particular, DHS's Privacy Office is required to publish all system PIAs, unless a PIA is deemed too sensitive to release publicly. Further, the department reports annually to Congress on the status of pattern-based data-mining systems.

However, DHS's and the component agencies' policies do not require providing information to external overseers (such as a congressionally-sponsored oversight board) to allow additional scrutiny of the privacy protections of the sensitive information-based

systems that are not publicly available. DHS privacy officials reported that they do not currently have enough resources to facilitate additional reviews for all sensitive systems and believe that current policies and guidance are sufficient to address review and approval of sensitive systems. Until DHS provides for increased scrutiny of its most sensitive systems, the department may be limited in its ability to assure the public that those systems have appropriate privacy protections in place.

While DHS and the three component agencies have implemented policies that address many of the desired attributes, there are key areas where policies are not comprehensive. One reason for this disconnect is the challenges DHS and its component agencies currently face in stabilizing and implementing acquisition policies throughout the department. Until the department and agencies expand and implement their policies, they may not have adequate assurance that critical data-mining systems used in support of counterterrorism are both effective and that they protect personal privacy.

## Program Offices Are Evaluating System Effectiveness and Privacy Protections, but Have Not Consistently Implemented Key Activities

The six DHS program offices we reviewed have taken steps to evaluate their system’s effectiveness and privacy protections; however, none performed all of the key activities associated with an effective evaluation framework. Table 6 describes the key elements from a practice perspective, detailing the activities an agency or program office should perform to evaluate how effectively their systems perform and protect privacy-related information.

**Table 6: Key Elements and Activities for Evaluating System Effectiveness and Privacy Protections**

Element	Agency and program office activities
Ensuring organizational competence	<ul style="list-style-type: none"> <li>• Have the established authority for the information system certify key acquisition decisions, including decisions that affect personal data about specific individuals.</li> <li>• Ensure, through the agency chief privacy officer (or his/her representative), that the system is in compliance with privacy laws, policies, and guidance.</li> <li>• Assess the program office workforce to determine the skills needed and to identify existing gaps in its ability to fulfill its program effectiveness and privacy responsibilities. Then, ensure the program office is sufficiently staffed to fulfill its responsibilities.</li> <li>• Provide program staff engaged in developing or using the information system with required security and privacy training.</li> </ul>

Element	Agency and program office activities
Evaluating system effectiveness	<ul style="list-style-type: none"> <li>• Perform a comprehensive evaluation of the information system’s consistency with its articulated purpose.</li> <li>• Identify any changes to the system that cause it to deviate from its original purpose and ensure that these changes are approved.</li> <li>• Evaluate the system before it is made operational to demonstrate expected effectiveness. In doing so, the evaluation/demonstration should be appropriate, scientifically valid, and sufficient and include documented effectiveness measures.</li> <li>• Assess the quality of the data to be used in the system.</li> <li>• Obtain an independent validation of test results (by an entity outside the program office).</li> <li>• Re-evaluate the system once it is operational to ensure the system continues to be effective and consistent with its intended purpose.</li> <li>• Assess system and operator performance, with mechanisms for detecting and reporting errors such as monitoring tools and regular audits.</li> </ul>
Evaluating program privacy impacts	<ul style="list-style-type: none"> <li>• Conduct a privacy impact assessment for the information system before developing, operating, and making major changes to the system.</li> <li>• Ensure the privacy impact assessment adequately addresses issues such as: privacy risks and actions taken to mitigate those risks; data collections; data uses; information security safeguards; and transparency, redress, and accountability regarding data issues.</li> <li>• Obtain an independent validation of the system’s privacy impacts and protections (by an entity outside the program office).</li> <li>• Have and use a process to periodically review the effectiveness of the program’s privacy and security controls to update privacy impact assessments and system of records notices as appropriate.</li> </ul>
Obtaining executive review and authorization of investments	<ul style="list-style-type: none"> <li>• Have the executive review board evaluate the information system at each major phase of development and have these assessments and decisions documented.</li> <li>• Examine the system’s effectiveness, privacy protections, information security, legal compliance, and alignment with the agency’s mission.</li> <li>• Track any review board recommendations and concerns until they are fully addressed and closed.</li> </ul>
Providing transparency and external oversight	<ul style="list-style-type: none"> <li>• Obtain regular reviews of the information system by external organizations (CIO, privacy office, other) to ensure compliance with privacy and effectiveness requirements.</li> <li>• Track corrective actions taken to address recommendations that were raised during regular external reviews until they are closed.</li> <li>• Provide reports for external oversight and publicly post reports, as required.</li> <li>• Document the legitimate reasons that a program office may not post required reports publicly and demonstrate that it has sought additional levels of scrutiny of the system’s privacy protections.</li> </ul>

Source: GAO analysis of NRC recommendations, federal law and guidance, and GAO guidance.

The program offices of the six systems we reviewed varied widely in performing the activities associated with an effective evaluation framework. The TECS-Mod program office performed most of the activities, while the AFI program office performed relatively few. The other systems’ program offices were in the middle of those extremes. The program offices were also stronger in certain elements. For example, four program offices performed all or most of the activities for ensuring

organizational competence, evaluating program privacy impacts, and ensuring transparency. Conversely, none of the program offices performed all of the activities related to evaluating system effectiveness or obtaining executive review and approval. Table 7 provides an assessment of each program office's efforts to perform activities associated with evaluating system effectiveness and privacy protections. More detailed assessments for each system can be found in appendix IV.

**Table 7: Assessment of System Practices**

Element	AFI	ATS-P	CIDR	DARTTS	ICEPIC	TECS-Mod
Ensuring organizational competence	●	●	●	●	●	●
Evaluating system effectiveness	●	●	●	●	●	●
Evaluating program privacy impacts	●	●	●	●	●	●
Obtaining executive review and authorization	●	n/a <sup>a</sup>	●	●	●	●
Providing transparency and oversight	●	●	●	●	●	●

Source: GAO analysis of agency data.

**Key**

- = The program office performed all of the activities of this element.
- = The program office performed most of the activities of this element.
- = The program office performed about half of the activities of this element.
- = The program office performed a few of the activities of this element.
- = The program office performed none of the activities of this element.

n/a = This element is not applicable to the program.

<sup>a</sup>The ATS-P program has been in operation for over a decade, and the program office has not performed any significant enhancements to the system. Accordingly, obtaining executive review and authorization for investment activities is not applicable.

- **Ensuring organizational competence:** Four of the six program offices performed all or most of the activities associated with ensuring organizational competence. Specifically, the ATS-P, DARTTS, and TECS-Mod program offices performed all of the activities, while the CIDR program office performed most of the activities. For example, while the CIDR program has an approved privacy assessment, it did not complete all acquisition requirements.

---

The two remaining program offices performed about half of the activities associated with organizational competence. Specifically, ICEPIC's program office is taking steps to assess its program workforce and has an approved PIA that covers that majority of the system, but its acquisition authority has not certified all acquisition documentation and the program office has not yet updated its PIA after making changes to the system in 2008. AFI's program office identified needed workforce skills, but did not ensure that the agency acquisition authority certified applicable acquisition documents, and the agency privacy officer has not yet affirmed that the program is compliant with applicable privacy laws and policies.

- *Evaluating system effectiveness:* Four of the six program offices performed most of the activities associated with evaluating system effectiveness. Specifically, the DARTTS and TECS-Mod program offices evaluated their systems' consistency with their respective intended purposes and evaluated system effectiveness through testing. However, the DARTTS program has not tested the quality of system data and the TECS-Mod program has not performed recurring operational assessments. In addition, CIDR's program office has evaluated system effectiveness and assessed data quality, but has not yet developed a plan for operational testing, and the ICEPIC program has evaluated its consistency with its intended purpose, but its assurance of the system's effectiveness is limited by poor data quality.

The two remaining program offices performed about half of the activities associated with evaluating system effectiveness. The AFI program office evaluated the system's consistency with its intended purpose. However, the program office's testing of whether the system will perform as intended is ongoing. The ATS-P program office performs ongoing monitoring of the system's effectiveness, but it has not assessed the system's consistency with its intended purpose or assessed the quality of the system's data.

- *Evaluating program privacy impacts:* Four of the six program offices performed all or most of the activities associated with evaluating privacy protections. Specifically, ATS-P's, CIDR's and DARTTS's program offices performed all of the activities associated with this element, and the TECS-Mod program office performed most of the activities. These activities include completing a privacy impact assessment that addresses system privacy risks and the steps taken to mitigate them and having the assessment independently validated by the DHS Privacy Office. The current privacy impact assessment for TECS only

---

covers three of the five main projects and does not address all potential uses of collected data. According to the program's executive director, the program office is performing an assessment to cover the remainder of the TECS platform, including the other two projects, and expects to complete the assessment in spring 2012.

The two remaining program offices—ICEPIC and AFI—performed about half or fewer of the activities, respectively. Specifically, ICEPIC's program office developed a privacy impact assessment that includes the expected uses of system-collected data and the associated information safeguards and a process for periodic evaluation of the system's effectiveness and privacy controls. However, the assessment and an associated independent validation of the system's privacy impacts and protections were completed before the program office added a component—called the Law Enforcement Information Sharing Service—that allows information sharing outside of the agency. As a result, personal information is being shared with multiple law enforcement agencies but this sharing has not been reported or disclosed. In fact, the approved PIA states that those outside the agency would not be given direct access to the personal information. Program officials recently began working to revise their PIA, but it has not yet been completed or approved. The AFI program office received independent validation of system security controls through testing; however, the office has not completed a privacy impact assessment or received independent validation of the effectiveness of the system's privacy controls.

- *Obtaining executive review and authorization of investments:* One of the six program offices—TECS-Mod—performed most of the activities associated with obtaining executive review and authorization of investments, and one other system—ATS-P—was deemed not applicable because it has not had any new investments in the past decade. The TECS oversight by the DHS acquisition review board included examining the system's effectiveness, privacy protections, information security, legal compliance, and alignment with the agency's mission. However, the acquisition plan that would be used to evaluate system effectiveness and alignment with the agency's mission was incomplete, and, as a result, the board's review was not comprehensive.

The remaining four program offices performed half or fewer of the activities associated with obtaining executive review and authorization of investments. Specifically, the office developing CIDR obtained the

---

approval of the Intelligence Systems Board on its business case; however, according to program officials it did not go through CIO life-cycle reviews—such as a review of the system’s design. The DARTTS program office performed system reviews that encompassed most framework elements. However, the reviews did not consistently address system performance measures and privacy and it is not clear that issues raised during the reviews were tracked to closure. The ICEPIC program office obtained reviews from the agency’s CIO for a component of the system that was added in March 2008 but did not obtain executive reviews for the basic system because a governance process was not in place before that system was deployed in January 2008. The AFI program office reported that acquisition documents were approved by members of the review board and the program has received review and approval during development. However, the office did not provide documentation of these reviews and decisions.

- *Providing transparency and external oversight:* Four of the six program offices performed all or most of the activities associated with providing transparency and oversight. Specifically, the ATS-P program office performed all of the framework activities, while the CIDR, DARTTS, and TECS-Mod program offices performed most of the activities. For example, the CIDR program office has posted required reports such as its privacy impact assessment and system of records notice publicly, and the system has been evaluated by external organizations such as the DHS Privacy Office and Intelligence Systems Board. However, the system has not received regular reviews by the Chief Information Officer.

The remaining two program offices, ICEPIC and AFI, performed about half or fewer of the activities. Specifically, the ICEPIC program office required regular external reviews of privacy and security protections and publicly posted their privacy reports; however, its PIA does not address functionality that was added after the system was deployed. The AFI program office has completed a security assessment, but it has not obtained a review by the Privacy Office and it has not yet publicly posted its PIA.

The six program offices provided varying reasons for not performing all of the framework activities.

- The AFI branch chief stated that AFI is using an alternative development methodology that focuses on the rapid development and deployment of solutions. He added that the accelerated development

---

cycles do not match well with the agency's system development review process. As a result, many of the program review activities, such as an acquisition review board examination and issuing a privacy impact assessment, have yet to occur.

- A program official stated that ATS-P has been in operation for over a decade and that document requirements for items such as a concept of operations or operational requirements may not have existed when the system was first developed. Thus, the program does not have the fundamental documentation that would serve as a baseline for evaluating system effectiveness.
- The CIDR program manager stated that the program had not performed all the activities associated with executive review and oversight simply because the program's cost was too low for most oversight thresholds to apply. While we acknowledge that the program is small and that certain acquisition documents were not required, a key document that was required was not produced or approved.
- A DARTTS program official acknowledged that the program office does not have documented performance measures to track the performance of the system. Rather, the program office receives informal feedback from users on whether the system is operating as intended.
- ICEPIC program officials stated that the system was initially developed by the business owner and that a governance process involving system development reviews by the CIO's office did not exist when the original system was deployed. However, the officials noted that ICEPIC has recently been designated a major acquisition and, as such, will be subject to review by ICE executive management in the future.
- The executive director for TECS-Mod acknowledged that one reason that the program had not performed all oversight activities was that program officials underestimated the time and level of detail they needed to complete required development documentation.

Although the systems' program offices performed key activities in each of the framework elements, none performed all of the activities. Taken collectively, the systems were stronger in ensuring organizational competence, evaluating privacy protections, and providing transparency and oversight and weaker in evaluating system effectiveness and obtaining executive review and authorization. By not performing activities



---

associated with effectively evaluating system effectiveness and not consistently applying executive review processes, DHS and the component agencies risk developing and acquiring systems that do not effectively support their agencies' mission and do not adequately ensure the protection of privacy-related information.

---

## DHS Faces Challenges in Implementing a Framework to Ensure System Effectiveness and Privacy Protections

DHS faces key challenges in implementing a framework to ensure that its counterterrorism-related data-mining systems are effective and that they provide required privacy protections. These include (1) reviewing and overseeing operational systems, (2) implementing new policies throughout the department, and (3) ensuring timely PIAs. Until DHS addresses these challenges, it will be limited in its ability to ensure that its systems have been adequately reviewed, are performing effectively, and are appropriately protecting individual privacy.

---

## Reviewing and Overseeing Operational Systems

DHS faces a challenge in reviewing and overseeing its systems once they are in operation. OMB guidance and DHS policy call for periodic reviews of operational systems to evaluate whether they continue to fulfill mission requirements, deliver intended benefits, and meet user needs.<sup>26</sup> However, the department does not ensure that component agency programs have implemented its required process. The program offices for two of the three major operational systems we reviewed did not conduct operational analyses consistent with DHS guidance. Specifically, while the ATS-P program office reported completing operational analyses in its latest Exhibit 300 submissions, the program did not maintain the supporting documentation (such as an acquisition program baseline) that would allow it to conduct a quality analysis. Moreover, while TECS has been operational for over a decade, the system does not have a completed operational analysis.

Officials responsible for ATS-P and TECS stated that they were not aware of policies that required them to complete operational analyses.

---

<sup>26</sup>See OMB, *Capital Programming Guide: Supplement to Circular A-11, Part 7, Preparation, Submission, and Execution of the Budget* (Washington, D.C.: June 2006); and DHS, *Operational Analysis Guidance, v. 1.1* (May 2008).

---

Moreover, the two central DHS offices with responsibility for reviewing acquisitions and investments once they are operational have not done so. According to officials from the DHS Acquisition Program Management Division, which is the organization responsible for ensuring adequate review of acquisitions, the division has primarily focused on reviewing systems early in their life cycle in order to prevent system issues from occurring later. In addition, an official from the CIO's office stated that the office does not review operational analysis documentation. Rather, it conducts other reviews such as executive steering committee and program reviews.

Agency officials acknowledge that there is room for improvement with respect to ensuring adequate evaluations of operational systems and stated that there is a need for additional policies and guidance to address this issue. DHS's CIO noted that his office is proposing a portfolio management process that may help address this issue. However, until DHS develops mechanisms to ensure that its systems (including operational ones) receive adequate reviews of effectiveness, the agency is placing itself at risk that investments are not meeting user needs or that an alternative solution may be more efficient or effective than the current investment.

---

## Implementing New Policies throughout the Department

Another challenge facing DHS involves stabilizing and implementing acquisition policies throughout the department. We recently reported that DHS has made progress in clarifying acquisition management oversight processes.<sup>27</sup> However, component agencies have had difficulty keeping their policies up to date with changes in departmental acquisition policies, and system program offices have experienced difficulty in ensuring that systems already in development are in compliance with changing policies and guidance.

Over the last few years, DHS has made several changes to its acquisition policies, governance structures, and implementing guidance. For example, in 2008, the department issued an interim management directive, acquisition guidebook, and system life-cycle guidance. In 2010, the department revised its acquisition management oversight policies and

---

<sup>27</sup>GAO, *Department of Homeland Security: Progress Made in Implementation and Transformation of Management Functions, but More Work Remains*, [GAO-10-911T](#) (Washington, D.C.: Sept. 30, 2010).

---

system life-cycle guide in order to formalize the interim policies while clarifying content and making other changes, such as revising certain acquisition approval responsibilities. In order to comply with the new policies, ICE and USCIS recently revised their acquisition oversight policies and system life-cycle guidance, while CBP is still in the process of updating its policies and guidance. In addition, ICE is in the process of transitioning to a new governance structure for its executive steering committees and review boards. However, according to the DHS CIO, the department is currently considering revising its acquisition management oversight policies and governance structures for IT systems. These changes may be valuable and warranted, but the frequency of the changes makes it difficult for component agencies to effectively implement them.

Program officials reported that these frequent policy changes make it difficult to move systems through development. For example, TECS program officials reported experiencing delays in completing required program documentation due in part to a lack of understanding of documentation requirements and approval processes at the department level. In addition, the AFI project manager reported that the review and documentation requirements for the program have changed multiple times since it began development. As a result, many of AFI's document approvals have not been completed in a timely manner.

Without consistent implementation of the department's acquisition policies and guidance, DHS will be limited in its ability to ensure that its component agencies conduct appropriate and timely reviews of IT systems. Moreover, making additional changes to acquisition policies and guidance at a time when component agencies are already challenged in complying with recent changes increases the risk that systems will not comply with new policies or may encounter schedule delays and cost overruns in trying to do so.

---

## Ensuring PIAs are Timely

A third challenge facing DHS is in ensuring that all of its privacy-sensitive systems have timely and up-to-date PIAs. Federal law and guidance require agencies to develop privacy impact assessments for systems that access or process personal information. These PIAs help ensure that a system is in compliance with privacy laws and guidance, and also provide transparency to the public. For new systems, PIAs must be completed and approved before the systems can be made operational. For operational systems, program offices are required to update PIAs when there are changes to the system that affect the PIA.

However, of the six systems we reviewed, three program offices reported experiencing a lengthy process in developing and completing their PIAs. For example, AFI has been working for over 2 years to develop and complete its PIA, while the CIDR PIA took over 18 months to finalize. Table 8 provides detail on the status of the PIAs for each of the systems we reviewed.

**Table 8: Status of Privacy Impact Assessments**

System	PIA status
AFI	<ul style="list-style-type: none"> <li>Not yet completed</li> <li>The program office has been working for over 2 years to develop the PIA</li> </ul>
ATS-P <sup>a</sup>	<ul style="list-style-type: none"> <li>Original was completed in 2006</li> <li>Revised PIAs completed in 2007 and 2008</li> <li>Currently being revised again</li> </ul>
CIDR	<ul style="list-style-type: none"> <li>Completed in 2010</li> <li>It took approximately 18 months to finalize the PIA once it was submitted</li> </ul>
DARTTS	<ul style="list-style-type: none"> <li>Completed in 2008</li> <li>Revised PIA completed in 2010</li> </ul>
ICEPIC	<ul style="list-style-type: none"> <li>Completed in January 2008</li> <li>Revised PIA now under development</li> </ul>
TECS-Mod	<ul style="list-style-type: none"> <li>Partially completed—a partial PIA was completed in 2010 after 3 years of work</li> <li>The remaining parts of the PIA are still in process</li> </ul>

Source: GAO analysis of DHS documents.

<sup>a</sup>The PIA for the ATS-P program is part of the PIA for the overall ATS system.

Officials from the system program offices and DHS’s Privacy Office reported multiple reasons for the delays they have experienced in finalizing PIAs. These include (1) programs that have significant legal or developmental issues that need to be addressed before going forward, (2) draft PIAs that require extensive rework due to the relative immaturity of the program’s development, (3) resource constraints within the Privacy Office, and (4) interdependencies between systems that require completing one PIA before a related system’s PIA can be completed.

Without timely completion of PIAs and revisions to those PIAs, DHS and its component agencies risk providing insufficient oversight and transparency for their systems. They also risk delaying the development of critical systems, or alternatively, continuing to spend money on developing systems that are not consistent with the department’s privacy principles.

---

## Conclusions

With a few exceptions, DHS and three component agency policies largely address the key elements and attributes needed to ensure that their data-mining systems are effective and provide necessary privacy protections. However, in practice, none of the systems we reviewed received the full set of effectiveness and privacy evaluations that are both desired and required for data-mining systems supporting counterterrorism. For example, as required by law and DHS policy, the ICEPIC system obtained an approved privacy impact assessment before it was deployed. However, program officials subsequently deployed an information-sharing component (called the Law Enforcement Information Sharing Service), which provides functionality that is explicitly excluded in the approved privacy impact assessment. Program officials noted several reasons for the disconnect we noted between policies and practices, including system components that were initiated before the latest DHS and component agency policies were in place. Until sound evaluation policies are implemented, DHS and its component agencies risk developing and acquiring systems that do not effectively support their mission and do not adequately ensure the protection of privacy-related information.

The shortfalls we noted in agency policies and practices provide insight into key challenges DHS faces in implementing a systematic framework to ensure that its data-mining systems are effective and that they protect individual privacy. These challenges include overseeing systems once they are in operation, implementing new policies throughout the department, and ensuring PIAs are timely. Until the department ensures that its components and programs are in compliance with its acquisition process, requirements, and privacy policies, there will be limited assurance that its data-mining systems have been adequately reviewed, are delivering required capabilities, are appropriately protecting individual privacy, and maintain appropriate transparency to the public.

---

## Recommendations for Executive Action

In order to improve DHS's policies and practices for ensuring that data-mining systems used for counterterrorism are effective and provide necessary privacy protections, we are making the following five recommendations to the Secretary of Homeland Security:

Direct the Chief Information Officer and Chief Procurement Officer to work with their counterparts at component agencies to

- ensure the consistency of component agencies' policies with DHS policies and proposed improvements to those policies, including requiring data quality assessments, requiring re-evaluations of

---

operational systems, and establishing investment review boards with clearly defined structures for system review; and

- identify steps to mitigate challenges related to the review and oversight of operational systems and to DHS's changing policy requirements and determine clear corrective actions, taking the impact on components and on individual program managers into account.

Direct the Chief Privacy Officer to

- develop requirements for providing additional scrutiny of privacy protections for the sensitive information systems that are not transparent to the public through PIAs; and
- investigate whether the information sharing component of ICEPIC, called the Law Enforcement Information Sharing Service, should be deactivated until a PIA that includes this component is approved.

Direct the appropriate component agency administrators to ensure that the system program offices for AFI, ATS-P, CIDR, DARTTS, ICEPIC, and TECS-Mod

- address the shortfalls in evaluating system effectiveness and privacy protections identified in this report, including shortfalls in applying acquisition practices, ensuring executive review and approval, and consistently documenting executive reviews.

---

## Agency Comments and Our Evaluation

We received written comments from DHS's Director of the Departmental GAO/OIG Liaison Office, which are reproduced in appendix V. In those comments, the department concurred with our recommendations and identified steps it is taking to address selected recommendations.

The department also noted that the definition of data mining used in our report is broader than the definition provided in the Federal Agency Data Mining Reporting Act of 2007. The act requires DHS and other federal agencies to report on their data mining systems that perform pattern-based queries and are used to detect terrorist or criminal activity. The act excludes reporting on systems that perform subject-based queries and any queries, searches or other analyses used exclusively for the detection of fraud, waste, or abuse in a government agency or program (among other exclusions). DHS expressed concern that our broader

---

definition captures nearly every system of records utilized by the department, and could leave readers with the impression that data mining is far more prevalent at DHS than the department discloses in its Annual Data Mining Report.

We acknowledge that there are different definitions of the term “data mining,” but note that the definition used in the act applies only to those systems that should be reported to Congress in the agency’s annual report. The act does not purport to be the sole authoritative definition of the term “data mining.” Further, the definition we use in our report is consistent with industry and academic definitions, which often use the term data mining to describe analytical searches on volumes of data, regardless of the type of query that is used.<sup>28</sup> It is also consistent with the definition we have used in prior reports on data mining systems, as well as the National Research Council report we cite in this report.<sup>29</sup> Thus, we affirm that data mining systems are more common at DHS than reported (or required to be reported) in the department’s annual report on its pattern-based data mining systems.

In its letter, DHS also commented on our evaluation of specific systems, noting that the CIDR program is still in development and therefore should not be expected to complete all of the items in the evaluation framework. DHS also noted that some evaluation framework attributes are not applicable to CIDR because the system’s cost falls below the threshold at which key acquisition documents are required.

---

<sup>28</sup>For example, the Gartner Group, a leading information technology research and advisory company, defined data mining as “a process whose goal is discovering new correlations, trends, patterns, relationships and categories...by sifting through large amounts of data, using subject-link and pattern recognition technologies, as well as statistical and mathematical techniques” Vining, Jeff, “Government Information Managers Using Data Mining Must Address Privacy Concerns.” (Gartner: March 1, 2006). The Merriam-Webster Dictionary notes that data mining is “the practice of searching through large amounts of computerized data to find useful patterns or trends.” See <http://www.merriam-webster.com/dictionary/data%20mining>, accessed September 1, 2011. And a recent book on detecting healthcare fraud noted that data mining is the “science of extracting information from large data sets or databases.” See Busch, Rebecca S., *Healthcare Fraud: Auditing and Detection Guide* (John Wiley & Sons: 2008).

<sup>29</sup>See, for example, [GAO-07-293](#), [GAO-05-866](#), and National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment* (Washington, D.C.: 2008).

---

We acknowledge that not all elements of our evaluation framework are applicable to every system; however, we believe that the elements on which we evaluated the systems are valid. For example, we found that the requirement to re-evaluate a system once it is operational is not applicable for the CIDR system because the system is not yet operational. However, other activities, including developing an operational test plan, are applicable to a system in development and we rated them accordingly. Further, we recognize that CIDR fell below certain USCIS acquisition thresholds, and so was not required to complete all of the standard acquisition documents or to be reviewed by the senior review board. However, the program office proposed developing an alternative set of acquisition documents to give senior management insight into the program's development. This alternative set of documents was approved by a senior manager. However, the program never produced a key document that was to document the system's requirements and design. We believe this is a shortfall in the program's development and in the executive review of the program, and that it should be remedied.

Regarding AFI, DHS reported that the system is in development and that GAO's framework is not adequate to evaluate the program while it is in this phase of its life cycle. DHS also noted that assessment grades were not applied uniformly, with some elements involving the PIA rated as "no," "partial," and "not applicable." Similar to the system discussed above, we believe that the elements that we rated were applicable to AFI. The system is being developed using a spiral methodology and its first module was provided authority to operate in November 2010.<sup>30</sup> Therefore, we consider it to have completed the development of a useable module—and to be at a stage where it should have a PIA. Other systems that are in development have completed and published their PIAs, including the CIDR system mentioned above. Further, we disagree that we were inconsistent in the way we rated the agency's PIA. We consistently report that the system does not have a completed PIA. However, because the activities in the framework vary in what is required, there are cases where different ratings are warranted. For example, one element of the framework involves whether or not the agency conducted a privacy impact assessment of the program. Because AFI's PIA has not been completed or approved, we rated this activity as a "no." Another element

---

<sup>30</sup>"Authority to Operate" is an official approval to use a system operationally. In AFI's case, its authority to operate was later modified to note that the agency was not permitted to use the system operationally until after a PIA was completed.



---

seeks an evaluation of the PIA, which cannot be done until it is completed. We rated this as “not applicable” to avoid penalizing the system for something that cannot yet be done. A third element considers whether an independent validation of the system’s privacy impacts and protections has been completed. We rated this element as “partial” because the agency has completed a review of information security controls but not the PIA.

DHS and the component agencies we reviewed also offered technical comments, which we addressed as appropriate.

---

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to interested congressional committees, the Secretary of Homeland Security, and other interested parties. In addition, the report will be available at no charge on GAO’s Web site at <http://www.gao.gov>.

If you or your staffs have any questions on the matters discussed in this report, please contact me at (202) 512-9286 or [pownerd@gao.gov](mailto:pownerd@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs can be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix VI.



David A. Powner  
Director, Information Technology  
Management Issues

---

# Appendix I: Objectives, Scope, and Methodology

---

Our objectives were to (1) assess the Department of Homeland Security's (DHS) policies for evaluating the effectiveness and privacy protections of data-mining systems used for counterterrorism, (2) assess DHS agencies' efforts to evaluate the effectiveness and privacy protections of their counterterrorism-related data-mining systems throughout the systems' life cycles; and (3) describe the challenges facing DHS in implementing an effective framework for evaluating its counterterrorism-related data-mining systems.

To evaluate DHS's policies and practices for evaluating the effectiveness and privacy protections of data-mining systems used for counterterrorism, we developed an assessment framework using a 2008 National Research Council (NRC) report, entitled "Protecting Individual Privacy in the Struggle against Terrorists: a Framework for Program Assessment." This report identifies questions to ask when evaluating the effectiveness and privacy protections of information-based systems—including data-mining systems—at agencies with counter-terrorism responsibilities. We organized NRC's suggested questions into five categories (which we call key elements) and established an assessment framework that can be used as a tool for assessing policies and practices. One component of the framework focuses on agency policies, and the other component focuses on system management practices. We supplemented and refined NRC's suggested questions with best practices identified by GAO and others in areas of IT investment management, sound acquisition practices, and effective privacy protections, as well as concepts and provisions from federal law and guidance.<sup>1</sup> We also had internal subject matter experts review the assessment framework, and we incorporated their comments.

We compared the policy component of our evaluation framework to DHS and selected component agencies' policies on acquisition management, investment management, privacy protections, and information systems

---

<sup>1</sup>See, for example, GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, Version 1.1, [GAO-04-394G](#) (Washington, D.C.: March 2004); *Information Technology: Federal Agencies Need to Strengthen Investment Board Oversight of Poorly Planned and Performing Projects*, [GAO-09-566](#) (Washington, D.C.: June 30, 2009); *Personal Information: Agency and Reseller Adherence to Key Privacy Principles*, [GAO-06-421](#) (Washington, D.C.: Apr. 4, 2006); and *Data Mining: Agencies Have Taken Key Steps to Protect Privacy in Selected Efforts, but Significant Compliance Issues Remain*, [GAO-05-866](#) (Washington, D.C.: Aug. 15, 2005), and Software Engineering Institute, *Capability Maturity Model<sup>®</sup> Integration (CMMI<sup>®</sup>) for Acquisition*, Version 1.2, CMU/SEI-2007-TR-017 (Pittsburgh, Pa., November 2007).

security. The component agencies we selected—Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and U.S. Citizenship and Immigration Services (USCIS)—were chosen because they represent a cross-section of DHS agencies performing data mining and also because they are the system owners for the systems we selected for review. We analyzed the agencies' policies and guidance, and interviewed DHS and component agency officials regarding their policies and any shortfalls we found in their policies.

We compared the practices component of our evaluation framework to six DHS counterterrorism-related data-mining systems. To determine an appropriate group of systems to review, we identified a list of DHS data-mining systems that both support counterterrorism and utilize personal information using DHS budget information on IT investments, publicly posted privacy impact assessments (PIA), reports by GAO and the DHS Inspector General, and interviews with DHS privacy officials. From this list, we selected a nonrandom sample of DHS data-mining systems that involve personal information using the following criteria: (1) a mix of different component agencies; (2) a mix of pattern-based and subject-based data-mining systems; (3) systems in different stages of their life cycles (development and operations); (4) systems with a large cost estimate or other factor that merits inclusion (including importance or risk). For each of the selected systems, we evaluated key privacy and effectiveness documentation, including published PIAs and system of records notices, DHS's reports to Congress under the Federal Agency Data Mining Reporting Act of 2007, and DHS IT investment documentation. We compared these systems' practices to our assessment framework. We interviewed officials from each program regarding their practices as well as any shortfalls we found in their practices. Because we reviewed a nonrandom group of systems, our results are not to be generalized to the agency as a whole or to other agency systems that we did not review. Nonetheless, the information we obtained from our assessment provided us with important information about the policies and practices used by DHS to evaluate data-mining systems.

In comparing both agency policies and practices to the framework, we determined whether individual policy attributes were in place and whether program activities had been completed. We rated each individual policy attribute and program activity as "yes," "partial," "no," or "not applicable." To provide an overall rating for each key element, we summarized the attributes and activities using a five-point scale. That is, the agency or program was determined to meet all, most, about half, a few, or none of the policy attributes and practices for each of the five elements. To do

this, we assigned a point value of 1 for each yes answer, 0 for each no answer, and 0.5 for each that was partially met and averaged each answer based on the number of questions. A question that was not applicable was not counted in the average. Each decision was verified by a second analyst.

To determine challenges facing DHS in implementing an effective framework for evaluating its counterterrorism-related data-mining systems, we evaluated the causes of shortfalls in DHS's policies and efforts to assess its counterterrorism-related data-mining systems' effectiveness and privacy protections. We reviewed GAO, Congressional Research Service, and DHS Inspector General reports that addressed DHS management challenges. We also interviewed program officials to obtain their view on challenges the agency faces in developing policies and assessing its systems.

We conducted our work at DHS and component agency offices in the Washington, D.C., metropolitan area. We conducted this performance audit from August 2010 to September 2011, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

# Appendix II: Fair Information Practices

---

In 1972, in response to growing concern about the harmful consequences that computerized data systems could have on the privacy of personal information, the Secretary of Health, Education, and Welfare commissioned an advisory committee to examine to what extent limitations should be placed on the application of computer technology to record keeping about people. The committee's report proposed a set of principles for protecting the privacy and security of personal information, known as the Fair Information Practices.<sup>1</sup> These practices were intended to address what the committee identified as a poor level of protection afforded to privacy under existing law, and they underlie the major provisions of the Privacy Act, which was enacted the following year.

A revised version of the Fair Information Practices, developed by the Organization for Economic Cooperation and Development (OECD) in 1980, has been widely adopted.<sup>2</sup> This version of the principles was reaffirmed by the organization in a 1998 declaration and further endorsed in a 2006 report.<sup>3</sup> In addition, in 2007, the National Research Council found that the principles of fair information practice for the protection of personal information were still as relevant as they were in 1973.<sup>4</sup> The principles are listed in table 9.

---

<sup>1</sup>Department of Health, Education & Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (Washington, D.C.: 1973).

<sup>2</sup>OECD, *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (Sept. 23, 1980). The OECD plays a prominent role in fostering good governance in the public service and in corporate activity among its 30 member countries. It produces internationally agreed-upon instruments, decisions, and recommendations to promote rules in areas where multilateral agreement is necessary for individual countries to make progress in the global economy.

<sup>3</sup>OECD, *Making Privacy Notices Simple: An OECD Report and Recommendations* (July 24, 2006).

<sup>4</sup>National Research Council of the National Academies, *Engaging Privacy and Information Technology in a Digital Age* (Washington, D.C.: 2007).

**Table 9: Fair Information Practices**

Principle	Description
Collection limitation	The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to those purposes and compatible purposes.
Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Source: Organization for Economic Cooperation and Development.

The Fair Information Practices are, with some variation, the basis of privacy laws and related policies in many countries, including the United States, Germany, Sweden, Australia, and New Zealand, as well as the European Union.<sup>5</sup> They are also reflected in a variety of federal agency policy statements, beginning with an endorsement of the principles by the Department of Commerce in 1981, and including policy statements from the Departments of Justice and Housing and Urban Development, and DHS.<sup>6</sup>

<sup>5</sup>European Union Data Protection Directive (“Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data”) (1995).

<sup>6</sup>See “Report on OECD Guidelines Program,” Memorandum from Bernard Wunder, Jr., Assistant Secretary for Communications and Information, Department of Commerce (Oct. 30, 1981); Global Information Sharing Initiative, U.S. Department of Justice, [www.it.ojp.gov/global](http://www.it.ojp.gov/global) (September 2005); “Homeless Management Information Systems,” U.S. Department of Housing and Urban Development (69 *Federal Register* 45888, July 30, 2004). See also “Options for Promoting Privacy on the National Information Infrastructure,” Information Policy Committee of the National Information Infrastructure Task Force, Office of Information and Regulatory Affairs, Office of Management and Budget (April 1997), and DHS, “Privacy Policy Guidance Memorandum: The Fair Information Practice Principles” (Dec. 29, 2008).

# Appendix III: Detailed Assessment of DHS and Selected Agencies' Policies

Table 10 provides a detailed assessment of DHS and selected component agencies' policies for evaluating the effectiveness and privacy protections of information-based systems. The table is organized according to key elements and attributes of an effective policy for evaluating system effectiveness and privacy impacts.

**Table 10: Detailed Assessment of DHS and Selected Agencies' Policies**

Key policy elements and attributes	DHS	CBP	ICE	USCIS
<i>Ensuring organizational competence</i>	●	◐	●	●
Establish acquisition decision authorities responsible for approving acquisitions as they progress through their life cycle.	Yes	Yes	Yes	Yes
Establish a policy-level chief privacy officer responsible for ensuring compliance with privacy laws, policies, and guidance, and as appropriate, component privacy officials responsible for assisting in this process.	Yes	Yes	Yes	Yes
Require agencies to develop staffing plans that include staff responsible for ensuring a system's effectiveness and privacy protections.	Yes	No	Yes	Yes
Require agencies to train those responsible for the system's privacy and security requirements.	Yes	n/a	n/a	n/a
<i>Evaluating system effectiveness</i>	●	◐	◐	◐
Require evaluations of systems while they are being developed or when they have major changes to ensure consistency with their stated purpose.	Yes	Yes	Yes	Yes
Require evaluations of system effectiveness (including adequate testing and data quality assessments).	Yes	Partial	Partial	Partial
Require an independent assessment of the system's effectiveness (by an entity outside of the program office).	Yes	Yes	Yes	Partial
Require routine re-evaluations of systems once deployed to ensure their continued effectiveness and consistency of purpose.	Yes	Partial	Partial	Partial
<i>Evaluating privacy impacts</i>	●	●	●	●
Require program offices to conduct privacy impact assessments before developing, operating, or making major changes to information systems that process personal information.	Yes	Yes	Yes	Yes
Require privacy assessments to include an evaluation of privacy risks and mitigation strategies, the manner in which data are collected and are to be used, security safeguards, and procedures for an individual to access and request corrections to their personal information. The assessment should also address transparency and accountability.	Yes	n/a	n/a	n/a
Require an independent assessment of a system's privacy impacts and protections (by an entity outside of the program office).	Yes	n/a	n/a	n/a
Require periodic re-evaluations of a system's privacy and security protections.	Yes	n/a	n/a	n/a
<i>Obtaining executive review and authorization of investments</i>	◐	◐	◐	●
Establish investment review boards that provide executive review and authorization to proceed at regular intervals throughout a system's life cycle—including design, development, and operation.	Partial	Partial	Partial	Yes

**Appendix III: Detailed Assessment of DHS and Selected Agencies' Policies**

<b>Key policy elements and attributes</b>	<b>DHS</b>	<b>CBP</b>	<b>ICE</b>	<b>USCIS</b>
Require investment reviews to				
• assess the system's alignment with the agency's goals and mission.	Yes	Yes	Yes	Yes
• ensure that the system is operating as intended.	Yes	Yes	Yes	Yes
• ensure that the system has adequate privacy and security protections in place.	Yes	Yes	Yes	Yes
<i>Providing transparency and external oversight</i>	●	●	●	●
Require regular reviews of operational information systems by non-system owners (such as the CIO and privacy office) to ensure compliance with privacy and effectiveness requirements.	Yes	Yes	Yes	Yes
Ensure that programs report on a system's effectiveness and privacy protections to external overseers, as required.	Yes	n/a	n/a	n/a
Require that information is provided to external overseers (such as a congressionally sponsored oversight board) to allow more intensive scrutiny of a system's privacy protections in cases where public reporting is not required.	Partial	Partial <sup>a</sup>	Partial <sup>a</sup>	Partial <sup>a</sup>

Source: GAO analysis of DHS, CBP, ICE, and USCIS policies and guidance.

**Key**

● = The agency's policies address all of the attributes for this element.

● = The agency's policies address most of the attributes for this element.

● = The agency's policies address about half of the attributes for this element.

● = The agency's policies address a few of the attributes for this element.

○ = The agency's policies address none of the attributes for this element.

Yes = The agency's policies address all of the attribute's characteristics.

Partial = The agency's policies address at least one, but not all, of the attribute's characteristics.

No = The agency's policies do not address any of the attribute's characteristics.

n/a = Certain elements and attributes are not applicable (n/a) at the component agency level because the authority for the relevant policies is at the department level.

<sup>a</sup>While the authority for this attribute is at the departmental level, DHS has only partially addressed this attribute.



---

# Appendix IV: Detailed Assessments of Selected Data-Mining Systems

---

The following sections provide a brief overview of each of the six systems we reviewed, including how well each system's program office addressed each of the five elements (ensuring organizational competence, evaluating the effectiveness of systems, evaluating the privacy protections of systems, obtaining executive review and authorization, and providing appropriate transparency and oversight throughout a system's life cycle). The sections also include a detailed assessment of the activities each program office conducted.

The keys that we used in tables 11 through 16 to convey the results of our assessment are as follows:

## **Program Rankings (Elements):**

- The program office performed all of the activities of this element.
- ◐ The program office performed most of the activities of this element.
- ◑ The program office performed about half of the activities of this element.
- ◒ The program office performed a few of the activities of this element.
- The program office performed none of the activities of this element.

n/a This element is not applicable to the program.

## **Program Rankings (Activities):**

- |         |  |
|---------|--|
| Yes     | The program office has completed the activity                        |
| Partial | The program office has completed some, but not all, of the activity. |
| No      | The program office has not completed the activity                    |
| n/a     | This activity is not applicable to the program.                      |

## Analytical Framework for Intelligence (AFI)

Responsible agency: CBP  
 Life-cycle stage: Under development since 2007  
 Life-cycle cost estimate: Approximately \$180 million  
 System designation: Non-major IT investment  
 PIA: Not yet completed

AFI is to enable CBP intelligence analysts to perform data queries and searches of multiple CBP data sources from a single interface, the results of which are presented in a single platform. This function is called a “federated search.” The data are collected by and maintained in the source systems. In addition, AFI is to provide access and federated search functions to other data sources and systems via interconnections. It is also to provide CBP intelligence analysts with automated tools and capabilities for analysis and visualization, including link analysis, anomaly detection, change detection analysis, temporal analysis, pattern analysis, and predictive modeling of the data and will assist with production management and work flow of intelligence products/reports.

The program office is using a “spiral” form of incremental development and completed a security assessment and production readiness review in November and December 2010, respectively. However, according to agency officials the office was unable to deploy the system because its PIA was not approved as its approval is pending changes to another system’s documentation. AFI is continuing further development while it waits to deploy its initial software release. Table 11 provides a detailed assessment of AFI’s compliance with the system-level evaluation framework.

**Table 11: Detailed Assessment of AFI**

Agency and program office activities	GAO assessment	Description
Ensuring Organizational Competence	●	
Have the established authority for the information system certify key acquisition decisions, including decisions that affect personal data about specific individuals.	Partial	The program has completed a security assessment and has approval of key acquisition documents; however, it does not have documented approvals of the full system and has not completed a PIA.
Ensure, through the agency chief privacy officer (or his/her representative), that the system is in compliance with privacy laws, policies, and guidance.	No	The program office does not yet have an approved PIA.
Assess the program office workforce to determine the skills needed and to identify existing gaps in its ability to fulfill its program effectiveness and privacy responsibilities. Then, ensure the program office is sufficiently staffed to fulfill its responsibilities.	Partial	The program has defined key roles and responsibilities; however, it did not assess workforce gaps in fulfilling its privacy responsibilities.
Provide program staff engaged in developing or using the information system with required security and privacy training.	Yes	The program office performed this activity.

**Appendix IV: Detailed Assessments of  
Selected Data-Mining Systems**

<b>Agency and program office activities</b>	<b>GAO assessment</b>	<b>Description</b>
<i>Evaluating System Effectiveness</i>		
Perform a comprehensive evaluation of the information system's consistency with its articulated purpose.	Yes	The program office performed this activity.
Identify any changes to the system that cause it to deviate from its original purpose and ensure that these changes are approved.	n/a	The system is not yet operational.
Evaluate the system before it is made operational to demonstrate expected effectiveness. In doing so, the evaluation/demonstration should be appropriate, scientifically valid, and sufficient and include documented effectiveness measures.	Partial	The program office completed system acceptance and security testing, and operational testing is ongoing; however, it has not evaluated whether the data in the system are appropriate and reliable, or whether the system is scalable.
Assess the quality of the data to be used in the system.	Partial	The program office has a data management plan that identifies steps for adding new data sources; however, it has not applied this plan to the data already in the system.
Obtain an independent validation of test results (by an entity outside the program office).	Partial	The program office conducted some system testing using independent testers, but has not yet completed an independent validation of test results.
Re-evaluate the system once it is operational to ensure the system continues to be effective and consistent with its intended purpose.	n/a	The system is not yet operational.
Assess system and operator performance with mechanisms for detecting and reporting errors, such as monitoring tools and regular audits.	Partial	The program office has several tools to assist in evaluating the system and detecting problems; however, a key tool for monitoring audit logs is not in place.
<i>Evaluating Program Privacy Impacts</i>		
Conduct a privacy impact assessment for the information system before developing, operating, and making major changes to the system.	No	The program office does not yet have an approved PIA.
Ensure the privacy impact assessment adequately addresses issues such as: privacy risks and actions taken to mitigate those risks; data collections; data uses; information security safeguards; and transparency, redress, and accountability regarding data issues.	n/a	The program office does not yet have an approved PIA.
Obtain an independent validation of the system's privacy impacts and protections (by an entity outside the program office).	Partial	The program office obtained an independent validation of the information security protections of the system; however, it has not yet obtained independent validation of the system's privacy impacts.
Have and use a process to periodically review the effectiveness of the program's privacy and security controls to update privacy impact assessments and system of record notices as appropriate.	Partial	The program office plans to review its security controls every three years or when there are major changes to the system and to install software for monitoring audit logs; however, it does not yet have privacy controls in place.

**Appendix IV: Detailed Assessments of Selected Data-Mining Systems**

<b>Agency and program office activities</b>	<b>GAO assessment</b>	<b>Description</b>
<i>Obtaining Executive Review/Authorization of Investments</i>		
Have the executive review board evaluate the information system at each major phase of development and have these assessments and decisions documented.	Partial	Executive review board members approved key acquisition documents during the development phase; however, there is no documentation of the scope of the board's review.
Examine the system's effectiveness, privacy protections, information security, legal compliance, and alignment with the agency's mission.	No	The program office does not have documentation of the scope of the review board's work.
Track any review board recommendations and concerns until they are fully addressed and closed.	n/a	There is no evidence that the review board has made recommendations to the program.
<i>Providing Transparency and External Oversight</i>		
Perform regular reviews of the information system by external organizations (CIO, privacy office, other) to ensure compliance with privacy and effectiveness requirements.	Partial	The system has been the subject of reviews by the CBP governance board and Enterprise Architecture Board, but has not yet completed the documents required for privacy compliance reviews.
Track corrective actions taken to address recommendations that were raised during regular external reviews until they are closed.	Partial	The program office tracked issues from system development reviews; however, issues from the privacy office are still outstanding.
Provide reports for external oversight and publicly post reports, as required.	No	The program office has not yet publicly posted its PIA or a system of records notice.
Document the legitimate reasons that a program office may not post required reports publicly and demonstrate that it has sought additional levels of scrutiny of the system's privacy protections.	n/a	The program office has not yet completed the required reports for them to be posted publicly.

Source: GAO analysis of DHS and CBP data.

## Automated Targeting System-Passenger Module (ATS-P)

Responsible agency: CBP

Life-cycle stage: Operational (since 1999)

Life-cycle cost estimate: approximately \$460 million (entire ATS system)

System designation: Major IT investment

PIA: Completed 2006, revised in 2007 and 2008. Currently being revised.

ATS collects, analyzes, and disseminates information that is gathered to target, identify, and prevent potential terrorists and terrorist weapons from entering the United States. One major component of this system, ATS-P, compares information in the ATS databases against watch lists, criminal records, warrants, and patterns of suspicious activity identified through past investigations and intelligence. CBP analysts use ATS-P to evaluate travelers prior to their arrival at, or departure from, U.S. ports of entry. According to DHS, the system facilitates decision-making about whether a passenger or crew member should receive additional screening because that person may pose a greater risk for terrorism and related crimes, or other violations of U.S. law.

Table 12 provides a detailed assessment of ATS-P's compliance with the system-level evaluation framework.

**Appendix IV: Detailed Assessments of  
Selected Data-Mining Systems**

**Table 12: Detailed Assessment of ATS-P**

<b>Agency and program office activities</b>	<b>GAO assessment</b>	<b>Description</b>
<i>Ensuring Organizational Competence</i>		
Have the established authority for the information system certify key acquisition decisions, including decisions that affect personal data about specific individuals.	Yes	The program office performed this activity.
Ensure, through the agency chief privacy officer (or his/her representative), that the system is in compliance with privacy laws, policies, and guidance.	Yes	The program office performed this activity.
Assess the program office workforce to determine the skills needed and to identify existing gaps in its ability to fulfill its program effectiveness and privacy responsibilities. Then, ensure the program office is sufficiently staffed to fulfill its responsibilities.	Yes	The program office performed this activity.
Provide program staff engaged in developing or using the information system with required security and privacy training.	Yes	The program office performed this activity.
<i>Evaluating System Effectiveness</i>		
Perform a comprehensive evaluation of the information system's consistency with its articulated purpose.	Partial	The program office has evaluated the system's consistency with the purpose articulated in the PIA. However, because it does not have an approved concept of operations or operational requirements document that describe the way the system is to be used operationally, it has not evaluated the system's consistency with the purpose that would be articulated in those documents.
Identify any changes to the system that cause it to deviate from its original purpose and ensure that these changes are approved.	n/a	The system has not undergone any changes that deviate from its intended purpose.
Evaluate the system before it is made operational to demonstrate expected effectiveness. In doing so, the evaluation/demonstration should be appropriate, scientifically valid, and sufficient and include documented effectiveness measures.	n/a	The system has been operational for over a decade; therefore, pre-operational effectiveness evaluations are not applicable.
Assess the quality of the data to be used in the system.	No	The program office has not conducted an assessment of data quality for the system.
Obtain an independent validation of test results (by an entity outside the program office).	n/a	The program office has not performed recent testing; therefore, an independent validation is not applicable.
Re-evaluate the system once it is operational to ensure the system continues to be effective and consistent with its intended purpose.	Partial	The program office performs ongoing monitoring of the system's effectiveness; however, it has not assessed the system's consistency with its intended purpose.
Assess system and operator performance with mechanisms for detecting and reporting errors, such as monitoring tools and regular audits.	Yes	The program office performed this activity.

**Appendix IV: Detailed Assessments of  
Selected Data-Mining Systems**

<b>Agency and program office activities</b>	<b>GAO assessment</b>	<b>Description</b>
<b><i>Evaluating Program Privacy Impacts</i></b>		
Conduct a privacy impact assessment for the information system before developing, operating, and making major changes to the system.	Yes	The program office performed this activity.
Ensure the privacy impact assessment adequately addresses issues such as: privacy risks and actions taken to mitigate those risks; data collections; data uses; information security safeguards; and transparency, redress, and accountability regarding data issues.	Yes	The program office addressed this activity.
Obtain an independent validation of the system's privacy impacts and protections (by an entity outside the program office).	Yes	The program office obtained an independent validation of privacy impacts and protections.
Have and use a process to periodically review the effectiveness of the program's privacy and security controls to update privacy impact assessments and system of record notices as appropriate.	Yes	The program office performed this activity.
<b><i>Obtaining Executive Review/Authorization of Investments</i></b>		
Have the executive review board evaluate the information system at each major phase of development and have these assessments and decisions documented.	n/a	ATS-P has not had any new investments in the past decade.
Examine the system's effectiveness, privacy protections, information security, legal compliance, and alignment with the agency's mission.	n/a	ATS-P has not had any new investments in the past decade.
Track any review board recommendations and concerns until they are fully addressed and closed.	n/a	ATS-P has not had any new investments in the past decade.
<b><i>Providing Transparency and External Oversight</i></b>		
Perform regular reviews of the information system by external organizations (CIO, privacy office, other) to ensure compliance with privacy and effectiveness requirements.	Yes	The program office performed this activity.
Track corrective actions taken to address recommendations that were raised during regular external reviews until they are closed.	Yes	The program office performed this activity.
Provide reports for external oversight and publicly post reports, as required.	Yes	The program office performed this activity.
Document legitimate reasons that a program office may not post required reports publicly and demonstrate that it has sought additional levels of scrutiny of the system's privacy protections.	n/a	The agency posted all required reports.

Source: GAO analysis of DHS and CBP data.

## Citizenship Immigration Data Repository (CIDR)

Responsible agency: USCIS  
 Life-cycle stage: under development (since 2008)  
 Life-cycle cost estimate: \$372,737.00  
 System designation: Non-major IT investment  
 Next major milestone: Security accreditation  
 PIA: Completed October 2010

CIDR is a subject-based data-mining system that is to use classified parameters to search for more information about an individual or group of people. CIDR is to be hosted on DHS's classified networks, in order to make information from USCIS benefits administration systems available for querying by authorized USCIS analysts. These analysts expect to use CIDR to: (1) assess USCIS applications for indications of immigration fraud and national security concerns, (2) detect possible fraud and misuse of immigration information or position by USCIS employees for personal gain or by coercion, and (3) respond to requests for information from DHS and federal intelligence and law enforcement community members that are based on classified criteria. CIDR currently holds an extract of data from one of USCIS's key benefits administration systems and is to eventually contain data from the other benefit administration systems.

Table 13 provides a detailed assessment of CIDR compliance with the system-level evaluation framework.

**Table 13: Detailed Assessment of CIDR**

Agency and program office activities	GAO assessment	Description
<i>Ensuring Organizational Competence</i>		
Have the established authority for the information system certify key acquisition decisions, including decisions that affect personal data about specific individuals.	Partial	The program office has an approved PIA. Also, because of its size, selected acquisition requirements were not required. However, key documents that were required were never produced or approved.
Ensure, through the agency chief privacy officer (or his/her representative), that the system is in compliance with privacy laws, policies, and guidance.	Yes	The program office performed this activity.
Assess the program office workforce to determine the skills needed and to identify existing gaps in its ability to fulfill its program effectiveness and privacy responsibilities. Then, ensure the program office is sufficiently staffed to fulfill its responsibilities.	n/a	The program office is extremely small. As a result, a workforce analysis is not warranted.
Provide program staff engaged in developing or using the information system with required security and privacy training.	Yes	The program office performed this activity.
<i>Evaluating System Effectiveness</i>		
Perform a comprehensive evaluation of the information system's consistency with its articulated purpose.	Yes	The program office performed this activity.
Identify any changes to the system that cause it to deviate from its original purpose and ensure that these changes are approved.	n/a	The system has not undergone any changes that deviate from its intended purpose.

**Appendix IV: Detailed Assessments of  
Selected Data-Mining Systems**

<b>Agency and program office activities</b>	<b>GAO assessment</b>	<b>Description</b>
Evaluate the system before it is made operational to demonstrate expected effectiveness. In doing so, the evaluation/demonstration should be appropriate, scientifically valid, and sufficient and include documented effectiveness measures.	Partial	The program office has performed developmental testing, but has not yet developed an operational test plan.
Assess the quality of the data to be used in the system	Yes	The program office performed this activity.
Obtain an independent validation of test results (by an entity outside the program office).	n/a	The program office must complete development before performing this activity.
Re-evaluate the system once it is operational to ensure the system continues to be effective and consistent with its intended purpose.	n/a	The system is not yet operational.
Assess system and operator performance, with mechanisms for detecting and reporting errors such as monitoring tools and regular audits.	n/a	The system is not yet operational.
<b><i>Evaluating Program Privacy Impacts</i></b>		
Conduct a privacy impact assessment for the information system before developing, operating, and making major changes to the system.	Yes	The program performed this activity.
Ensure the privacy impact assessment adequately addresses issues such as: privacy risks and actions taken to mitigate those risks; data collections; data uses; information security safeguards; and transparency, redress, and accountability regarding data issues.	Yes	The system has taken steps that support information security and protect privacy; however, information security certification and accreditation will not be obtained until after development is complete.
Obtain an independent validation of the system's privacy impacts and protections (by an entity outside the program office).	n/a	The system has taken steps that support information security and protect privacy; however, information security certification and accreditation will not be obtained until after development is complete.
Have and use a process to periodically review the effectiveness of the program's privacy and security controls to update privacy impact assessments and system of record notices as appropriate.	n/a	The program office must complete development activities before this activity is relevant
<b><i>Obtaining Executive Review/Authorization of Investments</i></b>		
Have the executive review board evaluate the information system at each major phase of development and have these assessments and decisions documented.	Partial	An executive review board approved the initiation of CIDR development; however, there is no evidence of subsequent executive reviews.
Examine the system's effectiveness, privacy protections, information security, legal compliance, and alignment with the agency's mission.	Partial	An executive review board examined the system/s privacy protections, legal compliance and mission, but has not yet examined effectiveness or information security.
Track any review board recommendations and concerns until they are fully addressed and closed.	No	The executive review board approved the business case with two conditions; however, there is no evidence the conditions were tracked until satisfied.



**Appendix IV: Detailed Assessments of Selected Data-Mining Systems**

<b>Agency and program office activities</b>	<b>GAO assessment</b>	<b>Description</b>
<i>Providing Transparency and External Oversight</i>		
Perform regular reviews of the information system by external organizations (CIO, privacy office, other) to ensure compliance with privacy and effectiveness requirements.	Partial	DHS's privacy office has reviewed and approved the system's PIA and the executive board approved the program's business case; however, there is no evidence of subsequent reviews.
Track corrective actions taken to address recommendations that were raised during regular external reviews until they are closed.	Partial	The program office tracked and addressed privacy office questions; however, the program has not yet undergone other regular external reviews since it is still under development.
Provide reports for external oversight and publicly post reports, as required.	Yes	The program office performed this activity.
Document the legitimate reasons that a program office may not post required reports publicly and demonstrate that it has sought additional levels of scrutiny of the system's privacy protections.	n/a	The agency posted all required reports.

Source: GAO analysis of DHS and USCIS data.

**Data Analysis and Research for Trade Transparency System (DARTTS)**

Responsible agency: ICE  
 Life-cycle stage: Operational since 2005  
 Life-cycle cost estimate: approximately \$24 million  
 System designation: Non-major IT investment  
 PIA: Completed in 2008, revised in 2010

DARTTS is a pattern-based data-mining system used to analyze trade and financial data in order to identify possible illegal activity based on anomalies in trade activities. ICE agents and analysts use DARTTS to conduct three main types of analyses: (1) international trade discrepancy analysis of U.S. and foreign import/export data; (2) unit price analysis of trade pricing data for over- or under-pricing of goods; and (3) financial data analysis, such as suspicious financial activity reports.

Table 14 provides a detailed assessment of DARTTS's compliance with the system-level evaluation framework.

**Appendix IV: Detailed Assessments of  
Selected Data-Mining Systems**

**Table 14: Detailed Assessment of DARTTS**

<b>Agency and program office activities</b>	<b>GAO assessment</b>	<b>Description</b>
<b><i>Ensuring Organizational Competence</i></b>		
Have the established authority for the information system certify key acquisition decisions, including decisions that affect personal data about specific individuals.	Yes	The program office performed this activity.
Ensure, through the agency chief privacy officer (or his/her representative), that the system is in compliance with privacy laws, policies, and guidance.	Yes	The program office performed this activity.
Assess the program office workforce to determine the skills needed and to identify existing gaps in its ability to fulfill its program effectiveness and privacy responsibilities. Then, ensure the program office is sufficiently staffed to fulfill its responsibilities.	Yes	The program office performed this activity.
Provide program staff engaged in developing or using the information system with required security and privacy training.	Yes	The program office performed this activity.
<b><i>Evaluating System Effectiveness</i></b>		
Perform a comprehensive evaluation of the information system's consistency with its articulated purpose.	Yes	The program office performed this activity.
Identify any changes to the system that cause it to deviate from its original purpose and ensure that these changes are approved.	n/a	The system has not undergone any changes that deviate from its intended purpose.
Evaluate the system before it is made operational to demonstrate expected effectiveness. In doing so, the evaluation/demonstration should be appropriate, scientifically valid, and sufficient and include documented effectiveness measures.	Partial	The program office analyzed the system's capabilities through development testing and evaluated the effectiveness of the system's security controls; however, the program office has not established performance measures for the system.
Assess the quality of the data to be used in the system.	Partial	The program office has mechanisms in place to correct source data; however, it has not assessed the system's data quality.
Obtain an independent validation of test results (by an entity outside the program office).	Yes	The program office obtained an independent validation of test results.
Re-evaluate the system once it is operational to ensure the system continues to be effective and consistent with its intended purpose.	Partial	The system has been reviewed during periodic program management reviews; however, operational evaluations of the system are limited without performance measures.
Assess system and operator performance, with mechanisms for detecting and reporting errors such as monitoring tools and regular audits.	Partial	The program office receives informal feedback from users, but does not have documented performance measures.
<b><i>Evaluating Program Privacy Impacts</i></b>		
Conduct a privacy impact assessment for the information system before developing, operating, and making major changes to the system.	Yes	The program office performed this activity.

**Appendix IV: Detailed Assessments of Selected Data-Mining Systems**

<b>Agency and program office activities</b>	<b>GAO assessment</b>	<b>Description</b>
Ensure the privacy impact assessment adequately addresses issues such as: privacy risks and actions taken to mitigate those risks; data collections; data uses; information security safeguards; and transparency, redress, and accountability regarding data issues.	Yes	The program office performed this activity.
Obtain an independent validation of the system's privacy impacts and protections (by an entity outside the program office).	Yes	The program office obtained an independent validation of privacy impacts and protections.
Have and use a process to periodically review the effectiveness of the program's privacy and security controls to update privacy impact assessments and system of record notices as appropriate.	Yes	The program office performed this activity.
<b><i>Obtaining Executive Review/Authorization of Investments</i></b>		
Have the executive review board evaluate the information system at each major phase of development and have these assessments and decisions documented.	Partial	The agency CIO evaluated the system multiple times during the system's development; however, according to ICE, the post-implementation review was limited because this was a new process.
Examine the system's effectiveness, privacy protections, information security, legal compliance, and alignment with the agency's mission.	Partial	The agency CIO evaluated the system's effectiveness multiple times during the system's development; however, these reviews did not address key factors, including defined business objectives, performance measures, and performance testing.
Track any review board recommendations and concerns until they are fully addressed and closed.	Partial	The program office tracked security concerns to closure; however, it did not track other concerns to closure, including concerns about requirements, system scalability, and development test plans.
<b><i>Providing Transparency and External Oversight</i></b>		
Perform regular reviews of the information system by external organizations (CIO, Privacy office, other) to ensure compliance with privacy and effectiveness requirements.	Partial	DHS's privacy office reports to Congress annually on the status of DARTTS, and the program office is subject to periodic management reviews of the program; however, program reviews are limited because the program office does not have performance measures for the system.
Track corrective actions taken to address recommendations that were raised during regular external reviews until they are closed.	n/a	No corrective actions have been identified.
Provide reports for external oversight and publicly post reports, as required.	Yes	The program office performed this activity.
Document the legitimate reasons that a program office may not post required reports publicly and demonstrate that it has sought additional levels of scrutiny of the system's privacy protections.	n/a	The agency posted all required reports.

Source: GAO analysis of DHS and ICE data.

## ICE Pattern Analysis and Information Collection (ICEPIC)

Responsible agency: ICE

Life-cycle stage: Mixed (in operation since 2008, with plans for new development under review)

Life-cycle cost estimate: approximately \$150 million

System designation: Major IT investment

PIA: Original completed in January 2008; the program recently started revising its PIA to reflect a system change made in March 2008

ICEPIC provides law enforcement agents and analysts a set of information analysis tools to identify non-obvious relationship patterns among individuals and organizations that are indicative of violations of customs and immigration laws or terrorist threats. ICE agents and analysts develop leads and intelligence to support new or ongoing investigations based on the relationships identified using ICEPIC. One component of this system is a Web service (called the Law Enforcement Information Sharing Service) which links federal, state, and local law enforcement sharing partners to ICEPIC's searchable data sets.

The ICE program office plans to increase the number of system users and improve the system's functionality, but these new development plans have not yet been approved.

Table 15 provides a detailed assessment of ICEPIC's compliance with the system-level evaluation framework.

**Table 15: Detailed Assessment of ICEPIC**

Agency and program office activities	GAO assessment	Description
<i>Ensuring Organizational Competence</i>		
Have the established authority for the information system certify key acquisition decisions, including decisions that affect personal data about specific individuals.	Partial	Future system development plans are being reviewed by acquisition authorities; however, the program office acknowledged that key system acquisition reviews did not occur before the system was deployed because there was no process for conducting these reviews.
Ensure, through the agency chief privacy officer (or his/her representative), that the system is in compliance with privacy laws, policies, and guidance.	No	The program office completed and the DHS privacy office approved a PIA for the system. However, one component of the operational system that allows information sharing outside the agency has been operational since 2008 but is not included in the PIA, and a revised PIA that includes this component was only recently started. Therefore, the system is not fully compliant with privacy laws and guidance.
Assess the program office workforce to determine the skills needed and to identify existing gaps in its ability to fulfill its program effectiveness and privacy responsibilities. Then, ensure the program office is sufficiently staffed to fulfill its responsibilities.	Partial	The program office assessed workforce skills and identified gaps; however, program officials noted that key positions have not yet been filled.
Provide program staff engaged in developing or using the information system with required security and privacy training.	Yes	The program office performed this activity.

**Appendix IV: Detailed Assessments of  
Selected Data-Mining Systems**

<b>Agency and program office activities</b>	<b>GAO assessment</b>	<b>Description</b>
<i>Evaluating System Effectiveness</i>		
Perform a comprehensive evaluation of the information system's consistency with its articulated purpose.	Yes	The program office performed this activity.
Identify any changes to the system that cause it to deviate from its original purpose and ensure that these changes are approved.	n/a	The system has not undergone any changes that deviate from its intended purpose.
Evaluate the system before it is made operational to demonstrate expected effectiveness. In doing so, the evaluation/demonstration should be appropriate, scientifically valid, and sufficient and include documented effectiveness measures.	Partial	The program office assessed the effectiveness of a key system component; however, the office was unable to provide evidence that it conducted effectiveness evaluations before the system was deployed.
Assess the quality of the data to be used in the system.	Partial	The program office has mechanisms to assess data quality including a means for users to provide feedback on the system; however, users have raised concerns about the system's accuracy. The program office is now taking steps to resolve these concerns.
Obtain an independent validation of test results (by an entity outside the program office).	Partial	The program office obtained an independent review of test results for the system component that was tested; however, it was unable to provide evidence that it obtained an independent review of test results before the system was deployed.
Re-evaluate the system once it is operational to ensure the system continues to be effective and consistent with its intended purpose.	Yes	The program office performed this activity.
Assess system and operator performance, with mechanisms for detecting and reporting errors such as monitoring tools and regular audits.	Yes	The program office performed this activity.
<i>Evaluating Program Privacy Impacts</i>		
Conduct a privacy impact assessment for the information system before developing, operating, and making major changes to the system.	Partial	The program office completed and the DHS Privacy Office approved a PIA for the system. However, a revised PIA that reflects changes to the system component was only recently started.
Ensure the privacy impact assessment adequately addresses issues such as: privacy risks and actions taken to mitigate those risks; data collections; data uses; information security safeguards; and transparency, redress, and accountability regarding data issues.	Partial	The PIA addresses data collections, information security safeguards, and redress and accountability regarding data issues; however, because it has not yet been updated to reflect the operational system, it only partially addresses data uses and transparency.
Obtain an independent validation of the system's privacy impacts and protections (by an entity outside the program office).	Partial	The program office obtained an independent validation of its 2008 PIA, but has not yet obtained validation of a revised PIA.

**Appendix IV: Detailed Assessments of  
Selected Data-Mining Systems**

<b>Agency and program office activities</b>	<b>GAO assessment</b>	<b>Description</b>
Have and use a process to periodically review the effectiveness of the program's privacy and security controls to update privacy impact assessments and system of record notices as appropriate.	Partial	The program office has a process for periodically reviewing the system's privacy and security controls; however, the process is not always followed. The program recently began the process of updating a PIA for a system modification that was made 3 years ago.
<b>Obtaining Executive Review/Authorization of Investments</b>		
Have the executive review board evaluate the information system at each major phase of development and have these assessments and decisions documented.	Partial	There are planned acquisition reviews for future enhancements to the system; however, key acquisition life-cycle reviews did not occur before the system was deployed because there was no process for conducting these reviews.
Examine the system's effectiveness, privacy protections, information security, legal compliance, and alignment with the agency's mission.	Partial	Planned acquisition reviews are expected to include system effectiveness, privacy, and security; however, these reviews did not occur before the system was deployed because there was no process for conducting these reviews.
Track any review board recommendations and concerns until they are fully addressed and closed.	n/a	Key acquisition reviews did not occur prior to the system's deployment.
<b>Providing Transparency and External Oversight</b>		
Perform regular reviews of the information system by external organizations (CIO, privacy office, other) to ensure compliance with privacy and effectiveness requirements.	No	While external organizations have performed regular reviews of the systems effectiveness and privacy protections, these reviews overlooked changes made to the system's operations in March 2008. The program office only recently began drafting a revised privacy assessment to reflect these changes.
Track corrective actions taken to address recommendations that were raised during regular external reviews until they are closed.	Yes	The program office performed this activity.
Provide reports for external oversight and publicly post reports, as required.	Partial	The program office has provided reports for external oversight that have been posted publicly. However, a revised PIA reflecting system changes made in March 2008 was only recently begun and, therefore, has not been publicly posted.
Document the legitimate reasons that a program office may not post required reports publicly and demonstrate that it has sought additional levels of scrutiny of the system's privacy protections.	n/a	The program office has posted its original PIA, and plans to publish its revised PIA once it is approved.

Source: GAO analysis of DHS and ICE data.

## TECS Modernization (TECS-Mod)

**Responsible agencies:** CBP (and ICE)  
**Life-cycle stage:** Mixed (TECS is operational and TECS-Mod is in development)  
**Life-cycle cost estimate:** \$1.1 billion (CBP's TECS-Mod only)  
**System designation:** Major IT investment  
**Major milestones:** Deployment is scheduled from 2011 through 2015  
**PIA:** Partial PIA completed December 2010

While the Department of the Treasury deployed the TECS system in the 1980s, DHS is now responsible for the system and it is operated by CBP. TECS is a mainframe-based system used to disseminate data to 20 federal agencies in support of border enforcement and the inspection and security screening of travelers and cargo entering or exiting the U.S. The system processes over 2 million transactions daily.

TECS-Mod is a joint effort between CBP and ICE, with each agency expected to develop system capabilities to support their respective missions and deliver those capabilities in coordination with each other. We evaluated CBP's portion of TECS-Mod, which is expected to improve search capabilities, enhance data integration, provide the flexibility necessary to respond to evolving threats, and eliminate older, unreliable technology. CBP plans to execute its modernization program in five segments and has begun deployment of the first segment. ICE's portion of TECS-Mod is still in a planning stage and development has yet to begin.

Table 16 provides a detailed assessment of TECS-Mod's compliance with the system-level evaluation framework.

**Table 16: Detailed Assessment of CBP's TECS-Mod**

Agency and program office activities	GAO assessment	Description
<i>Ensuring Organizational Competence</i>		
Have the established authority for the information system certify key acquisition decisions, including decisions that affect personal data about specific individuals.	Yes	The program office performed this activity.
Ensure, through the agency chief privacy officer (or his/her representative), that the system is in compliance with privacy laws, policies, and guidance.	Yes	The program office performed this activity.
Assess the program office workforce to determine the skills needed and to identify existing gaps in its ability to fulfill its program effectiveness and privacy responsibilities. Then, ensure the program office is sufficiently staffed to fulfill its responsibilities.	Yes	The program office performed this activity.
Provide program staff engaged in developing or using the information system with required security and privacy training.	Yes	The program office performed this activity.
<i>Evaluating System Effectiveness</i>		
Perform a comprehensive evaluation of the information system's consistency with its articulated purpose.	Yes	The program office performed this activity.

**Appendix IV: Detailed Assessments of  
Selected Data-Mining Systems**

<b>Agency and program office activities</b>	<b>GAO assessment</b>	<b>Description</b>
Identify any changes to the system that cause it to deviate from its original purpose and ensure that these changes are approved.	Yes	The program office performed this activity.
Evaluate the system before it is made operational to demonstrate expected effectiveness. In doing so, the evaluation/demonstration should be appropriate, scientifically valid, and sufficient and include documented effectiveness measures.	Partial	The program performed operational tests of the system to demonstrate its effectiveness; however, the tests could not determine the system's effectiveness against all documented measures. In several cases, the test reports indicated additional capabilities needed to be completed before they could be evaluated.
Assess the quality of the data to be used in the system.	Yes	The program office performed this activity.
Obtain an independent validation of test results (by an entity outside the program office).	Yes	The program office obtained an independent validation of test results.
Re-evaluate the system once it is operational to ensure the system continues to be effective and consistent with its intended purpose.	n/a	It is too early to re-evaluate the system, since the first segment is now being deployed.
Assess system and operator performance, with mechanisms for detecting and reporting errors such as monitoring tools and regular audits.	Partial	The program office has defined performance metrics for the system and has mechanisms for reporting errors, but has not performed recurring operational assessments.
<b><i>Evaluating Program Privacy Impacts</i></b>		●
Conduct a privacy impact assessment for the information system before developing, operating, and making major changes to the system.	Partial	The program has completed a PIA that addresses several, but not all of the TECS-Mod program segments. A PIA covering the remaining segments is not yet complete.
Ensure the privacy impact assessment adequately addresses issues such as: privacy risks and actions taken to mitigate those risks; data collections; data uses; information security safeguards; and transparency, redress, and accountability regarding data issues.	Partial	The PIA addresses privacy risks, data collections, information security safeguards, transparency, and redress; however, it only partially addresses data uses and accountability on data issues because the program has not evaluated the accuracy of its results.
Obtain an independent validation of the system's privacy impacts and protections (by an entity outside the program office).	Yes	The program office obtained an independent validation of privacy impacts and protections.
Have and use a process to periodically review the effectiveness of the program's privacy and security controls to update privacy impact assessments and system of record notices as appropriate.	Partial	The program office has a process to evaluate the effectiveness of the system's security controls; however, it has not yet completed all PIAs and therefore has not updated its privacy controls.
<b><i>Obtaining Executive Review/Authorization of Investments</i></b>		●
Have the executive review board evaluate the information system at each major phase of development and have these assessments and decisions documented.	Yes	The program office performed this activity.



**Appendix IV: Detailed Assessments of Selected Data-Mining Systems**

<b>Agency and program office activities</b>	<b>GAO assessment</b>	<b>Description</b>
Examine the system's effectiveness, privacy protections, information security, legal compliance, and alignment with the agency's mission.	Partial	An executive review board examined the system's effectiveness measures, privacy protections, information security, legal compliance, and mission alignment. However, the acquisition plan that would be used to evaluate system effectiveness and alignment with the agency's mission was incomplete, thereby limiting the effectiveness of the executive review.
Track any review board recommendations and concerns until they are fully addressed and closed.	Yes	The program office performed this activity.
<i>Providing Transparency and External Oversight</i>	●	
Perform regular reviews of the information system by external organizations (CIO, Privacy office, other) to ensure compliance with privacy and effectiveness requirements.	Yes	The program office performed this activity.
Track corrective actions taken to address recommendations that were raised during regular external reviews until they are closed.	Yes	The program office performed this activity.
Provide reports for external oversight and publicly post reports, as required.	Partial	The program office completed and publicly posted a PIA that addresses several, but not all, of the TECS-Mod program segments. A PIA covering the remaining segments is not yet complete.
Document the legitimate reasons that a program office may not post required reports publicly and demonstrate that it has sought additional levels of scrutiny of the system's privacy protections.	n/a	The agency posted all required reports.

Source: GAO analysis of DHS and CBP data.

# Appendix V: Comments from the Department of Homeland Security

U.S. Department of Homeland Security  
Washington, DC 20528



August 19, 2011

David A. Powner  
Director, Information Technology Management Issues  
441 G Street, NW  
U.S. Government Accountability Office  
Washington, DC 20548

Re: Draft Report GAO-11-742, "DATA MINING: DHS Needs to Improve Executive Oversight of Systems Supporting Counterterrorism"

Dear Mr. Powner:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note the report's positive acknowledgement of DHS's progress in addressing GAO's concerns on acquisition management challenges, data mining systems, and privacy concerns identified in prior reviews. DHS is committed to continuing efforts to ensure that Components and programs are in compliance with acquisition processes, requirements, and privacy policies so that data mining systems are adequately reviewed, deliver required capabilities, appropriately protect individual privacy, and maintain appropriate transparency to the public.

As a threshold matter, we believe the statutory basis for the definition of "data mining" DHS uses in contrast to the broader definition employed by GAO for the purpose of this report, requires additional discussion and clarification, which we provide here. Specifically, for DHS and other federal agencies, the *Federal Agency Data Mining Reporting Act of 2007* defines data mining, in relevant part, as pattern-based queries, searches, or other analyses of electronic databases conducted to discover predictive patterns or anomalies indicative of criminal or terrorist activity<sup>1</sup>. Subject-based queries are explicitly excluded. GAO's

<sup>1</sup> The statutory definition of data mining in whole:

DATA MINING.—The term "data mining" means a program involving pattern-based queries, searches, or other analyses of 1 or more electronic databases, where—

(A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;

(B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and

(C) the purpose of the queries, searches, or other analyses is not solely—

(i) the detection of fraud, waste, or abuse in a Government agency or program; or

definition, nonetheless, includes both pattern-based and subject-based queries, searches, and analyses—a substantial expansion of the statutory definition applied by the Department. In fact, GAO’s definition is broad enough to capture nearly every system of records utilized by DHS.

GAO’s use of such a broad definition could have an unintended consequence of leaving readers with the impression that data mining is far more prevalent at DHS than the Department discloses in its Annual Data Mining Report, required under the Data Mining Reporting Act. While GAO is free to adopt any definition it chooses for data mining, the report could have been clearer about both the statutory definition that DHS is required to follow and the fact that GAO’s chosen definition is much broader. An explanation is attempted in a footnote that reads:

DHS does not refer to its subject-based data mining systems as “data mining systems.” Instead, the department only uses the term “data mining” to refer to its pattern-based data mining systems (as defined in the 2007 Data Mining Reporting Act)<sup>2</sup>.

This passage, however, can easily be understood to mean that “pattern-based data mining systems” are defined by the Act. But, only “data mining” is defined by the Act and it is defined only as pattern-based queries, et al. – again, subject-based queries are explicitly excluded. Without this clarification, the footnote’s statement that DHS simply does not “refer” to its subject-based data mining as data mining only reinforces the ambiguity.

DHS would have preferred that GAO use a definition of data mining for this report, consistent with the congressional definition provided in the *Data Mining Reporting Act*. Short of that, the Department believes the report could have been clearer about the statutory definition DHS is required to use and how GAO’s definition greatly expands on the statutory framework for evaluating and reporting on the Department’s data-mining activities.

The draft report contained five recommendations, with which DHS concurs. Specifically, GAO recommended that the Secretary of Homeland Security direct:

**Recommendation 1:** the Chief Information Officer and Chief Procurement Officer to work with their counterparts at Component agencies to ensure the consistency of Component agencies policies with DHS corporate policies and proposed improvements to those policies, including requiring data quality assessments and re-evaluations of operational systems and establishing investment review boards with clearly defined structures and thresholds for system review.

**Response:** Concur. *The Homeland Security Act of 2002*, as amended (Homeland Security Act), expressly authorizes the Department “to use data mining, among other analytical tools, in furtherance of its mission”<sup>3</sup>. The DHS Office of the Chief Information Officer (OCIO)

---

(ii) the security of a Government computer system.

42 U.S.C. § 2000ee-3 (emphasis added).

<sup>2</sup> Report at 9, n.6.

<sup>3</sup> The Act states that, “[s]ubject to the direction and control of the Secretary, the responsibilities of the Under Secretary for Information Analysis and Infrastructure Protection, shall be as follows . . . To establish and utilize, in conjunction with the chief information officer of the Department, a secure communications and information technology infrastructure, including

exercises this authority to engage in data mining in the programs discussed in this GAO Audit report, all of which have been reviewed by the DHS Chief Privacy Officer for potential and actual impact on privacy. DHS OCIO and DHS Privacy use three main documents related to privacy compliance: (1) a Privacy Threshold Analysis (PTA)<sup>4</sup>; (2) a Privacy Impact Assessment (PIA); and (3) a System of Record Notice (SORN)<sup>5</sup>. PTAs, PIAs, and SORNs serve the common purpose of identifying and documenting areas of privacy focus for OCIO major Information Technology (IT) investment programs, IT systems, and collections of Personally Identifiable Information (PII).

The Chief Privacy Officer's authority for reviewing DHS data mining activities is derived from three principal sources of authority: the *Privacy Act of 1974*, as amended (Privacy Act); the *E-Government Act of 2002* (E-Government Act); and section 222 of the Homeland Security Act, which states, in part, that the Chief Privacy Officer is responsible for "assuring that the [Department's] use of technologies sustains, and does not erode, privacy protections relating to the use, collection, and disclosure of personal information." The DHS Privacy Office serves as the steward of section 222 of the Homeland Security Act. The Office also ensures that the Department complies with the Privacy Act, the *Freedom of Information Act*, the E-Government Act, and the numerous laws, Executive Orders, court decisions, and Departmental policies that protect the collection, use, and disclosure of personal and Departmental information.

The Secretary of Homeland Security tasked the DHS OCIO and the DHS Component OCIOs [Components] with the responsibility for maintaining the security and integrity of electronic data and ensuring that data is appropriately shared. This includes administering privacy requirements with respect to electronic data and compliance with information security and records management requirements. DHS OCIO works in connection with the DHS Privacy Office to ensure that corporate policies are in alignment with Privacy Office policies, and that these policies are distributed to the Components for consistency. In furtherance, OCIO and the Privacy Office require Components with programs using PII to complete federally mandated privacy documentation consistent with a PIA<sup>6</sup>, as required by the E-Government Act, the SORN, and the Privacy Act. DHS IT investments that use PII issue PIAs and SORNs, including all DHS data mining systems.

Information collected and maintained by the Components is critical to DHS counterterrorism missions. Therefore, the Components, and DHS as a whole, are responsible for defining and documenting data-mining processes, sources, and flow of data for the organization and safeguarding such documentation for retrieval, review, and reuse.

---

data mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate." 6 U.S.C. § 121(d)(13).

<sup>4</sup> The PTA is the first document completed by a DHS Component seeking to implement or modify a system, program, technology, project, or rulemaking. The PTA identifies whether the system, program, technology, or project is privacy sensitive and thus requires additional privacy compliance documentation such as a PIA or SORN.

<sup>5</sup> SORNs provide notice to the public regarding Privacy Act information maintained in an agency system of records, as well as insight into how information is used, retained, and may be corrected. The Program Manager works with the component privacy officer and component counsel to write a SORN and submit it to the DHS Privacy Office compliance group for review and approval by the Chief Privacy Officer.

<sup>6</sup> A PIA is a tool that examines the privacy impact of IT systems, programs, technologies, projects, or rule-makings. The PIA is the method by which DHS and Components work with the DHS Privacy Office's Compliance Group to review system management activities in key areas such as security and how information is collected, used, and shared.

DHS uses technologies, programs, and systems that involve the acquisition, use, retention, or sharing of information about individuals to fight terrorism or serve other important national goals. These systems are diverse requiring specialized analytical skills<sup>7</sup> to interpret random output or pattern recognition data, as well as to ensure that basic American values are not compromised when collecting, analyzing and deciding mitigation actions on the basis of data output. DHS considers these systems to be “information-based” programs.

As DHS evolves, it faces challenges in maintaining data integrity, assuring successful system integration and operation and adhering to privacy compliance. DHS Corporate is aware that the Components’ policies must remain in-sync to retain completeness, integrity, accessibility, and security in continuance of national laws and regulations. Therefore, DHS Corporate schedules regular acquisition investment review meetings with Component CIOs and Program Managers in continuation of discussions on new system development or updated system migration as part of DHS’s compliance documentation process.

**Recommendation 2:** the Chief Information Officer and Chief Procurement Officer to work with their counterparts at Component Agencies to identify steps to mitigate challenges related to the review and oversight of operational systems and to DHS’s changing policy requirements and determine clear corrective actions, taking into account the impact on Components and on individual program managers.

**Response:** Concur. The DHS Privacy Office participated in a Department of Defense Technology and Privacy Advisory Committee which produced a research document in 2004 titled *The Report of the Technology and Privacy Advisory Committee: Safeguarding Privacy in the Fight against Terrorism*<sup>8</sup>. The Committee was tasked to develop safeguards to ensure that the application of this or any like technology developed within DOD is carried out in accordance with U.S. law and American values related to privacy. In the report, the role of data mining and behavioral surveillance technologies in counterterrorism programs was examined to provide a framework for making decisions about deploying and evaluating information-based programs on the basis of their effectiveness and associated risks to personal privacy.

The study recommended that a framework be designed to guide decisions about the development, procurement, and use of information-based programs. Consistency in these guidelines closely resembles best practices reflected in the Control Objectives for Information and Related Technologies, the IT Infrastructure Library, International Organization for Standards 17799, and standards disseminated by the National Institute of Standards and Technology, among others. The framework made routine monitoring and [re]evaluation; ongoing auditing; and clear, competent oversight of major IT investment programs—at a minimum—necessary. Although the framework under development by the Committee is deliberately broad, because it is designed to apply to all information-based programs across government and commercial organizations, not all points addressed by the framework are applicable to DHS OCIO. Where a point is not applicable, but required when establishing consistency, DHS OCIO consults with the DHS Privacy Office on methods and use while

<sup>7</sup> All persons engaged in developing or using information-program based systems for data-mining are trained in the their appropriate use and the laws and regulations applicable to their use (i.e., federal, state, local, tribune law enforcement)

<sup>8</sup> <http://www.cdt.org/security/usapatriot/20040300tapac.pdf>

clearly documenting an explanation as to why the point is inapplicable. At times, consultation may result in policy recommendations or changes.

The framework and processes outlined in the study recommend conducting ongoing [re]evaluations of development, integration, and operation and maintenance of systems and programs, both technical and business, on a regular basis. They also recommend revising planning, as necessary, to ensure that objectives are achievable, programs are compliant with laws, and systems are operational within the design scope. DHS has generally adopted these recommendations. These information program reviews are conducted by the DHS OCIO, Component OCIOs, and the Acquisition Program Management Division (APMD) and are evidence that DHS executes oversight procedures to ensure its management, technological, and financial resources are managed wisely and efficiently.

DHS understands, through this GAO Audit, that some Components may exercise use of DHS-directed plans and processes, whereas other Components did not sufficiently address requirements, such as data quality, for evaluating system effectiveness or transparency and external oversight. To mitigate discrepancies, DHS is conducting oversight and portfolio review of data-mining systems at a risk-based level, assessing modules that engage active graphical user interfaces and legacy-based platforms to ensure program creations are valid, permanent, and tamper-resistant. For example, within application modules, codes or “rules” are created that summarize intricate concepts of business activity that help identify suspicious or unusual behavior. The risk-based rules are derived from discrete data elements, including criteria that pertain to specific operational or tactical objectives or local enforcement efforts. These rules are constantly evolving or changing to both meet new threats and refine existing rules. DHS Component OCIOs use these rules to develop programs intended to target specific criminal activity or pattern behavior, through either integration of other OCIO Component programs or development of new pattern-detecting programs.

DHS Headquarters will work with the Components ensuring that documentation is developed and disseminated across DHS OCIOs describing the administration of rules to satisfy successful integration of systems DHS-wide; and to apply corrective action, bringing corporate and Component guidelines in sync with privacy regulations. DHS will also use best-practices guidance to identify data-mining tools, both developmental and Commercial Off-the-Shelf (COTS) to implement and/or leverage design concepts within its Systems Engineering Life Cycle process. Changes to DHS policies<sup>9</sup> and APMD Management Directive 102-1 are to be discussed, as well.

DHS OCIO currently works jointly with—and intends to continue strengthening internal relationships with—the IT Services Office, the Chief Information Security Office, and the Office of Applied Technology (Enterprise Architect Division) to discuss changes in acquisition policies and challenges in systems integrations (COTS and legacy). Additionally, these joint interactions will allow DHS to keep current with changes in rules, best practices, laws, regulations, mandates, and processes to minimize privacy intrusion and to ensure DHS and its Component OCIOs continue safeguarding the infrastructure. The outcome of these

<sup>9</sup> DHS Management Directives System, MD Number: 0007.1, Issue Date: 03/15/2007, Information Technology Integration and Management – and – DHS Management Directive System, MD Number: 4300.1, Information Technology Systems Security

meetings will create improved transparency for continued reporting<sup>10</sup> to the public and the Office of Management and Budget and protect trade secrets and the privacy of the agency.

**Recommendation 3:** the Chief Privacy Officer to develop requirements for providing additional scrutiny of privacy protections for the sensitive information systems that are not transparent to the public through PIAs.

**Response:** Concur. Transparency is one of the DHS Fair Information Practice Principles and an important element of the DHS Privacy Office mission. DHS recognizes that PIAs are often the most complete and sometimes the only public description of DHS systems and practices. The DHS Privacy Office website has a vast library of PIAs, SORNs, reports (such as the annual DHS Data Mining Report), and other information that help the public understand how DHS collects, uses, maintains, and disseminates PII. Transparency necessarily becomes more challenging when systems are classified or otherwise sensitive because they address, for example, law enforcement techniques (e.g., Law Enforcement Sensitive) or methods of protecting the transportation system from terrorist attacks (e.g., Sensitive Security Information).

In response to this recommendation, the Privacy Office will include an annex to its Annual Report to Congress marked and handled with the appropriate national security classification (or other sensitive, but unclassified restriction) that lists all PIAs conducted during the reporting period that are either redacted in part or withheld from publication, providing an abstract of each. After reviewing the annex, interested Members of Congress can request the documents or schedule a briefing with the appropriate DHS stakeholders. This step will help provide additional transparency, while maintaining the classified or sensitive nature of the program that national security law and other restrictions are designed to preserve.

We note that DHS has very few unpublished PIAs. DHS favors unclassified, wholly available PIAs, the majority of which are posted on the DHS Privacy Office's public Website. This library includes a number of PIAs addressing national security or other sensitive programs, appropriately redacted following a sensitivity review. This affords the public a measure of transparency consistent with national security and other authorities. In addition, DHS conducts a number of PIAs for systems that are exempt from the E-Government Act's PIA requirements, including the requirement to make them available to the public. DHS, however, routinely shares these PIAs with Members of Congress and others, as appropriate.

**Recommendation 4:** the Chief Privacy Officer to investigate whether the information sharing component of ICEPIC, called the Law Enforcement Information Sharing Service, should be deactivated until a PIA that includes this component is approved.

**Response:** Concur. The Chief Privacy Officer will conduct an investigation. The DHS Privacy Office is already coordinating with the U.S. Immigration and Customs Enforcement Privacy Officer and relevant program officials to review and revise the ICE Pattern Analysis and Information Collection PIA, as appropriate.

<sup>10</sup> Most current report: DHS Privacy Office – 2010 Data Mining Report to Congress, December 2010

**Recommendation 5:** the appropriate component agency administrators to ensure that the system program offices for AFI, ATS-P, CIDR, DARTTS, ICEPIC, and TECS-Mod address the shortfalls in evaluating system effectiveness and privacy protections identified in this report, including shortfalls in applying acquisition practices, ensuring executive review and approval, and consistently documenting executive reviews.

**Response:** Concur. The appropriate component agency administrators will ensure that system program offices for AFI, ATS-P, Citizenship and Immigration Data Repository (CIDR), Data Analysis and Research for Trade Transparency System, ICEPIC, and TECS Modernization address the shortfalls in evaluating system effectiveness and privacy protections identified in this report, including shortfalls in applying acquisition practices, ensuring executive review and approval and consistently documenting executive reviews. The ICEPIC PIA Update is in progress and will address the deficiencies indicated in the GAO Report. This should be completed shortly. However, DHS notes the following for the AFI and CIDR systems.

**CIDR:** Version 1.0 of the CIDR system is still under development. Most of the shortcomings GAO identified are related to the fact that CIDR is still in development. This system has not reached the stage of operational testing and operator and system assessments and therefore could not be completed. In both these cases, the program office already has plans to conduct user, system, and operational testing once development is complete.

The GAO recognized CIDR's approved PIA, but noted that the program office did not document "acquisition requirements or obtain a waiver for them." Given the overall cost of the CIDR program (\$350,000), waivers were not required because the system costs did not exceed the thresholds established in Management Directive 102-01R. An Advance Acquisition Plan for CIDR was approved in April 2008 in accordance with existing U.S. Customs and Immigration Services (USCIS) and DHS acquisition policies on the basis of the estimated value of the system as cited above. The program office will continue to comply with all established DHS and USCIS acquisition policies.

Development for CIDR was approved by the Intelligence System Board and later the National Security Systems Board (NSSB). Periodic updates were provided to the NSSB on the status of CIDR. It should be noted that Investment/Acquisition Review Board approval is not required on the basis of the total estimated value of the system. In addition, the program office worked with the NSSB and DHS OCIO to bring the servers online that support CIDR on DHS's Homeland Top Secret Network. The program office also received approval from the Homeland Secure Data Network Security Accreditation Working Group (HSAWG). HSAWG review included DHS OCIO and information security certification. The HSAWG approval came with no follow-up action items or conditions of approval.

The program office will continue to work with USCIS and DHS Privacy Offices, NSSB, and HSAWG to ensure that all system documentation requirements are met. In addition, the program office has initiated a CIDR-specific project check list for future releases of the software to ensure that all aspects of the system are documented and approved by the appropriate authority.

**AFI:** Currently, the AFI system is in the development phase of the System Life Cycle (SLC) and has not yet reached production readiness, nor is it operational. The template used by



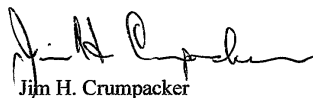
GAO to assess AFI is not adequate to evaluate the status of the AFI program while in this phase of the SLC. Assessment grades have not been applied uniformly across all assessment points. For example, the fact that AFI's PIA is currently under review (not yet approved) has resulted in ratings of "No," "N/A," and "Partial." DHS believes that any assessment point that is not yet fully met, but is within the DHS or U.S. Customs and Border Protection (CBP) defined process that would meet the assessment point should either be rated as "Yes" (as the program is following approved processes and assessing the program against where it is in the approved lifecycle) or at a minimum as "N/A."

The AFI Program Office has a comprehensive project plan that currently requires that for AFI to become operational, the following items will be completed:

- A PIA must be signed and any other privacy concerns must be answered to the satisfaction of DHS Privacy Office leadership;
- Independent testing will be completed by competent authorities within the CBP Office of Information and Technology;
- Data verification and validation checks will be complete by both user acceptance testing participants and competent system testing authorities within CBP;
- Approvals of the system by responsible executives within CBP will be completed as part of the certification and accreditation process and approval; and
- Privacy controls and clock (time from signing of a PIA) will be in place and maintained within the approval schedules referenced above.

Again, thank you for the opportunity to review and comment on this draft report. Extensive technical comments were previously provided under separate cover. We look forward to working with you on future Homeland Security issues.

Sincerely,



Jim H. Crumpacker  
Director  
Departmental GAO/OIG Liaison Office

---

# Appendix VI: GAO Contact and Staff Acknowledgments

---

## GAO Contact

David A. Powner, (202) 512-9286 or [pownerd@gao.gov](mailto:pownerd@gao.gov)

---

## Staff Acknowledgments

In addition to the contact name above, individuals making contributions to this report included Colleen Phillips (Assistant Director), Justin Booth, Josh Leiling, Kathleen S. Lovett, Lee McCracken, and David Plocher.

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site ([www.gao.gov](http://www.gao.gov)). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to [www.gao.gov](http://www.gao.gov) and select "E-mail Updates."

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Ralph Dawn, Managing Director, [dawnr@gao.gov](mailto:dawnr@gao.gov), (202) 512-4400  
U.S. Government Accountability Office, 441 G Street NW, Room 7125  
Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548

