

DEPARTMENT OF HOMELAND SECURITY
Office of Inspector General

**ADVISE Could Support Intelligence
Analysis More Effectively**





Homeland
Security

JUL - 2 2007

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report addresses how well the Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE) system enables intelligence analysts to search rapidly and integrate information to identify and understand potential threats to homeland security. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.



Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Executive Summary	3
Background	4
Results of Audit	8
R&D Planning Approach Does Not Effectively Support ADVISE.....	8
System Has Not Been Effectively Implemented to Meet Mission Requirements	9
DHS Components Have Not Committed to ADVISE	17
Recommendations.....	21
Management Comments and OIG Evaluation	22

Appendices

- Appendix A: Scope and Methodology
- Appendix B: Management Comments to the Draft Report
- Appendix C: Major Contributors to this Report
- Appendix D: Report Distribution

Abbreviations

All-WME	All Weapons of Mass Effect
ADVISE	Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement
DHS	Department of Homeland Security
GAO	Government Accountability Office
IPT	Integrated Product Team
IT	Information Technology
OI&A	Office of Intelligence and Analysis
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PTA	Privacy Threshold Analysis
R&D	Research and Development
S&T	Science and Technology Directorate
TVIS	Threat-Vulnerability Integration System

Table of Contents/Abbreviations

Figures

Figure 1 ADVISE Connects and Visualizes Data to Support Intelligence Analysis4

Figure 2 ADVISE Pilot Implementations6

Figure 3 ADVISE Funding Summary7

Figure 4 Key Areas Not Addressed During ADVISE Effort10

Figure 5 ADVISE Implementations and Privacy Assessments.....12

Figure 6 Key ADVISE System Operational and Privacy Dates12

Figure 7 TVIS Deployment Challenges at OI&A14

Figure 8 ADVISE Customer Buy-in21

OIG

*Department of Homeland Security
Office of Inspector General*

Executive Summary

The *Homeland Security Act of 2002* requires DHS to create and use data mining tools to access, receive, and analyze law enforcement and intelligence information for the purpose of identifying potential terrorist threats within the United States. As of August 2006, there were 12 major data mining efforts in existence within DHS. One such effort is the Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE) program, developed by the Directorate of Science and Technology (S&T) to support DHS' strategic goals of terrorism awareness and prevention.

As directed by the Conference Report (House Report No. 109-699) on H.R. 5441, *Department of Homeland Security Appropriations Act of 2007*, we audited the ADVISE program. Our audit objectives were to determine the effectiveness of (1) strategies, policies, and procedures for conducting data mining to produce actionable intelligence on terrorists; (2) systems and activities using data mining techniques; and (3) communication and coordination with information security partners and the public to help prepare for and counter the potential threats identified. The scope and methodology of this review are discussed in Appendix A.

The ADVISE program is at risk, due to a number of factors. Specifically, S&T program managers did not develop a formal business case for the research and development project, in part because they were unaware of requirements to do so. In addition, program managers did not address privacy impacts before implementing three pilot initiatives to support ADVISE. Further, due to inadequate data access and system usability, Office of Intelligence and Analysis (OI&A) analysts did not use the ADVISE pilot. Finally, because S&T did not effectively communicate and coordinate with DHS leadership about the benefits of ADVISE, departmental components have been unwilling to adopt ADVISE to support their intelligence analysis operations. As a result of privacy concerns, DHS has discontinued the three ADVISE pilots. Further, due to a lack of stakeholder commitment, program managers have stated that continuation of the ADVISE program is in question if an owner cannot be found to pay for future system operations and maintenance costs.

Background

S&T is the department's primary research and development arm, responsible for providing federal, state, and local officials with the technology and capabilities needed to protect the homeland. S&T fulfills this mission through its strategic objectives of, among other things, developing and deploying state-of-the-art, high performance systems to prevent, detect, and mitigate the consequences of chemical, biological, radiological, nuclear, and explosive attacks.

S&T developed ADVISE as a key technology to carry out its strategic goals. ADVISE is a collection of software, hardware, and operational standards that can be adapted and tailored to meet the specific needs of the user organization. ADVISE provides the ability to search, integrate, and gain rapid insights from large quantities of information across disparate databases, a process that would otherwise be overwhelming to intelligence analysts. ADVISE identifies connections among people, organizations, and events, and produces visual representations of these patterns, as shown in Figure 1.

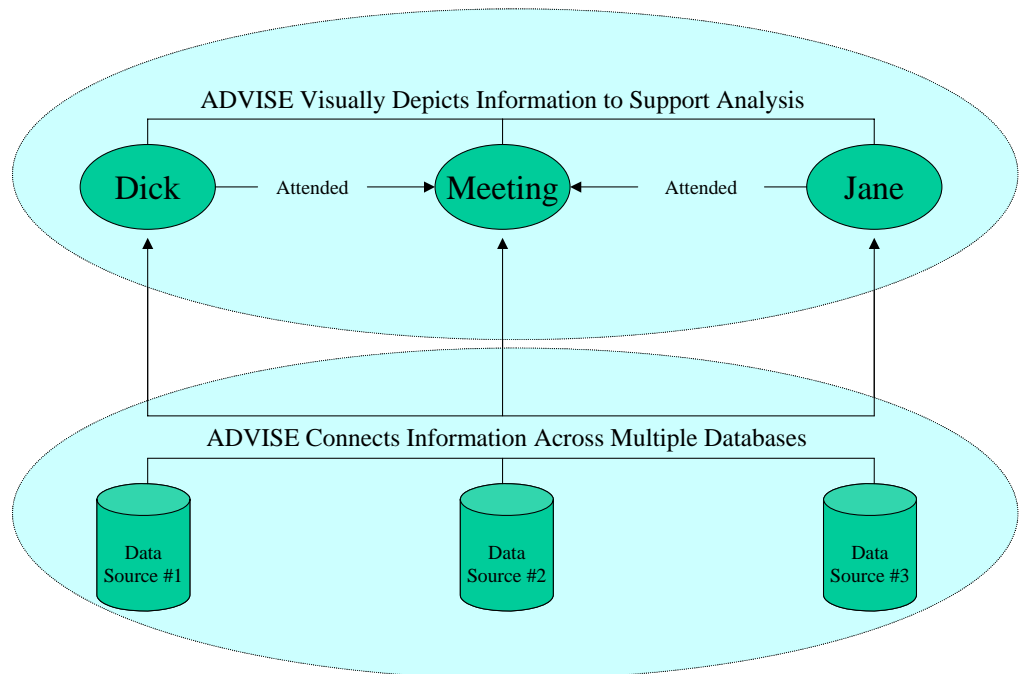


Figure 1: ADVISE Connects and Visualizes Data to Support Intelligence Analysis

ADVISE is intended to benefit intelligence analysts by:

- Revealing information or related topics that would otherwise go unnoticed;
- Enabling comprehensive analysis capabilities in one place; and

ADVISE Could Support Intelligence Analysis More Effectively

-
- Providing a watch and warning capability to notify analysts when a certain pattern is detected.

DHS is to use the analysis made possible through ADVISE to help detect, deter, and mitigate threats to our homeland and disseminate timely information to its homeland security partners and the American public.

ADVISE development began in early 2003 following discussions between S&T officials and personnel at the Department of Energy's national laboratories, including Lawrence Livermore National Laboratory (Livermore) and Pacific Northwest National Laboratory (Pacific Northwest), about developing a data mining and visualization technology for DHS intelligence analysts.¹ These laboratories had prior knowledge and experience in developing such technologies for another federal intelligence agency. S&T provided funding for the laboratories to develop ADVISE, building on this prior work.

In 2004, S&T expanded the ADVISE concept to provide a general framework for supporting the analytical activities of multiple DHS organizations. By 2005, S&T had used the ADVISE framework to implement the following three pilot programs:

- The Biodefense Knowledge Management System, developed to explore linkages among biodefense data and assessment to produce actionable, scientifically rigorous information for anticipating, preventing, and responding to biological threats. With funding by S&T, the Biodefense Knowledge Center at Livermore uses this pilot system to help integrate biodefense information and anticipate and respond to bioterrorist attacks.
- All Weapons of Mass Effect (All-WME), which uses ADVISE to determine the capabilities of foreign and domestic terrorist groups to develop and deploy weapons of mass effect. The All-WME program is also an S&T-funded initiative at Livermore.
- The Threat-Vulnerability Integration System (TVIS), which combines and fuses data in unique ways to create and share knowledge of potential terrorist threats. S&T implemented the ADVISE pilot at OI&A, the primary pilot system for demonstrating ADVISE capabilities. The system is to support the office's mission of providing homeland security intelligence to the DHS Secretary and other federal, state, local, and private sector partners.

¹ The *Homeland Security Act of 2002* gives DHS the authority to use the Department of Energy's national laboratories to support homeland security activities.

The pilots used live data, including personally identifiable information, from multiple sources in attempts to identify potential terrorist activity. Figure 2 provides a timeline for the three ADVISE initiatives, which became operational in late 2004 to early 2005.

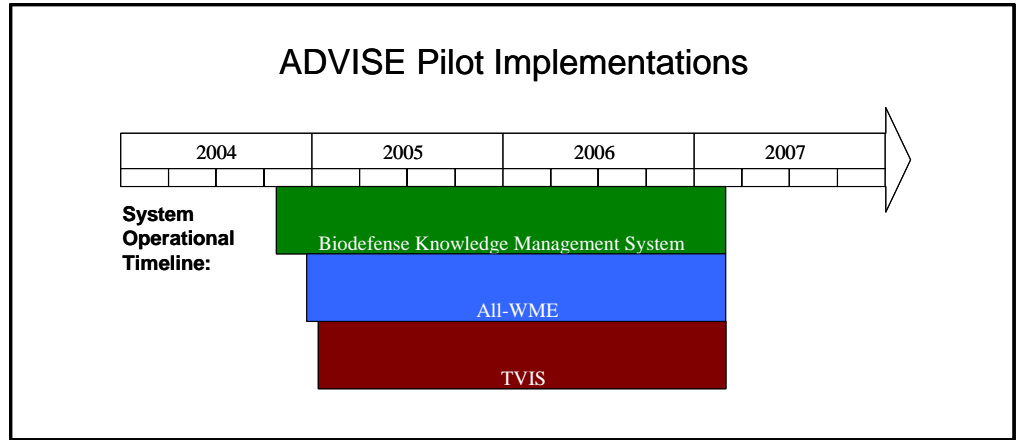


Figure 2: ADVISE Pilot Implementations

The ADVISE pilot initiatives use a data mining approach to glean insights from large amounts of data across various sources. Data mining is the process of knowledge discovery and predictive modeling and analytics, traditionally involving the identification of patterns and relationships from databases.² Data mining has been used successfully for a number of years in the private and public sectors for a broad range of applications. For example, in commercial industry these applications include customer relationship management, market research, retail and supply chain analysis, medical analysis and diagnostics, financial analysis, and fraud detection. In government, data mining is increasingly used to help detect terrorist threats through the collection and analysis of both public and private sector data. Although data mining does not replace the expertise that an analyst provides, it automates and facilitates some of the laborious tasks that an analyst performs.

Due to the ease with which automated systems can be used to gather and analyze large amounts of previously isolated data, a number of concerns about potential misuse of personally identifiable information have been raised. Prior federal data mining efforts faced challenges in balancing the benefits and risks of this activity. For example, the Total Information Awareness program, a Department of Defense research and development data mining program to defend against the threat of terrorism, faced considerable negative publicity and was ultimately shut down by the Congress due to privacy concerns.

² Survey of DHS Data Mining Activities, OIG-06-56, August 2006.

Given these data mining challenges, in 2006, the Congress directed the Government Accountability Office (GAO) to review the ADVISE program to determine the system’s capabilities, uses, and associated benefits. The Congress wanted to know whether potential privacy issues could arise from using the tool and how DHS has addressed such issues. Based on its review, GAO reported that prior to implementing the system DHS needed to ensure that privacy protections were in place.³ As such, GAO recommended that DHS immediately conduct a privacy impact assessment (PIA) of the ADVISE tool and implement privacy controls, as needed, to mitigate any identified risks. Based on the system’s cost and potential privacy impact, the Congress directed our office to review the ADVISE program, as well.⁴

Figure 3 charts the ADVISE budget through fiscal year 2007, showing a total program budget of about \$42 million. S&T has used these funds for development of the ADVISE framework and deployment of the pilot systems, since the program was based on prior research at the national laboratories. S&T plans to transition funding for ADVISE operations and maintenance to system customers in subsequent years. Hence, funding for FY 2008 is limited, subject to appropriations. Funding for FY 2009 and beyond has not yet been determined.

ADVISE FUNDING SUMMARY						
Funding (\$ κ)	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	Total
Research			200	60		
Development	3,100	8,300	7,000	4,190	1,000	
Pilot Deployments	1,900	3,200	7,300	4,250		
Operational Prototype					1,500	
Total:	5,000	11,500	14,500	8,500	2,500	42,000

Figure 3: ADVISE Funding Summary

³ *Data Mining: Early Attention to Privacy in Developing a Key DHS Program Could Reduce Risks*, GAO-07-293, February 2007.

⁴ H. Rep. No. 109-699 (on DHS Appropriations for FY 2007, P.L. 109-295).

Results of Audit

R&D Planning Approach Does Not Effectively Support ADVISE

S&T planning and management activities for ADVISE have been insufficient to support effective implementation of the program. Specifically, S&T program managers were unaware of standards and requirements for research and development projects and did not develop a formal business case for the program. Program managers also did not address privacy impacts before implementing three pilot initiatives to support ADVISE. DHS has discontinued its three ADVISE pilot programs, pending completion of such privacy assessments.

Program Management Unaware of Guidelines for Conducting R&D Projects

As with systems acquisitions, research and development (R&D) program managers can benefit from clear guidance and procedures on planning, justifying, and deciding from among competing technology solutions. However, according to ADVISE program managers, they were unaware of requirements for accomplishing R&D projects and ultimately transitioning the information technology (IT) solution to potential customers.

S&T began ADVISE research efforts in 2003, just after the creation of DHS. At that time, major department organizations, including S&T, were still in a formative stage and had not clearly adopted or communicated the standards for conducting critical program management functions. For example, S&T program managers stated that because the directorate had no structured R&D process in place, they relied instead on their own knowledge and personal experience to determine what program management activities needed to be performed. They focused their efforts on technical capabilities and IT engineering and had no standard list of activities to consult to ensure that important management steps in the R&D process were adequately addressed to meet end user needs.

Similarly, it was not clear to ADVISE program management that the system needed a privacy assessment. When the DHS Privacy Office began operations in 2003, it was comprised of only the Chief Privacy Officer and one support staff member, and did not have the resources or capacity to review all DHS IT projects for privacy impacts. Therefore, the office concentrated its privacy evaluation efforts on only those IT projects with completed business cases. Lacking a business case, the ADVISE R&D effort received little Privacy Office oversight and review. The responsibility for performing and documenting privacy impact assessments was not brought to the attention of ADVISE program managers in the early stages of the initiative.

Business Case Not Prepared for ADVISE

Office of Management and Budget (OMB) Circular A-11 requires that a federal agency, as part of its capital planning process, prepare a business case for each major IT project, system, or initiative.⁵ Likewise, DHS' *Guide to Information Technology Capital Planning and Investment Control*, issued in May 2003, states that a program or project manager is responsible for completing project documentation, including a business case.

A business case serves as the primary means of justifying an IT investment proposal, as well as managing the investment once it is funded. For example, a business case can serve as a management tool that helps an agency provide for oversight and periodic review of an IT asset to ensure that it delivers intended benefits and fulfills mission needs and user requirements. As program managers develop business cases, they can demonstrate that they have considered and addressed, among other things, the alignment of the project to customers' needs, alternative solutions, data requirements, and potential effects on privacy.

S&T produced a variety of planning documents, including a concept of operations and system development and implementation plans. However, S&T did not develop a business case for ADVISE, which would have provided a more structured approach to justifying and supporting the IT investment. As previously stated, because S&T had not clearly adopted or communicated R&D processes and procedures at this phase in the directorate's evolution, program managers were unaware of the requirement to develop such documentation. S&T program managers were unaware of overarching guidance, such as DHS' *Investment Review Process*, which requires completion of business cases for IT projects, including R&D projects, that meet specific cost thresholds.⁶ Although the ADVISE program's lifecycle cost of approximately \$42 million through fiscal year 2007 met this threshold, S&T program managers proceeded without a business case and have made no plans to prepare one in the future.

System Has Not Been Effectively Implemented to Meet Mission Requirements

Inadequate R&D planning has resulted in problems with ADVISE pilot implementation. Specifically, S&T program managers did not conduct assessments to ensure that personal privacy issues were addressed effectively as part of systems implementation. Access to the data needed to demonstrate system capability and effectiveness in meeting mission needs was not adequately coordinated. Moreover, because ADVISE contained limited data

⁵ OMB Circular No. A-11, Part 7, Planning, Budgeting, Acquisition, and Management of Capital Assets, July 2004, amended June 2006.

⁶ DHS Management Directive 1400, March 2003.

and was complicated and time consuming to operate and maintain, few intelligence analysts were committed to using the system.

Key Program Management Activities Not Performed

Without a business case, key issues were not identified and addressed during ADVISE R&D. OMB guidance identifies specific key areas that should be addressed in developing business cases for proposed IT initiatives.⁷ These areas include conducting privacy impact assessments; identifying the types of data needed for successful system operations; determining how the proposed technology will align with customers’ needs; deciding how integrated product teams (IPT) will be used to plan, budget, procure, and manage the IT project; and, discussing how alternatives were considered before committing to the chosen IT solution. Figure 4 depicts the key areas not addressed during ADVISE R&D due to lack of a business case.

Key Areas To Address Within a Business Case	Effect of Not Addressing Key Areas During ADVISE Effort
Privacy Impacts	Privacy Not Addressed Timely
Types of Data Needed for the System	Data Needs Not Determined
IT Alignment to Customers’ Needs	Customers’ Needs Not Determined
Integrated Project Teams (IPT)	IPTs Not Used Effectively
Alternative IT Solutions	Alternative Solutions Not Evaluated

Figure 4: Key Areas Not Addressed During ADVISE Effort

Failure to address these issues during the R&D process limited the effectiveness of the ADVISE pilot program, as discussed below.

Privacy Impacts Not Determined for ADVISE

Section 208 of the *E-Government Act of 2002* requires federal agencies to conduct a Privacy Impact Assessment (PIA) for each new or substantially changed IT system that collects, maintains, or disseminates personally identifiable information. Additionally, DHS’ official guidance for PIAs, which was first issued in 2004 and updated in 2006, says that if a system is being designed to handle personal information, a PIA is required at the very earliest stage of a project or prior to commencement of a pilot test.⁸

⁷ OMB Circular No. A-11, Part 7, Section 300, Planning, Budgeting, Acquisition, and Management of Capital Assets, July 2004, amended June 2006.

⁸ DHS Privacy Office, *Privacy Impact Assessment Official Guidance*, March 2006, previously *Privacy Impact Assessments Made Simple*, February 2004.

PIAs have many benefits. Among other things they document what information is to be collected, the intended use of the information, with whom the information will be shared, and how the information will be secured. Conducting a PIA ensures that:

- Public citizens are aware of the information that an agency collects about them;
- Any impacts that these systems have on personal privacy are adequately addressed; and
- An agency collects only enough personal information to administer its programs, and no more.

Further, a PIA confirms that an agency uses the information for the purpose intended, that the information remains timely and accurate, and that it is protected by the agency and held only as long as needed.

Despite the requirements for, and benefits of, addressing potential privacy impacts early during system design, ADVISE program managers did not begin this process until after the pilot programs were already operational. DHS privacy officials told S&T that no such action was required during the initial stages of ADVISE development. Because S&T program managers did not maintain regular contact with the Privacy Office during ADVISE R&D, they did not obtain additional guidance on when to begin the privacy documentation process or who was responsible for completing it. S&T program managers were unaware of DHS' Investment Review Process that requires that when a project is sponsored directly by S&T, as was ADVISE, the S&T project team is responsible for meeting all investment management requirements, including developing a business case and, in this context, addressing privacy issues. Not understanding this process, ADVISE program managers believed it was the responsibility of the individual DHS component offices, not S&T, to develop and submit privacy documentation because those offices owned the data that would be used by the system.

For its part, the DHS Privacy Office did not know that S&T had proceeded with implementation of the ADVISE pilot programs with live data, but without addressing privacy matters. In a July 6, 2006, report to the Congress, the Privacy Office stated that the ADVISE tool alone does not perform data mining. However, the report went on to state that implementation of this system with live data could be considered a data mining tool. Unbeknownst to the Privacy Office, the ADVISE pilots had been implemented at least 18 months prior to its July 2006 report.

Given the lack of communication and coordination between S&T and the DHS Privacy Office, ADVISE program managers did not conduct the first step in the privacy assessment process—completing privacy threshold

ADVISE Could Support Intelligence Analysis More Effectively

analyses (PTAs) to determine whether PIAs were necessary for each of the three pilots—until one to two years after the systems had been deployed. Upon reviewing the PTAs, the Privacy Office determined that each of the three ADVISE pilot systems would require a PIA. Figure 5 illustrates the time lapse between ADVISE implementation and submission of the initial PTAs and PIAs for the three pilot systems.

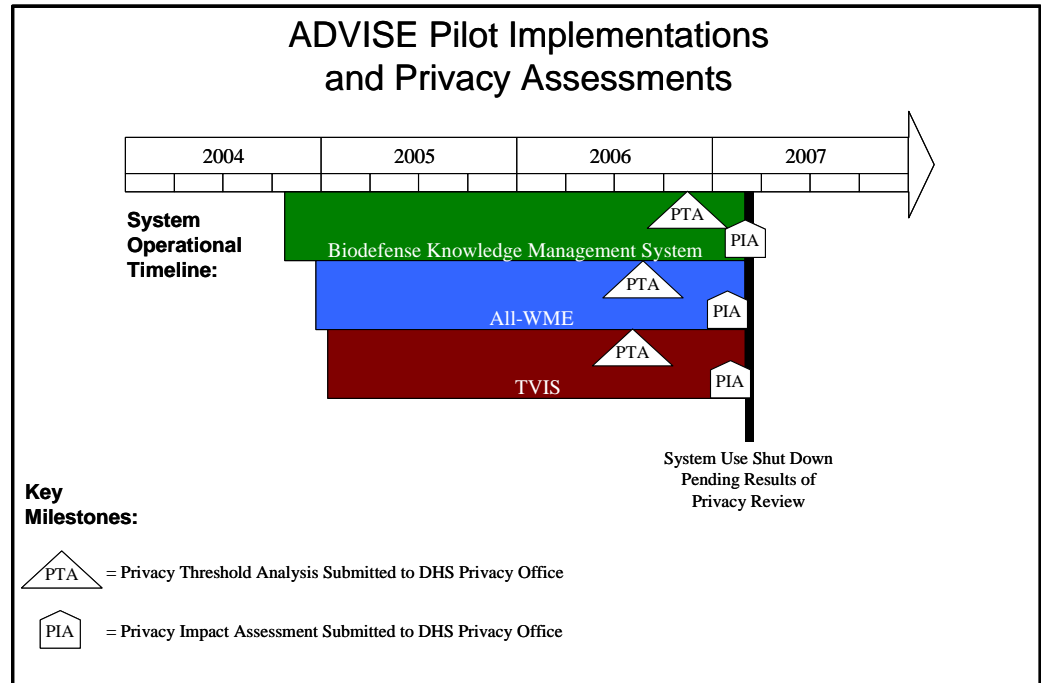


Figure 5: ADVISE Implementations and Privacy Assessments

According to the Privacy Office, S&T submitted the PTAs for the three operational ADVISE pilot systems in mid to late 2006. The actual submission dates of the PTAs and PIAs are shown in Figure 6.

ADVISE Implementations and Operational Start Timeframe		PTA Submission Date	PIA Submission Date
BKMS	Oct 2004	11/06/2006	03/07/2007
All-WME	Dec 2004	07/21/2006	01/19/2007
TVIS	Jan 2005	06/27/2006	01/19/2007

Figure 6: Key ADVISE System Operational and Privacy Dates

Failure to properly address privacy issues prior to deploying the three pilots had the ultimate effect of bringing the ADVISE program to a halt. In its

ADVISE Could Support Intelligence Analysis More Effectively

February 2007 report, GAO recommended that DHS immediately conduct ADVISE privacy impact assessments and implement privacy controls, as needed, to mitigate any identified risks. Subsequently, in March 2007, S&T shut down all of the ADVISE pilot programs until privacy impacts can be determined.

Privacy considerations cannot be ignored in the context of data mining systems and activities. Maintaining the appropriate balance between the need to “connect the dots” and the need to respect the privacy and other legal rights of U.S. citizens can be a difficult and time-consuming effort, but is a necessary one. Civil liberties organizations have challenged other data mining activities in the past; unaddressed privacy concerns pose similar challenges for the ADVISE program success. Recognizing the risks created by not addressing privacy issues in a timely manner, senior S&T management is now working with the Privacy Office to complete the required assessments and help get the program back on track.

Limited Data Access

OMB Circular A-130 directs that agencies, as part of their IT investments planning process, determine how data will be accessed and used to support proposed systems.⁹ Similarly, OMB Circular A-11 directs agencies to consider the risks inherent in acquiring data from existing sources and converting it for use in implementing new IT systems.

Despite these requirements, S&T did not address adequately data access issues prior to implementing TVIS, one of the three ADVISE pilots, intended for use by OI&A intelligence analysts who are the primary customer of ADVISE. S&T program planning documents indicate that the national laboratories, responsible for developing TVIS, identified the risks that a lack of available data could pose to the system’s success. Specifically, TVIS was designed to identify connections across multiple databases with large quantities of data. To operate effectively, TVIS requires direct connection with source databases and depends on data being extracted and ingested routinely and automatically from these sources. The national laboratories identified approximately 50 internal DHS data sources and 100 external data sources that could support the system.

However, S&T did not take sufficient action to ensure access to the data needed for TVIS pilot implementation. At the start of the program, S&T did not know who owned the data needed or how to get access to it. S&T also had no process in place for working through these issues. Assuming that OI&A already had easy access to large amounts of data and the processes in

⁹ Revision of OMB Circular No. A-130, Transmittal 4, *Management of Federal Information Resources*, November 28, 2000.

place to facilitate obtaining such access, S&T relied on OI&A intelligence analysts to provide the system data on an ad hoc basis. However, this approach was not effective. Although the OI&A analysts had access to considerable data via individual accounts, they lacked direct access to the source databases. The OI&A analysts also did not have the position or authority to coordinate the information sharing agreements necessary to ensure data access on a continuing basis.

Nonetheless, the intelligence analysts provided the limited data that they had to support TVIS, but found that the amount of information was inadequate to make ADVISE more useful than their existing analysis tools. Although TVIS planning documents indicated a goal of having 15 data sources loaded into TVIS by 2007, as of March 2007, only seven data sets had been loaded—more than two years after TVIS was deployed. Further, these seven data sets that were loaded were of limited size, and inadequate to demonstrate the broad analytical capability of the system. Due to the lack of data to populate the system, the analysis provided through TVIS was no greater than results obtainable via other existing intelligence analysis tools. For example, Analyst’s Notebook, an off-the-shelf tool currently used, also provides analysts with the ability to visually depict connections among people, organizations, and events. Figure 7 illustrates the extended amount of time required to access the limited data sets used to conduct the TVIS pilot.

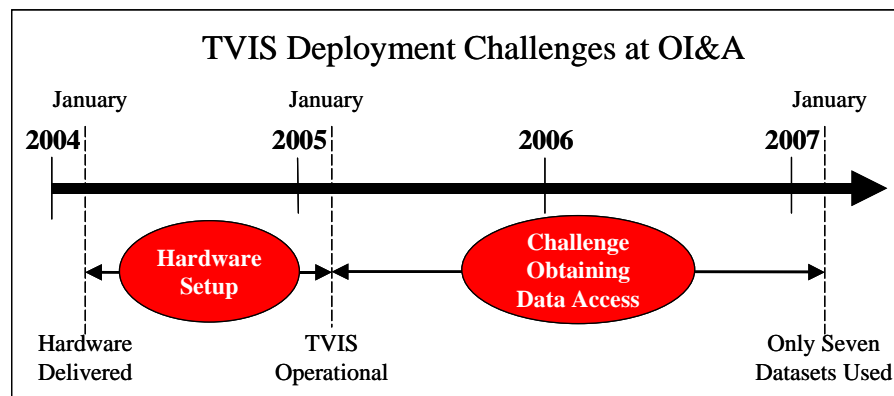


Figure 7: TVIS Deployment Challenges at OI&A

In contrast to TVIS, the two other ADVISE pilot systems—the Biodefense Knowledge Management System and All-WME—had access to sufficient data. The programs engaged in these pilots have been able to dedicate the staff resources required to input data to the systems. Analysts that use these pilot systems have found the analysis that they provide to be highly beneficial. For example, All-WME analysts have used their pilot system to uncover previously unknown connections between organized crime and terrorism. Additionally, Biodefense Knowledge Management System users rely on their pilot system to explore linkages among open source medical resources and

ADVISE Could Support Intelligence Analysis More Effectively

documentation, and produce actionable biodefense information and assessments.

System Usability Could be Improved

OMB Circular A-11 directs agencies to reduce project risk by involving stakeholders in the design of IT assets.¹⁰ When users are not involved in system development, it is difficult to ensure that the system will provide for their needed functions.

Despite these requirements, S&T did not involve adequately users early in the design of TVIS—the primary pilot system for demonstrating ADVISE capabilities. The initial requirement for TVIS was based on the high-level need identified after the September 11, 2001, terrorist attacks to enhance information sharing across federal, state, local, and private sector organizations. TVIS was conceived as an advanced analytical tool to help “connect the dots” and synthesize vast amounts of information across multiple sources in ways not yet available in the commercial marketplace. As such, S&T set out to develop a large, powerful system, with far-reaching capabilities that, some components believed, exceeded the processing capacity needed. Consequently, TVIS performance metrics focused on technical functionality, such as the number of facts the system could process simultaneously, rather than on ease of use.

S&T program managers said that they attempted to include OI&A analysts in TVIS development activities to obtain more specific user requirements. For example, at one point, S&T met with selected OI&A analysts to elicit their input and document user requirements.¹¹ However, the newness and uncertain mission of the DHS intelligence office at that time made it difficult to understand its business requirements. Further, the high turnover among intelligence analysts made it difficult to maintain relationships with the users long enough to understand sufficiently their functional and IT needs.

Due to the challenges in working with OI&A analysts, S&T reached out to intelligence analysts at the national laboratories to obtain requirements input. However, by focusing on analysts at the labs, S&T compiled user requirements that did not consider the constraints and work environment at OI&A, the primary customer of ADVISE. Specifically, OI&A analysts’ work tends to be short-term, tactical analysis, yielding immediate response. As such, OI&A analysts typically remain busy with daily workloads and have minimal time for other matters such as training and data input. In contrast,

¹⁰ Circular No. A-11, Part 7, *Planning Budgeting, Acquisition, and Management of Capital Assets, Executive Office of the President*, Office of Management and Budget, June 2006.

¹¹ S&T met with intelligence analysts of the former Information Analysis and Infrastructure Protection directorate, which no longer exists under the current DHS organization. Following the Secretary’s 2005 Second Stage Review, former functions of the directorate were divided among OI&A, and Preparedness.

intelligence analysts at the Biodefense Knowledge Center and All-WME tend to work on long-term, strategic intelligence problems that allow considerable time to identify and acquire data sources and prepare data for analysis in the system. By focusing on the system functionality requirements of the national lab users in developing ADVISE, S&T did not address effectively its primary users' requirements for ease of use and quick turnaround.

For example, OI&A analysts found that preparing data for processing in TVIS was difficult and time consuming. Much of the information needed by OI&A analysts is generally found in unstructured formats, such as text documents and email messages. However, TVIS was designed to easily process large amounts of structured information, accessed directly from other systems or databases. TVIS cannot readily extract information from unstructured sources. Analysts must first review available documentation, manually tag the relevant portions, and then input the information to the system—a time consuming and resource intensive activity. Analysts said they do not have time to devote to such data preparation and input, but must rely on technical support staff to perform these tasks.

Because of data limitations and system complexity, OI&A intelligence analysts never became committed, routine users of TVIS, even though the pilot remained operational for more than two years. Further, S&T had developed a goal of deploying TVIS to more than 100 OI&A analysts' desktops by summer 2007; however, only one or two analysts had access to TVIS at any given time while the system was operational at OI&A. Without widespread use of TVIS, S&T was not able to demonstrate fully the pilot system's potential to synthesize and process large amounts of information from disparate data sources.

Lacking the capability that TVIS was intended to provide, analysts said they cannot accomplish their mission responsibilities effectively. Analysts continue to rely on previously existing systems, such as Analyst's Notebook, to support their intelligence activities; however, this tool does not provide the capability needed to connect large quantities of information across multiple databases. As a result, analysts continue to waste time searching through individual, unconnected data sets for related information. Analysts also lose valuable time due to cumbersome processes to gain access to needed data. Specifically, in the absence of interagency agreements for broad-based data sharing, OI&A intelligence analysts individually must submit written requests for information that they need from other DHS component organizations. With limited tools, analysts are concerned that they may miss the data interrelationships necessary to help identify potential terrorist threats and activities.

To address the department's data sharing issues, DHS Secretary Chertoff recently issued a policy instructing component offices to review their

ADVISE Could Support Intelligence Analysis More Effectively

procedures and ensure that they facilitate, rather than impede, the exchange of information with OI&A.¹² In the policy, the Secretary directed all DHS components to ensure that employees have access to all information pertinent to their responsibilities. The Secretary also emphasized that DHS must move to using standardized technology to describe, access, exchange, and manage information in its automated systems. To help carry out this direction, an Information Sharing and Collaboration Branch, recently established by OI&A, is working in conjunction with the DHS Chief Information Officer to catalog existing information sharing agreements that can be leveraged to support OI&A data sharing and exchange.

Despite the challenges of loading data into ADVISE, recent tests have provided positive results regarding the system's user interface. Specifically, the Interagency Center for Applied Homeland Security Technology conducted an evaluation of ADVISE in early 2007 using simulated data preloaded into the system. The center provided various federal and state analysts with training prior to giving them tasks to perform using the system. When asked to evaluate the usability and utility of ADVISE, test participants generally gave the tool a good rating.

Further, S&T program management has initiated efforts to address TVIS user-friendliness issues by developing simple tools with which to perform data searches in TVIS. For example, a pre-defined query has been developed to alert analysts of travel by suspected terrorists to the United States. The query uses specific criteria for assessing the timing and frequency of suspect attempts to cross the U.S. border. The national laboratories also are developing tailored knowledge products to facilitate use of ADVISE so that less training is required. For example, one tailored knowledge product allows analysts to query information on bio-weapons, such as anthrax, using a simple keyword search.

DHS Components Have Not Committed to ADVISE

S&T did not coordinate effectively with stakeholders to ensure their commitment to adopt ADVISE as a solution for their intelligence analysis activities. Specifically, S&T did not involve stakeholders in the IT selection process via IPTs. S&T also did not explore alternative solutions to meeting customer needs within their existing financial, infrastructure, and facility constraints. As a result, the component stakeholders are not convinced that they need ADVISE and have not agreed to accept ownership for the system after the pilot phase of the program has been completed.

¹² DHS Policy for Internal Information Exchange and Sharing, February 1, 2007.

Ineffective Communication and Coordination With Stakeholders

Partnering with stakeholders is critical to securing end user commitment and ensuring the success of an IT investment. Conversely, limiting stakeholder involvement can lead to the development or acquisition of systems that might not meet user needs and ultimately might not be adopted for mission use. OMB Circular A-11 recommends the use of IPTs as one way to engage stakeholders in, and effectively guide, IT efforts.¹³ An IPT is a multi-disciplinary team led by a program manager responsible and accountable for planning, budgeting, acquiring, and managing a project throughout its life cycle to ensure that it successfully achieves cost, schedule, and performance goals. Participants on an IPT might include senior leadership of user organizations, program managers, system developers, customer representatives, and acquisition officials. Working together, IPT participants can use a consensus approach to exploring needs, identifying possible solutions, and validating strategies for moving forward.

In developing ADVISE, S&T did not take steps to ensure DHS component commitment by instituting IPTs or other methods for involving the components in the development process. As previously discussed, S&T built ADVISE from high-level system requirements and did not obtain an understanding of the privacy, data, and system usability concerns of the individual DHS components. The limited outreach that S&T did perform consisted of ad hoc meetings, demonstrations, and briefings on the technical capabilities of the system. As such, potential customers did not get a clear understanding of how ADVISE might benefit their individual organizations. Potential ADVISE customers also did not get a chance at the beginning stages of system design to discuss costs, consider constraints, and ensure that their specific user needs would be addressed.

Without the opportunity to dialogue on such issues during the early phases of the program, potential customers are finding it difficult to fit this large, expensive system into their budgets. While estimates are not yet complete, initial projections indicate that purchasing and installing ADVISE will be at least \$1 million, with yearly operations and maintenance costs of approximately \$400,000. Although S&T paid for ADVISE operations and maintenance during the pilot phase of the program, it is expected that these costs will transfer to the DHS customers when they take ownership of the system. As of December 2006, S&T did not have an estimate of the costs that each potential ADVISE customer would incur to operate and maintain ADVISE after implementation. Nonetheless, a number of potential customers

¹³ OMB Circular No. A-11, Part 7, *Planning Budgeting, Acquisition, and Management of Capital Assets*, Executive Office of the President, Supplement, June 2006.

said they are already concerned about their ability to assume what they expect to be a significant financial burden.

For example, officials of Customs and Border Protection's Office of Strategic Trade initially expressed interest in ADVISE as a potential solution to their requirement to view and process millions of pieces of trade data. Customs and Border Protection officials received a demonstration of ADVISE capabilities and attended a training session at Livermore. However, after learning the cost of ADVISE, these officials told S&T that the system was too expensive and therefore would not be a good option for them. Similarly, Immigration and Customs Enforcement officials complained that there has not been any clear analysis of the support costs for ADVISE. For example, they asked how much it would cost to train their personnel to use the system, but S&T provided no response. Lacking such information, Immigration and Customs Enforcement officials have been unable to make a decision about adopting the system.

In addition to issues related to system cost, some components expressed concerns about their ability to house and maintain the system, given their infrastructure limitations. ADVISE is a powerful system that operates using ten to fifteen servers and other multiple processors. Once installed and running, the hardware requires considerable electrical power and generates a large amount of heat. Components were concerned that they would have to update their physical infrastructures to meet these power and cooling requirements. Immigration and Customs Enforcement officials were fairly certain that they do not have the capacity or facilities needed to support these needs. As a result, these officials are exploring the possibility of using just the visualization portion of ADVISE.

Recently, in efforts to involve customers better and more consistently in its IT selection process, DHS has established ten IPTs covering major DHS functional areas, one of which is information sharing. The IPTs bring DHS leadership and user representatives into the IT acquisition process where they can help identify capability gaps, offer technical solutions to fill these gaps, provide a system end-user perspective in selecting IT solutions, and validate a plan for IT acquisition. The expected result of this IPT process is a prioritized list of proposed S&T technology investments. The S&T Under Secretary has given DHS' Transition Office responsibility for coordinating IPT activities.

In early 2007, based on information gathered through this recently established IPT process and other communications with DHS components, S&T shifted its focus to building a smaller version of ADVISE that will cost much less than the full-scale version. National laboratory officials agree that a scaled down version of ADVISE can offer comparable capabilities, but will lack the capacity to handle very large data sets. As a result, this smaller system may

not be able to fulfill DHS' mandate to synthesize vast amounts of information across multiple sources.

Lack of Alternative Analysis

IT project selection involves, among other things, a preliminary investigation of alternative solutions. Specifically, OMB Circular A-130 requires that agencies prepare, and update as necessary, a benefit-cost analysis for each information system, demonstrating consideration of alternatives and choosing the most cost-effective one.

However, in addition to not assessing DHS' existing intelligence analysis systems, S&T did not examine commercially available products to determine whether or not they might meet users' needs. For example, even though the ADVISE pilot operated within OI&A for more than 2 years, office leadership did not understand how ADVISE compared with existing intelligence analysis technologies such as Analyst's Notebook, or other systems that could be purchased off-the-shelf. About a year ago, one OI&A official requested that S&T provide a comparison of ADVISE to other systems, as well as a projection of the corresponding system operations and maintenance costs. It was not until March 2007 that ADVISE program officials provided a response to this request, via a presentation of the system to OI&A leadership. However, OI&A leadership found the presentation to be too technical and remained unconvinced that ADVISE was unique or would be the right solution for OI&A.

It was in the course of this presentation that OI&A became aware of a potentially viable off-the-shelf tool called "Riverglass," which is currently being used successfully at the Illinois State Fusion Center to support intelligence analysis. Riverglass uses a "federated" search capacity; that is, the data can be accessed by the system remotely. OI&A prefers this type of data access capability because the information does not have to be brought into a central location prior to system use. Also, because the system is commercially available, some users believe that it would be easier to maintain than a custom-built solution. OI&A expressed interest in Riverglass and requested that S&T test it as a potential candidate to meet its needs.

Components Have Not Agreed to Accept Ownership of ADVISE

Because S&T did not adequately involve DHS stakeholders in the process to identify system needs, solutions, and program strategies, and also did not sufficiently evaluate technical alternatives, the components are not convinced that they need ADVISE and thus are not committed to the system. DHS component leaders also are not sure that the benefits of ADVISE outweigh the costs and have not agreed to accept ownership for the system after the pilot has been completed. Figure 8 shows the major DHS organizations at which

ADVISE Could Support Intelligence Analysis More Effectively

S&T has either demonstrated or piloted ADVISE, along with their decisions concerning adoption of the system or not.

ADVISE CUSTOMER BUY-IN	
DHS CUSTOMER	STATUS OF ADVISE
Office of Intelligence and Analysis	DECLINED SYSTEM
Customs and Border Protection Office of Strategic Trade	DECLINED SYSTEM
Immigration and Customs Enforcement	PARTIALLY DECLINED SYSTEM
Bio-defense Knowledge Center*	PILOT - Currently Suspended
All Weapons of Mass Effect*	PILOT - Currently Suspended
Note: There are no commitments from customers to take ownership of ADVISE. As of March 7, 2007, all ADVISE testing and development activities were suspended.	
* Internally-funded S&T Program, not an external customer.	

Figure 8: ADVISE Customer Buy-in

Specifically, OI&A leadership have declined ADVISE, stating that for the moment they will continue to use their existing tools until the appropriate off-the-shelf solution can be determined and acquired. One OI&A official said that even if ADVISE provided slightly better functionality than other off-the-shelf systems, the preference would be to adopt an off-the-shelf solution that is easy to maintain and operate versus a government-built solution like ADVISE. Also, Customs and Border Protection, Office of Strategic Trade officials declined the system, saying that ADVISE is too expensive to set up and maintain. Lastly, Immigration and Customs Enforcement has declined ADVISE, but has expressed interest in the visualization part of the system that would allow them to view information better from within their existing system. S&T program management have stated that without identifying a customer to help pay for ADVISE operations and maintenance costs by 2008, the ADVISE program will come to an end.

Recommendations

To ensure effectiveness of the ADVISE program and the management of other R&D efforts, we recommend that the Under Secretary for Science and Technology:

1. Develop and document an R&D process for S&T and communicate this process to IT program management.
2. Ensure that business cases are developed for R&D efforts as a means of addressing critical program management activities.
3. Appoint an S&T privacy point of contact to act as a liaison with the DHS Privacy Office to help ensure that privacy issues are addressed in a timely manner.
4. Coordinate with OI&A management and the Information Sharing and Collaboration Branch to create a data requirements and access strategy that includes, at a minimum, defining and documenting the process to

ADVISE Could Support Intelligence Analysis More Effectively

-
- obtain access to internal DHS databases and information from external sources.
5. Define usability requirements and related performance measures to ensure that future data mining technology implementations are sufficiently user-friendly to enable DHS analysts to use them effectively.
 6. Involve DHS stakeholders in the IT acquisition process to ensure the system will meet their needs.
 7. Ensure program management conducts a comparative analysis of available tools to determine whether or not they meet customer needs and provide viable alternatives to ADVISE.

Management Comments and OIG Evaluation

We obtained written comments on a draft of this report from the Under Secretary for Science and Technology. We have included a copy of the comments in their entirety at Appendix B.

In the comments, the Under Secretary for Science and Technology disagreed with many of the findings and recommendations from the report, stating that there were several areas in the report that needed to be corrected in order to provide an accurate picture of the ADVISE program. With the exception of our fourth recommendation regarding coordination on information sharing requirements, the Under Secretary neither concurred nor non-concurred with our recommendations. The Under Secretary provided detailed comments and supporting documentation directed at the overall findings of the report and recommendations, as well as a list of specific comments to clarify statements in the report believed to be inaccurate.

We have reviewed the Under Secretary's comments and made changes to the report as appropriate. However, we disagree with several of the major issues that the Under Secretary raised in the response to our draft report. The following is our evaluation of the issues raised, grouped in line with our report recommendations.

Documented R&D Process:

Regarding recommendation 1 that S&T develop, document, and communicate an R&D process for IT program management, the Under Secretary stated that the directorate's R&D programs follow a structured process and are reviewed by multiple management forums, such as the S&T Requirements Council. The Under Secretary also said that S&T's current IPT processes help satisfy this recommendation. We are aware of the multiple councils and forums that S&T has in place to manage R&D efforts; however, they do not provide a clear R&D process for program managers to follow. We reviewed the documents that the Under Secretary provided on the multiple councils and forums, but found that they also do not address our recommendation that the

ADVISE Could Support Intelligence Analysis More Effectively

directorate provide guidance on activities, such as conducting privacy assessments and developing business cases that need to be performed as part of R&D program management.

Business Case:

Concerning recommendation 2, we disagree with the Under Secretary's determination that ADVISE is not an IT system and therefore does not require an OMB Exhibit 300 business case. Specifically, OMB and department guidance do not exclude R&D projects such as ADVISE from the OMB Exhibit 300 business case process. The DHS Guide to Information Technology Capital Planning and Investment Control also holds program managers responsible for completing business cases. In addition, a recent draft of DHS Management Directive 1400 specifically requires formal business cases for R&D projects, such as ADVISE, that meet funding thresholds for Investment Review Process oversight.

As we state in our report, if S&T had developed a formal business case for the ADVISE program as required, it would have been beneficial in addressing certain key program management activities, such as aligning the effort with customer needs, identifying alternative technical solutions, and determining data requirements and potential effects on privacy, which were overlooked. As the Under Secretary suggests, using the Capstone IPT concept may assist in defining requirements and getting signed Technology Transfer Agreements in place and ensuring commitment to delivery of technologies to address customer needs. However, this IPT concept alone does not address the full intent of our recommendation.

Privacy:

In response to recommendation 3, the Under Secretary stated that privacy law and DHS Privacy Office guidance on assessing privacy impacts do not apply to ADVISE for a number of reasons. First, the Under Secretary asserted that ADVISE is a tool set and thus not a system, requiring such privacy assessments. However, we do not direct our recommendation at conducting privacy assessments on a technical tool. Rather, we recommend completing privacy assessments for implementation of the holistic ADVISE solution which, as piloted, has involved the use of personally identifiable data that must be protected. ADVISE program managers did not begin the privacy assessment process until well after the pilot programs were already using personally identifiable information; this effort is still in process. Consequently, our report recommends that S&T appoint a privacy point of contact to act as a liaison with the DHS Privacy Office to help ensure that the privacy assessments are completed and that related issues are addressed in a timely manner.

Second, the Under Secretary misinterprets our use of the term “operational” to describe the ADVISE pilots. With the term “operational pilot,” we simply are restating ADVISE program officials’ description of the pilots, recognizing that they were conducted using live data. Indeed, during our audit, we found that several ADVISE pilots were conducted with personally-identifiable information prior to S&T having completed privacy assessments as required. Further, the Under Secretary states that the data was only used in the ADVISE pilots for a short period of time and was never used in an operational mode for decision-making. However, our audit work shows that the data was used in pilot systems for one to two years. Additionally, on at least one occasion, the data was used to produce classified intelligence information.

Third, the Under Secretary interprets our report as stating that ADVISE program managers neither conducted the appropriate privacy assessments and analysis, nor prepared related documentation. We do not say that program managers did not undertake this responsibility. Rather, our report states that S&T’s failure to properly address privacy issues in a timely manner *prior to* deploying the three ADVISE pilots had the ultimate effect of bringing the program to a halt. The additional information that the Under Secretary provides on time frames for conducting the pilots provides no new insights and further substantiates our findings. Specifically, the time frames do not differ greatly from the dates that the DHS Privacy Office provided, which we outlined in our report.

Fourth, the Under Secretary suggested that we change the name of the Bio Defense Knowledge Center pilot that we discuss in our report. We disagree. Our discussion refers to an ADVISE pilot conducted at the Bio Defense Knowledge Center since 2004, not to any additional pilot projected for later in 2007. A copy of documentation that DHS provided to congressional staff shows that the pilot was operational beginning in 2004.¹⁴ Further, during our visit to the center, we also received a demonstration of the pilot, showing that it was underway and contained personally identifiable information.

Lastly, we closed our recommendation on privacy coordination, given the Under Secretary’s statement that an S&T liaison to the DHS Privacy Office was appointed recently.

Data Access:

The Under Secretary stated that S&T is not directly responsible for data access at OI&A. We agree with this assertion. However, as we state in our report, without first determining what data was needed and how it would be accessed, OI&A analysts had no effective means of evaluating the utility of

¹⁴ *Threat Awareness Portfolio, FY 2007 TAP Budget*, DHS Briefing to Homeland Security Appropriations Subcommittee Staff, April 21, 2006.

the system during the pilot phase. For example, OI&A analysts and ADVISE program officials that we interviewed indicated that limited data access posed significant challenges to testing and evaluating TVIS.

The Under Secretary concurred with our recommendation that S&T coordinate with OI&A to create data requirements and an access strategy. However, because this was not done early on, S&T did not fully understand user requirements for an automated means of easily processing and analyzing large amounts of unstructured data. Although the Under Secretary stated that extracting facts and relationships from unstructured text accurately is very difficult and time consuming, this is precisely what ADVISE must do to address the needs of the intelligence analyst user community. Without such utility, analysts find limited value in using ADVISE and continue to rely upon their existing systems instead.

Further, although the Under Secretary stated that the timeline for TVIS is incorrect, he does not specify what revisions are needed. As depicted, our timeline reflects documentation that Pacific Northwest National Laboratory provided to us that TVIS went “on-line January 2005.”

Usability and Performance Measures:

In response to recommendation 5, the Under Secretary disagreed with our assessment of ADVISE usability, and provided additional information on usability tests conducted at the Interagency Center for Applied Homeland Security Technology using pre-loaded data and involving analysts from various backgrounds. We updated our report with the results of this test, which was completed after our audit fieldwork had ended. However, in his response to the recommendation, the Under Secretary misinterprets the message of our report, which addressed whether or not analysts at OI&A found the pilot system, broadly speaking, useable when applied to their specific intelligence work and not the usability of the ADVISE user interface alone. As we stated in the report, OI&A analysts indicated that preparing data for ADVISE processing was difficult and time consuming, which led to limited use of the system.

The Under Secretary neither concurred nor non-concurred with our recommendation to define usability requirements and related performance metrics to ensure that future data mining efforts will be sufficiently user friendly to support analysts. Instead, the Under Secretary discussed the goals of the new IPT process, which include developing capability gaps, identifying related performance measures, defining usability, and incorporating that definition into program plans. We believe the IPT process is an effective step toward addressing our recommendation and look forward to receiving additional information on the results of IPT efforts.

Stakeholder Involvement:

In response to recommendation 6, the Under Secretary said that S&T effectively communicated and coordinated with OI&A system users during pilot activities. We agree that S&T provided OI&A analysts with on-site support and training; however, we determined that communication with leadership regarding the ADVISE acquisition was lacking. For example, as we stated in our report, S&T did not coordinate effectively with senior OI&A executives to ensure their commitment to adopting ADVISE as a solution for their intelligence analysis needs.

The Under Secretary disagreed with our statement in the report that OI&A had declined to be an ADVISE customer. The Under Secretary questioned how we had made this determination, asserting that OI&A has not made a decision yet on acquiring ADVISE. S&T provided us with a copy of an email in an attempt to disprove our statement. However, we were unable to rely on it for support as sender and recipient information on the document had been redacted. As such, we stand by our determination. During our audit fieldwork, the senior OI&A decision maker told us specifically that, given the privacy and data mining concerns about ADVISE, as well as the availability of off-the-shelf alternatives, the component likely would not pay to acquire the system. This official said that OI&A would continue to use existing tools until an appropriate IT solution could be identified and acquired.

Additionally, the Under Secretary did not concur or non-concur with our recommendation to involve DHS stakeholders in the IT acquisition process as a means of ensuring that the system will meet their needs. The Under Secretary countered that S&T does not perform IT acquisitions because that is a function of the DHS CIO. Nonetheless, S&T's recent introduction of the IPT process, involving stakeholders at all levels, is a step in the right direction and may help in involving leadership and gaining their commitment to R&D efforts.

Comparative Analysis:

The Under Secretary did not concur or non-concur with our recommendation 7 that a comparative analysis of available tools be conducted to determine if the current tools meet customer's needs and provide viable alternatives. The Under Secretary countered this recommendation by stating that S&T has already conducted an alternatives analysis. We agree. ADVISE program staff briefed senior OI&A Management on a comparative analysis of the tools on March 15, 2007. However, S&T conducted this analysis two years after the system had already been piloted. Further, as we state in our report, S&T's presentation to OI&A leadership on the results of this analysis was too technical and did not convince the leadership that ADVISE was unique and the right solution in comparison with other potential off-the-shelf tools.

ADVISE Could Support Intelligence Analysis More Effectively

The Under Secretary incorrectly interprets our report as stating that ADVISE will replace Analyst's Notebook. Rather, our report states that Analyst's Notebook, similar to ADVISE, provides analysts with the ability to depict connections between people and organizations. With this statement, we compare the tools, but do not suggest that ADVISE will replace Analyst's Notebook.

Other Topics of Concern:

As part of his response, the Under Secretary provided a table of detailed comments cross-referenced to specific pages of our report. We reviewed the comments and made changes to our report as appropriate. Many of the comments related to our report recommendations, which we have addressed above.

However, the Under Secretary provided an additional comment that our report implicitly compares the defunct Total Information Awareness (TIA) system to ADVISE. Rather, we mentioned TIA as part of the background discussion of the report to illustrate the challenge of balancing privacy assurance with data mining processes. We do not specifically compare ADVISE with TIA.

The Under Secretary also stated that our report should address GAO's recommendation that S&T conduct a privacy assessment on the ADVISE system alone, even prior to entering data into the system. However, our report does not make this recommendation; as such, it is not appropriate for us to address this issue. Nonetheless, as we indicated in our report, privacy should have been assessed in a timely fashion for each ADVISE pilot.

As background for this audit, we researched and reviewed IT laws, regulations, and other federal guidance applicable to DHS' responsibility for data mining to determine terrorist activity. We reviewed prior GAO and DHS OIG reports related to data mining. We searched the Internet to obtain testimony, reports, documents, and news articles regarding DHS' data mining approach and the use of data mining systems. Additionally, we coordinated with GAO to ensure that an audit it was conducting did not overlap with our audit objectives. Using this information, we designed a data collection approach that consisted of focused interviews and documentation analysis. We developed a series of questions and discussion topics to facilitate our interviews.

We interviewed DHS officials and staff at S&T and OI&A to obtain an understanding of DHS' approach to using data mining for determining potential terrorist activity. These officials discussed their roles, responsibilities, and activities related to planning, developing, testing, and implementing ADVISE. We collected and reviewed numerous documents from DHS officials about their plans and current initiatives for ADVISE.

Further, we visited various technical facilities to gain an understanding of their operations and involvement in development, testing, and deployment of ADVISE. We also met with potential customers of the system to learn about their experiences with S&T program and project management throughout the system development and transition process. Specifically, we visited:

- The Interagency Center for Applied Homeland Security Technologies, a state-of-the-art independent testing facility, operated by Johns Hopkins University in Laurel, MD. The Center plays an instrumental role in testing and evaluating the ADVISE system using fabricated synthetic data. The Center's officials provided their perspectives on ADVISE program management, communications, and training.
- The Lawrence Livermore National Laboratory in Livermore, CA, and Pacific Northwest National Laboratory in Richland, WA, to understand ADVISE requirements definition and development, and to observe system operations using real data. While at Livermore, we visited the Biodefense Knowledge Center and the All-WME at Livermore to understand how ADVISE is used to contain bio-terrorism and terrorism using weapons of mass effect. We interviewed contractor personnel there, focusing on implementation of ADVISE, as well as business processes, communication and coordination with DHS, and systems training. Where possible, we obtained reports and other materials to support the comments and information they provided during the interviews.

Appendix A

Scope and Methodology

- Immigration and Customs Enforcement, Customs and Border Protection, and the Office of Intelligence and Analysis to gather their feedback on interaction with S&T and any system implementation challenges.

We limited our review of the privacy implications of ADVISE to those aspects not covered in the GAO's review of ADVISE, particularly OI&A.

We conducted our audit from October 2006 through March 2007. We performed our work pursuant to the Inspector General Act of 1978, as amended, and according to generally accepted government auditing standards.

The principal OIG points of contact for the audit are Frank Deffer, Assistant Inspector General for Information Technology Audits, and Sondra McCauley, Director, Information Management. Major contributors to the audit are identified in Appendix C.

Appendix B Management Comments to the Draft Report

Under Secretary for Science and Technology
U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

June 1, 2007

Frank Deffer
Assistant Inspector General, Information Technology
Office of the Inspector General
Department of Homeland Security
Washington, D.C. 20528

Dear Mr. Deffer:

The Department of Homeland Security's Science and Technology (S&T) Directorate appreciates the opportunity to review and comment on the Office of the Inspector General's (OIG) draft report titled "ADVISE Could Support Intelligence Analysis More Effectively." S&T disagrees with many of the findings and recommendations from the report.

There are several areas in the report that need to be corrected in order to provide an accurate picture of the ADVISE program. S&T has provided detailed comments and supporting documentation. S&T's comments are directed at the overall findings of the report as well as the OIG's recommendations. S&T has included a list of more specific comments to clarify inaccurate statements. Some of the major concerns are highlighted below.

As repeatedly indicated in S&T literature, briefed to the Hill and numerous DHS officials, and finally, as acknowledged by the DHS Privacy Office in its own comments on the subject, the ADVISE tool set is little more than an empty framework to which data must be applied. Neither section 208 of the E-Government Act of 2002 (Pub. L. 107-347) nor current Privacy Office guidance contemplate the conduct of PIAs for tools such as ADVISE. Both 208 and Privacy Office guidance are predicated upon use of PII. They do not clearly apply to a manipulative tool, like the ADVISE framework. The IG report should address this inconsistency as it has significant implications in determining the correct documentation needed for the ADVISE framework and the ADVISE evaluation and pilots.¹

¹ Based on a meeting in 2004, the Privacy Office advised that the Privacy Impact Assessment document was not an appropriate vehicle for assessing the potential privacy impacts of the ADVISE Technology Framework, because as a set of generic capabilities, the Framework does not collect, maintain or use data and the PIA document is focused on how information is to be used. Each deployment of the Framework, including pilots, that used personally identifiable information would be subject to the PIA requirement.

www.dhs.gov

In several instances, the report refers to the pilots as being “operational.” The pilots were never used in an operational mode for decision making. The data loaded in the system only demonstrated how ADVISE could be used as an analytical tool. The purpose of the ADVISE pilots was to test the functional capability of the framework. This is different from an operational system that directly supports operational missions of the Department. The short duration of a pilot as well as the short life-span of data in the system also distinguishes a pilot from an operational system.

The draft report asserts that the Office of Intelligence and Analysis (I&A) has officially declined to be a customer. However, according to I&A leadership, I&A has not made a decision regarding ADVISE. Before making a decision on ADVISE, I&A will look at the functionality, supportability, and ease of use of the current generation of commercially available tools in comparison to ADVISE. In the new S&T alignment, legacy research and development programs that do not have an identified customer will be gracefully concluded and the technology shelved in the event a future need arises.

It is inaccurately stated in the report that ADVISE is complicated, difficult to use, and time consuming to operate. An evaluation of ADVISE was conducted at the Interagency Center for Applied Homeland Security Technologies with a group of analysts using simulated test data. At the conclusion of the evaluation, the users reported the tools to be efficient and effective, and most were able to use the tool with minimal training.

The draft report notes a lack of communication between S&T and I&A. From 2003 to the present, S&T has provided I&A with on-site support, training, and maintenance for the Threat-Vulnerability Integration System directly from the national laboratories. S&T has also provided numerous formal and informal presentations and program reviews to I&A.

Thank you again for the opportunity to comment on the draft report. We request that a copy of this letter and our detailed comments be including as an Annex or Appendix to the final report.

Sincerely,



Jay M. Cohen
Under Secretary for Science and Technology

S&T Responses to Draft Report OIG Review of the Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE) Program

The following comments address S&T's concerns with the Department of Homeland Security's Office of Inspector General's report titled "ADVISE Could Support Intelligence Analysis More Effectively." The comments are arranged in the following order:

1. Comments regarding general themes expressed in the report;
2. Comments on Biodefense Knowledge Management Systems (BKMS) and Biological Knowledge Center (BKC)
3. Comments on specific language in the report; and
4. S&T's response to the reports recommendations.

A separate section on BKMS and BKC is warranted as the programs are very distinct from other ADVISE actions. This distinction is not reflected in the OIG report.

In addition, S&T is providing an appendix that contains several supporting documents from ADVISE program managers.

1. General Themes

A. R&D Planning Approach Does Not Effectively Support ADVISE

Audit Findings:

- Program Management Unaware of Guidelines for Conducting R&D Projects
- Business Case Not Prepared for ADVISE

S&T Response:

OIG has a significant misconception that ADVISE is an IT system. The heart of the problem is that ADVISE was identified by S&T as an **R&D project**, and *not as an IT system*. ADVISE correctly followed guidelines and procedures for R&D projects (See tab 1, FY 2004 Office of Research and Development Execution Guidance: ADVISE Knowledge Management System and tab 2, Overview of Department of Homeland Security Intelligence Science and Technology Requirements (unclassified briefing). For instance, ADVISE was reviewed by management with other R&D projects such as R&D detector technologies or BioWatch. All S&T R&D programs followed a structured process and were reviewed in multiple forums by S&T management and external peer review (see appendix tab 3, SRC Process Document, for more information on the review process). Management Directive 10120 Science and Technology Requirements Council (SRC) applied to R&D programs, including ADVISE. Management Directive 10120 states:

"In response to section 302 of the Homeland Security Act of 2002, the SRC is chartered as a senior-level review board responsible for soliciting, validating, and prioritizing science and technology requirements from all DHS organizational elements. The SRC will make recommendations to the Under Secretary for Science and Technology regarding program priorities and the allocation of S&T resources across the DHS mission areas to develop the most effective S&T

1

program possible using existing resources. The SRC will prioritize remaining programs requiring additional resources. The Under Secretary will consider these recommendations in conjunction with externally derived S&T requirements (e.g., statutory, national guidance).”

Portfolio managers were required to identify how their programs met the SRC requirements. The Threat Awareness Portfolio, under which ADVISE resided, aligned with SRC requirements (see appendix tab 4, Threat Vulnerability Testing and Assessment Portfolio, for more information).

This management directive also specifies:

“The SRC will report proposed IT investments and program initiatives to the EAB (Enterprise Architecture Board) as necessary... The SRC process and associated products will fully support the DHS investment review process and timelines.”

OIG requested an OMB 300 as part of its review of ADVISE, which includes a business case. S&T determined that an OMB 300 was not necessary as ADVISE was not an IT system, however, this does not imply that ADVISE proceeded without a business case or requirements. The draft report ignores the processes used by S&T to develop programs and plans for ADVISE. The following process was used in place of the OMB 300:

- S&T had in place an Integrated Project Team (IPT) process that was operational for the ADVISE portfolio from early 2004 through early 2006. The IPTs were portfolio based and comprised representatives (one each) from the four S&T Offices at the time, namely, Plans, Programs, and Budgets (PPB later PPR); Research and Development (ORD); Homeland Security Advanced Research Projects Agency (HSARPA); and Systems Engineering and Development (SED).
- Those IPTs were supported by a formal requirements process between the Directorate and DHS components. The centerpiece was the S&T Requirements Council (SRC), which was chaired successively by the Under Secretary, the Assistant Secretary for PPB, and the Assistant Secretary for Research and Development. Component representatives sat on the Council, which met on a quarterly basis.
- Each portfolio’s program and project plans were reviewed every Spring of the years 2004, 2005, and 2006 by the S&T Corporate Review Board (CRB), which in the later years was called the Executive Review Team (ERT). The CRB or ERT comprised S&T’s Assistant Secretaries, and the requirements collected in the SRC process were addressed in the deliberations

In hindsight, it may be convenient to fault the structure, operations, and ultimate effectiveness of the IPTs and suggest that the Directorate adopt an IPT process similar to the one now being used. Nonetheless, saying that there was no IPT nor similar business case requirements process is not accurate.

B. System Has Not Been Effectively Implemented to Meet Mission Requirements

Audit Findings:

- Privacy Impacts Not Determined for ADVISE
- Limited Data Access
- System Usability Could be Improved

S&T Response:

The draft OIG report states that ADVISE program managers did not conduct appropriate privacy assessments or analysis, nor prepared related documentation; including applicable Privacy Threshold Analyses (PTA) and Privacy Impact Assessments (PIA). ADVISE has submitted PTAs for each of its pilots and PIAs where necessary. The DHS Privacy Office is in the process of evaluating the PTAs and PIAs submitted for the various pilots.

The table below provides submission dates and current status of relevant privacy documentation related to the ADVISE evaluation and pilots. This information should be included in the OIG report.

Table 1: PTA and PIA Status for ADVISE-related Pilots and Evaluations

Name of Pilot or Evaluation	PTA status	PIA status
ADVISE Evaluation at the Interagency Center for Applied Homeland Technologies (ICHAAT)	PTA Approved by the DHS Privacy Office 12/06.	No PIA required.
Threat-Vulnerability Integration System (TVIS)	Submitted to the DHS Privacy Office, 6/06.	PIA required. First PIA submitted, 2/07; updated PIA submitted, 4/07. Currently under review by the DHS Privacy Office.
ADVISE-Based Evaluation of All Weapons of Mass Effect.	Submitted to the DHS Privacy Office, 7/06. Redrafted PTA submitted, 3/07. Updated PTA submitted, 4/07	PIA initially required and submitted, 2/07. Revised PIA submitted, 4/07. Currently under review by the DHS Privacy Office.

Table 2: PTA and PIA Status for Biodefense Knowledge Management System (BKMS)-related Pilots

Name of Pilot	PTA status	PIA status
BKMS Pathogen Demonstration	PTA approved by the DHS Privacy Office on 4/2/2007.	No PIA required.
BKMS BioEncyclopedia Pilot	PTA submitted to the DHS Privacy Office on 3/7/2007;	Currently under review by the DHS Privacy Office.

BMKS ADVISE Pilot	On hold, will be ready to pilot in November 2007 timeframe. PTA will be submitted in advance of potential release date.	Currently, not applicable.
-------------------	---	----------------------------

In addition, the report states on page 8 that “it was not clear to ADVISE program management that the system needed a privacy assessment” and continues, saying “the responsibility for performing and documenting privacy impact assessments was not brought to the attention of ADVISE program managers in the early states of the initiative.” These statements are not completely accurate – ADVISE contains no data, it is a framework. Privacy documentation is required for ADVISE evaluations, demonstrations and pilots when they contain data. In addition, S&T met with the DHS Privacy Office in 2004. At that time, the Privacy Office was aware of ADVISE activity and did not require PTAs or PIAs. Following up on previous conversations, ADVISE program managers provided the DHS Privacy office with briefings and other information related to ADVISE in February and March of 2006. Please see the tab 5 of the appendix for a historical record of these interactions.

**Now on
Page 16**

S&T disagrees with OIG’s perception that limited access to data in ADVISE hampered the program’s performance. For instance, on page 14 the report incorrectly asserts that TVIS was designed to work only with structured data. TVIS is agnostic about the data format – it is structured to work with an ontology. What is true is that the Office of Intelligence and Analysis (I&A) does not have much structured data; what is of value to them lies within unstructured data. The point of the OIG report should not be that ADVISE fails to provide successful analysis of unstructured text to meet its goal, but that the process of extracting facts and relationships from unstructured text accurately is very difficult and time consuming and something analysts have not shown an interest in devoting time and energy.

**Now on
Page 13**

Also on page 14, the report states that “S&T did not take sufficient action to ensure access to the data needed for TVIS pilot demonstration.” S&T is not responsible for I&A data access as I&A owns the data, which is already available to their analysts. ADVISE worked with I&A to understand what data sources were their most important sources (S&T did this survey, not I&A) and did attempt to access I&A data. S&T placed support personnel within I&A to coordinate access to data and analysts.

The draft report states several times that the ADVISE pilot(s) are complicated, difficult to use, and time consuming to operate. The draft report also states that training on the ADVISE system is too complex and time consuming for analysts to support. This is not true. An evaluation of ADVISE was conducted at the Interagency Center for Applied Homeland Security Technology (ICAHST) in early 2007. The test used simulated data and involved two groups of intelligence and criminal analysts who had never seen nor heard of ADVISE. Each group of five was trained on the ADVISE tools set, and then applied each training session to a related task to solve. By the end of the week, all analysts were successfully using the ADVISE tools to solve scenarios. In some cases, analysts were successfully using the tools within two days. The users reported the tools to be efficient and effective within the week, and something they wished they had in the

performance of their duties. Additional details regarding the ICAHST evaluation are found in tab 6 of the appendix. See enclosed CD for videos of the ICAHST evaluation and overview.

C. DHS Components Have Not Committed to ADVISE

Audit Findings:

- Ineffective Communication and Coordination with Stakeholders
- Lack of Alternative Analysis
- Components have not Agreed to Accept Ownership of ADVISE

S&T Response:

The draft report points to lack of communication from S&T with the customer, namely I&A. From 2003 to the present, S&T has provided I&A with on-site support, training, and maintenance for TVIS directly from the national laboratories as well as numerous formal and informal presentations and program reviews (see tab 2, Overview of Department of Homeland Security Intelligence Science and Technology Requirements; and tab 7, Vulnerability, Testing and Assessment (TVTA) Requirements Meeting Notes, in the appendix for examples of interactions with I&A). Senior engineers were placed with the analysts specifically to interact with users and systems staff.

Regarding OIG's assertion that ADVISE failed to conduct an alternative analysis, a comparative tools analysis briefing was presented by ADVISE program staff to senior I&A Management on March 15, 2007. As a result of that briefing, a proposal was presented to I&A on April 12, 2007 to demonstrate integration between TVIS and Intelligence & Information Fusion (I2F) in support of a use case involving weapons of mass effect (WME) analysis.

The report makes comparisons between ADVISE and Analyst's Notebook on page 14. ADVISE is not designed to replace Analyst's Notebook (which is more aptly described as a report writing tool), as the report implies, but instead provide analysts with another analysis tool. The report fails to take into account that Analyst's Notebook requires analysts to manually enter data before any analysis can occur. Analyst's Notebook does not contain an automated data loading process. Failure to acknowledge this important detail provides the reader with an inadequate view of what Analyst's Notebook is and what it can provide.

The report asserts that I&A has officially declined to be a customer (page 21). However, according to I&A leadership, I&A has not made a decision regarding ADVISE (see tab 8 of the appendix for an e-mail from senior I&A staff). It is unclear how OIG determined that I&A had "declined" the ADVISE system.

2. Biodefense Knowledge Management Systems (BKMS) and Biological Knowledge Center (BKC) Comments:

The BKC as a program was stood up in June 2004. The BKMS ADVISE pilot was not operational in 2004. The BKMS was designed in 2006. Prior to this, separate technologies (non-operational) were being developed.

The BKMS ADVISE pilot is not operational. The differential for pilot systems is the purpose and life-span of the personally identifiable information that would be used. The purpose of a pilot system may be to test the functional capability of the modules within the pilot system. This is qualitatively different from the purpose of an operational system: to directly support operational missions of the Department.

The description below hopefully clarifies the BKMS development efforts. Previous documents did not use consistent terminology and as such lead to significant confusion. The following figures are wrong:

- Figure 2 is incorrect. BKMS ADVISE pilot was NOT OPERATIONAL in Oct 2004. It is still in development phase (see below).
- Figure 5 is incorrect. BKMS ADVISE pilot was NOT OPERATIONAL in Oct 2004. It is still in development phase (see below).
- Figure 6 is incorrect. BKMS ADVISE pilot was NOT OPERATIONAL in Oct 2004. It is still in development phase (see below).

“The DHS Biodefense Knowledge Center (BKC) is a leading-edge biodefense analysis center using spiral development to build knowledge management systems to help DHS users analyze and characterize biological threats posed by terrorists. The BKC plans to use ADVISE to help understand biological threats and generate analyses. As part of the spiral development process, a series of demonstrations and pilots are planned. The BKC pilots will reside on Official Use Only (OUO), Secret (Homeland Secure Data Network), and Top Secret (Joint Worldwide Intelligence Communication System) networks to support DHS users at the appropriate classification level.

Currently, the BKC has one demonstration and two systems under development. A demonstration of the Biodefense Knowledge Management System (BKMS) related strictly to pathogens (BKMS Pathogen Demonstration) is currently under review by the DHS Privacy Office. The current pilot version of the Biodefense Knowledge Management System (BKMS) is based on a simplified semantic graph design and is not an ADVISE deployment since it does not use any ADVISE technology. This version is called the BKMS BioEncyclopedia Pilot. Several major open-source biodefense-related datasets will be loaded into the BKMS BioEncyclopedia. Upon approval, this pilot will be released to a limited number of DHS users to determine system effectiveness. This release is tentatively scheduled for June 2007.

6

The BKC has been actively working on the next release of the BKMS, called the BKMS ADVISE Pilot. Based upon the ADVISE toolset, this version will build upon ADVISE's analysis, security and privacy capabilities to significantly enhance the overall capabilities of the knowledge management system. The goal of this pilot is to determine the utility of the BKMS-ADVISE system to meet DHS knowledge management and information retrieval needs to better understand biological threats. Scheduled to be released in October-December 2007, this version will also build upon knowledge gained from the BKMS BioEncyclopedia Pilot.

The BKC and the BKMS pilots will provide the DHS users:

- Curated biodefense-related information sources relevant to DHS analysts
- Information fusion capabilities to support knowledge discovery in the biodefense domain
- Information in new areas such as emerging technologies related to biothreats

Privacy status: A Privacy Threshold Assessment (PTA) was submitted for the BKMS Pathogen Demonstration. This demonstration has no personally identifiable information. A PTA and PIA have been submitted for the BKMS BioEncyclopedia Pilot. The PTA and PIA for the BKMS ADVISE Pilot will be submitted in advance of the planned release. The BKC was established in 2004. The BKMS ADVISE pilot is not operational. This pilot is under development with a planned release in late 2007 pending DHS approval. The BKMS Pathogen Demonstration approved by the Privacy Office on 4/2/2007 and the BKMS BioEncyclopedia Pilot awaiting approval are not ADVISE based. The Privacy Threshold Assessment was first submitted 3/12/2007. Several updates to the PTA have been submitted to the Privacy Office, the most recent version was submitted 6/1/2007.

3. Specific Comments

Page	OIG Comment	Response
Page 3	The report states "In addition, program managers did not address privacy impacts before implementing three pilot initiatives to support ADVISE"	The sentence should read that program managers did not "fully address privacy impacts..." The narrative discussion is basically correct that S&T program managers made a visit to the nascent Privacy Office, briefed the program, and were not instructed to do any follow-up. Much of this failure can be attributed to the fact that these policies and procedures were still in their infancy. It is important that these "failures" be put in the correct historic

**Now on
Page 6**

		perspective.
Page 5:	“With funding by S&T, the Biodefense Knowledge Center at Livermore uses this pilot system to help integrate biodefense information and anticipate and respond to bioterrorist attacks.”	This sentence should be changed from “uses a pilot system” to “is developing a pilot system.”
Pages 5-6	The report provides a timeline for ADVISE efforts.	The timeline is incorrect. The Threat Vulnerability Integration System (TVIS) actually pre-dates the ADVISE efforts. TVIS was delivered to I&A in January 2004, and had been developed with funding provided to Lawrence Livermore National Laboratory (LLNL) earlier. TVIS was not installed on the I&A network until August 2004, after certification and accreditation was completed. This is another example of how the ADVISE research and development effort is being confused with a particular system deployment.
Page 6	In several instances, the report refers to the pilots as being “operational.” For instance, on page 6, the report says the following: “The pilots used live data, including personally identifiable information, from multiple sources in attempts to identify potential terrorist activity...which become operational in late 2004 to early 2005.”	The pilots were never used in an operational mode for decision making. The data loaded in the system (which was already resident at I&A) demonstrated how ADVISE could be used as an analytical tool. S&T supplied documents supporting this assertion to OIG.
Page 6, paragraph 2, first sentence	The report states that the ADVISE pilots “use a data mining approach.”	Use of the term “data mining” to categorize and describe ADVISE fails to account for the major differences between a tool such as ADVISE and data mining. ADVISE uses a technique called data fusion and a structured ontology with techniques like pattern matching. While ADVISE could be used for data mining, that determination is made based on how ADVISE is used on a case-by-case basis and the data that is loaded into the framework. On its own, ADVISE is not a data mining tool in that there is no inherit data in the framework.

Page 6	The report makes an implicit comparison between the defunct Total Information Awareness (TIA) and ADVISE.	TIA actively collected, maintained, and processed information; ADVISE has no such functionality – it is simply a tool to which data could be applied. The distinction is critical for purposes of <u>applying privacy requirements</u> .
Page 7	The draft report states that the majority of ADVISE efforts were focused on development and deployment of pilot systems.	This is incorrect. The majority of funding in 2004 and 2005 was used for research and development of the basic framework. Support to pilot activities was included at lower levels. In 2006 the plan was to decrease the R&D component of the work and support pilot activities.
Page 7	The report contains a cross reference to the GAO report which states that “DHS immediately conduct a privacy impact assessment of the ADVISE tool and implement privacy controls, as needed, to mitigate any identified risks.”	The ADVISE tool set is an empty framework to which data must be applied. Neither section 208 of the E-Government Act of 2002 (Pub. L. 107-347) nor current Privacy Office guidance contemplate the conduct of PIAs for tools such as ADVISE. Both 208 and Privacy Office guidance are predicated upon use of PII. They do not clearly apply to a manipulative tool, like ADVISE. The IG report should address this inconsistency.
Pages 8 and 9	The report refers to ADVISE as an information technology (IT) project.	The draft report consistently confuses ADVISE with an “IT System.” ADVISE is a framework for managing a suite of information analysis tools. Those tools were provided by the national laboratories as well as commercial firms. In fact, some of the TVTA Portfolio’s funded efforts in 2004 and 2005 specifically focused on commercial tools, such as entity extraction, that could be incorporated into the ADVISE framework. This project was categorized as an S&T R&D project and subject to S&T R&D guidelines and review process. Under the S&T R&D reviews, the review panels could have made the recommendation or comment that

		ADVISE needs to go through the Investment Review Board process – this was never recommended during these reviews.
Page 8	The report states that “the directorate has no structured R&D process in place”	ADVISE followed the S&T process in place performing annual reviews to S&T management (Executive Review Team, etc). ADVISE followed all S&T processes as an R&D project.
Page 10, Figure 4	This page discusses types of data needed and IT alignment to customer’s needs.	S&T anticipated that I&A would have access to more data sources since its inception in 2004. I&A needs have also evolved under senior management.
Page 11	“Despite...ADVISE program managers did not begin this process until after the pilot programs were already operational...DHS Privacy officials told S&T that no such action was required during the initial stages of ADVISE development.”	The Privacy Office advised that the Privacy Impact Assessment document was not an appropriate vehicle for assessing the potential privacy impacts of the ADVISE Technology Framework, because as a set of generic capabilities, the Framework does not collect, maintain or use data and the PIA document is focused on how information is to be used. Each deployment of the Framework, including pilots, that used personally identifiable information would be subject to the PIA requirement. The Privacy Office is currently developing a Privacy Technology Implementation Guide which is better suited to the nature of development Frameworks like the ADVISE Technology Framework and is collaborating with S&T to fit this refined approach to the nature of S&T's research and development work.
Page 11	The report states the following: “For its part, the DHS Privacy Office did not know that S&T had proceeded with implementation of the ADVISE pilot programs with live data, but without addressing privacy matters.”	This text should be changed to: “For its part, the DHS Privacy Office did not know that S&T had proceeded with testing of the ADVISE pilot programs with live data, but without fully addressing privacy matters.”
Page 12, Figure 5	Figure 5 lists ADVISE implementations	BKMS was not operational in October 2004.
Page 13, Figure 6	Figure 6 lists key ADVISE operational systems	BKMS was not operational in October 2004.

**Now on
Page 12**

**Now on
Page 15**

**Now on
Page 15**

**Now on
Page 17**

Page 15	The report states that analysts using BKMS found it to be highly beneficial	BKMS has no external users. It is in testing phase.
Page 15	The report states that "S&T did not involve adequately users early in the design of TVIS."	S&T staff were involved in early on in the development process at I&A in order to develop user requirements and understand needs. S&T also met with the I&A Chief Information Officer (CIO) to discuss TVIS.
Page 16	The report implies ADVISE only worked with I&A at "one point."	Onsite S&T personnel continuously received input from I&A analysts.
Page 16, Second paragraph	The report states "To circumvent the challenges in working with OI&A analysts . . ."	Change to "Due to the challenges in working with I&A analysts . . ."
Page 18	The report states that "S&T did not involve stakeholders in the IT selection process via integrated project teams (IPT)."	IPTs with stakeholders did not exist prior to 2006. Stakeholder input, however, was received from I&A analysts as well as through the SRC review process.
Page 20	The report discusses the need for a framework	<p>The draft report correctly states one of the primary reasons for pursuing the ADVISE research and development program, namely, that other solutions – at present and especially in the past - do not have the capacity to handle vast amounts of information across multiple sources.</p> <p>Individual point solutions for the various components within DHS can be developed and delivered with Commercial Off the Shelf (COTS) and Government Off the Shelf (GOTS) systems, meeting a limited, specific set of requirements. The resulting systems will, unfortunately, require individual operations and maintenance activities. Furthermore, ensuring data integrity and security and enabling collaboration and information sharing, which is key to the need, as the reports states, for "connecting the dots", will require the development and implementation of additional, complex software.</p> <p>The ADVISE efforts were focused on developing a common capability, rather</p>

		than individual customer systems.
Page 20	The report states “In efforts to better and more consistently involve customers in its IT selection process, DHS established ten IPTs . . .”	The IPT process is not limited to “IT selection process.” This is another example of the report mixing R&D projects with IT projects.
Page 21, Figure 8	Figure 8 shows that I&A declined the system.	S&T is not aware that anyone in I&A has declined the system. This has not been communicated to S&T. (See appendix)
Page 21, Figure 8	Figure 8 shows that the BKC Pilot is suspended.	The figure should be corrected to show that the BMKS ADVISE pilot on hold pending the completion of privacy requirements.

4. Audit Recommendations

1. Develop and document an R&D process for S&T and communicate this process to IT program management.

S&T Response: Prior to August, 2006 S&T used the SRC review system to document the R&D process. As cited on page 20, since August, 2006, S&T’s current IPT processes satisfies this recommendation.

2. Ensure that business cases are developed for R&D efforts as means of addressing critical program management activities.

S&T Response: S&T is utilizing a Capstone IPT concept in which an identified DHS customer chairs the various IPTs to work closely with S&T to identify requirements and technology gaps. The result of this process is to get signed Technology Transfer Agreements from the customer for technologies that S&T will deliver to address customer needs. Please see tab 9 in the appendix for IPT templates and tab 10 for preliminary Capstone IPT results.

3. Appoint an S&T privacy point of contact to act as a liaison with the DHS Privacy Office to help ensure that privacy issues are addressed in a timely manner.

S&T Response: Elliott Avidan is the S&T liaison to the Privacy Office. Elliot works under the supervision of the Associate General Counsel.

4. Coordinate with I&A management and the Information Sharing and Collaboration Branch to create a data requirements and access strategy that includes defining and documenting the process to obtain access to internal DHS databases and information from external sources.

S&T Response: S&T currently coordinates with the ISCB and concurs with this recommendation. In addition, S&T participates on the ISCB Program Manager Information Sharing Environment IPT and I&A is the lead on the S&T Capstone IPT for information sharing.

-
5. Define usability requirements and related performance measures to ensure that future data mining technology implementation are sufficiently user-friendly to enable DHS analysts to use them effectively.

S&T Response: The goals of the IPT process include developing capability gaps and defining usability and related performance measures and incorporating those definitions into program plans.

6. Involve DHS stakeholders in the IT acquisition process to ensure the system will meet their needs.

S&T Response: S&T does not perform IT acquisition. IT acquisition is a function of the DHS CIO. In developing its R&D portfolio, S&T is using a Capstone IPT concept in which an identified DHS customer chairs the various IPTs to work closely with S&T to identify requirements and capability gaps. This process will provided signed Technology Transfer Agreements between S&T and the customer for programs that S&T will deliver to address customer capability gaps.

7. Ensure program management conducts a comparative analysis of available tools to determine whether or not they meet customer needs and provide viable alternatives to ADVISE.

S&T Response: A comparative tools analysis briefing was presented by ADVISE program staff to senior I&A Management on March 15, 2007. As a result of that briefing, a proposal was presented to I&A on April 12, 2007 to demonstrate integration between TVIS and I2F in support of a use case involving WME analysis.

Appendix C
Major Contributors to this Report

Information Management Division

Sondra McCauley, Director
Richard Harsche, Audit Manager
Steve Staats, Auditor
Shannon E. Frenyea, Auditor
Anthony Nicholson, Referencer

Appendix D Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative and Intergovernmental Affairs
DHS OIG Liaison
DHS Chief Information Officer
DHS Deputy Chief Information Officer
Directorate for Science and Technology Audit Liaison
Assistant Secretary, Office of Intelligence and Analysis
Office of Intelligence and Analysis Chief Information Officer
Director, GAO/OIG Liaison Office
Under Secretary, Science and Technology
Under Secretary, Office of Intelligence and Analysis

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- **Call** our Hotline at 1-800-323-8603;
- **Fax** the complaint directly to us at (202) 254-4292;
- **Email** us at DHSOIGHOTLINE@dhs.gov; or
- **Write** to use at:
DHS Office of Inspector General/MAIL STOP 2600, Attention:
Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410,
Washington, DC 20528,

The OIG seeks to protect the identity of each writer and caller.