DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Survey of the Information Analysis And Infrastructure Protection Directorate

Notice: The Department of Homeland Security, Office of Counsel to the Inspector General, has reviewed this report and excised information according to the Freedom of Information Act, 5 U.S.C. Section 552, as amended.

Office of Inspections, Evaluations, & Special Reviews

OIG-04-13

February 2004

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, investigative, and special reports prepared by the OIG periodically as part of its oversight responsibility with respect to DHS to identify and prevent fraud, waste, abuse, and mismanagement.

This report is the result of an assessment of the strengths and weaknesses of the program, operation, or function under review. 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, if any, have been developed on the basis of the best knowledge available to the OIG, and have been discussed in draft with those responsible for implementation. It is my hope that this report will result in more effective, efficient, and/or economical operations. I express my appreciation to all of those who contributed to the preparation of this report.

Clark Kent Ervin
Inspector General

Contents

Introduction 1

Results in Brief 1

Background 2

Purpose, Scope and Methodology 3

Programs of the Information Analysis and Infrastructure Protection Directorate (by offices and divisions) 4

The Budgetary Programs of the IAIP 4

Organizational Chart of IAIP 5

Administration and Outreach – Office of the Under Secretary 7

Homeland Security Operations Center 10

Intelligence and Warning - Office of Information Analysis 12

Protecting Critical Infrastructure and Key Assets – Office of Infrastructure Protection 16

Issues for Inspections/Evaluations 21

Hiring Personnel to Work in a Classified Environment Takes a Substantial Amount of Time 21

The Ability of IAIP to Exchange Threat Information Electronically with Partners is Necessary to Fulfill its Mission 22

Maintaining Close Partnerships that Facilitate Unobstructed Information Flows is Crucial to the Success of IAIP 23

The Extent of IAIP's Involvement With the Homeland Security Advisory System is Not Clear 24

IAIP Needs to Develop a Prioritized List of Critical Infrastructure and Assets 24

Contents

Appendices

Appendix A: Summary of IAIP Statutory Functions.. 26
Appendix B: Lead Agencies and Critical Infrastructure Sectors and Key Assets 27
Appendix C: IAIP Response to OIG 28
Appendix D: Major Contributors to this Report.. 29
Appendix E: Report Distribution 30

Abbreviations

CAEO	Competitive Analysis and Evaluation Office
CIA	Central Intelligence Agency
COS	Chief of Staff
DHS	Department of Homeland Security
DoD	Department of Defense
FBI	Federal Bureau of Investigation
FTE	Full Time Equivalent
FY	Fiscal Year
HSA	Homeland Security Act
HQBO	Headquarters Business Office
HSAS	Homeland Security Advisory System
HSC	Homeland Security Council
HSOC	Homeland Security Operations Center
HV/HPS	High Value/High Probability of Success
IA	Office of Information Analysis
IAIP	Information Analysis and Infrastructure Protection Directorate
ICD	Infrastructure Coordination Division
IMRD	Information Management and Requirements Division
IP	Office of Infrastructure Protection
IT	Information Technology
IWD	Information and Warnings Division
NCS	National Communication System
NCSD	National Cyber Security Division
NSTAC	National Security Telecommunication Advisory Committee
NS/EP	National Security Emergency Preparedness
OIG	Office of Inspector General

PPO	Planning and Partnerships Office
PSD	Protective Security Division
RAD	Risk Assessment Division
TTIC	Terrorist Threat Integration Center

Introduction

The Information Analysis and Infrastructure Protection (IAIP) directorate was created to support a key strategic mission of the Department of Homeland Security (DHS). IAIP analyzes and integrates terrorist threat information, mapping those threats against both physical and cyber vulnerabilities to critical infrastructure and key assets, and implementing actions that protect the lives of Americans, ensures the delivery of essential government services, and protects infrastructure assets owned by US industry. IAIP is unique in that no other federal organization has the statutory mandate to carry out these responsibilities under one organizational framework.

The Office of Inspector General (OIG) conducted this survey to learn more about the department's plans for IAIP and to prepare us for more detailed future work as part of our general oversight responsibility for DHS and its component parts. Issues of particular importance to us were:

- The methodology for transferring and integrating the functions and agencies responsible for protecting critical infrastructure into IAIP;
- How IAIP offices and divisions are working (or intend to work) with non-DHS entities to protect critical infrastructure; and
- IAIP's ability to communicate with entities within DHS and other federal, state, local, and private sector partners.

Additionally, we endeavored to determine the obstacles IAIP faces in "standing-up" the organization. We reviewed and analyzed documents pertaining to IAIP and interviewed IAIP officials from May 2003 through July 2003.

Results in Brief

Since its establishment approximately nine months ago, IAIP has faced the daunting task of becoming fully operational as a new directorate, while maintaining the workload it acquired from legacy agencies. In addition to maintaining a full workload, IAIP has also encountered several other complicating factors. For example, during the past nine months, IAIP has been hampered by turnover of key management positions. Also, IAIP has dealt with severe space problems, as many of its personnel are required to work from separate locations throughout the Washington, D.C. metropolitan area, or to work with one or more other people at one workstation at the department's headquarters.

In addition to these difficulties, the OIG has identified several other issues that may warrant future inspections. During interviews, executives within IAIP maintained that the inability to hire personnel who have, or can quickly obtain, the necessary security clearances to work in a classified environment was a major obstacle to IAIP becoming fully operational. Another obstacle often cited by IAIP executives was its inability to connect to secure systems and databases residing at other agencies. Future inspections geared toward making recommendations on how to shorten the clearance process for new hires and assessing the progress made in systems connectivity would help IAIP advance in its mission. Though not identified as a current issue by IAIP executives, much of the future success of IAIP depends on its ability to maintain close partnerships with other federal departments and agencies that have homeland security responsibilities for infrastructure sectors not covered by DHS. Close partnerships with the intelligence and law enforcement communities are also vital to the success of IAIP. A future inspection that measures how well IAIP maintains its partnerships with key outside agencies would help to gauge the effectiveness of IAIP in supporting the overall mission of DHS. Finally, IAIP plays an important role in analyzing threat information in support of the Homeland Security Advisory System (HSAS).[1] However, it is not clear how intelligence will be deemed actionable, or what the intelligence requirements are for the different threat conditions. An inspection that will clarify these matters may promote a more effective, efficient, and economical process for changing the threat condition.

Background

In response to the recognized need for a coordinated, national approach[2] to protect the homeland against potential terrorist attacks, Congress enacted the Homeland

[1] The Homeland Security Advisory System provides a means to disseminate information regarding the risk of terrorist attacks against federal, state, local, and private sector authorities and the American people by characterizing appropriate levels of vigilance, preparedness, and readiness in a series of graduated threat conditions.

[2] Before DHS was created in November 2002, protecting the homeland was primarily a federal responsibility and was mainly coordinated through the military, the intelligence agencies, the Department of Justice, and the Department of State. Since the September 11, 2001 terrorist attack, homeland security has become a national rather than a federal responsibility because the federal government alone cannot protect the entire country.

Security Act (HSA) of 2002, resulting in the creation of DHS. The primary strategic objectives of the DHS are:

- To prevent terrorist attacks within the homeland;
- To reduce the vulnerability of the homeland to terrorism; and
- To minimize the damage and assist in the recovery from terrorist acts that occur within the homeland.

IAIP was vested with responsibility to analyze and integrate terrorist threat information, map threats against both physical and cyber vulnerabilities to critical infrastructure and key assets, and implement actions that protect the lives of Americans, ensure the delivery of essential government services, and protect infrastructure assets owned by U.S. industry. IAIP carries out its mission through the Administrative and Outreach, Intelligence and Warning, and the Protecting Critical Infrastructure and Key Assets programs, as well as the Homeland Security Operations Center.

Purpose, Scope, and Methodology

The objective of this survey was twofold. First, we sought to gain a basic understanding of IAIP, including learning the missions of the offices and divisions within IAIP, defining the operational relationships between those offices and divisions, diagramming internal and external terrorist threat information flow, and identifying the obstacles impeding IAIP's ability to become fully operational. Second, this survey provided an opportunity to identify issues suited for future detailed inspections or audits. With regard to programs or operations meriting special or focused attention, we reviewed and analyzed the following:

- Documentation pertinent to DHS and IAIP including program guidance, policy memorandums, briefing packages, meeting notes, Internet websites, and various news articles;
- Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (Nov. 25, 2002);
- Patriot Act of 2001, Pub. L. 107-56, 115 Stat. 272 (Oct. 26, 2001);
- Congressional testimony, namely the joint hearing with both the Judiciary Committee and the Select Committee on Homeland Security, on "The Terrorist Threat Integration Center (TTIC) and its Relationship with the Departments of Justice and Homeland Security," July 22, 2003;
- Congressional testimony, namely the Subcommittee on Intelligence and Counter-Terrorism to the House Select Committee on Homeland Security,

“Improving the Department of Homeland Security’s Information Sharing Capabilities,” July 24, 2003; and

- IAIP organizational chart as of August 11, 2003.

We interviewed key IAIP officials, including the Under Secretary, the Assistant Secretary for Information Analysis, the Assistant Secretary for Infrastructure Protection, and the Director of the Homeland Security Operations Center. In addition, we interviewed the Chief of Staff and the office directors for the Risk Assessment Division, the Information and Warnings Division, the Infrastructure Coordination Division, the Protective Security Division, the National Communications System, the Planning and Partnership Office, and the Competitive Analysis and Evaluation Office.

The bulk of the interviews conducted during the interview phase of this survey were conducted from May 2003 to July 2003 under the authority of the Inspector General Act of 1978, as amended. Follow-up questions regarding the National Asset List were answered on December 16, 2003.

Programs of the Information Analysis and Infrastructure Protection Directorate (by offices and divisions)

Guided by the requirements of the HSA, IAIP combines the capability to: (1) identify and assess current and future threats to the nation’s critical infrastructure; (2) communicate identified threats and issue warnings to relevant federal, state, local, private, and international partners; and (3) implement strategies to protect the nation’s critical infrastructure. No other government agency has the statutory mandate to combine these capabilities under one organizational framework. Consequently, many refer to IAIP as the “central information nerve center” of the overall effort to protect the homeland and, thus, of DHS.

The Budgetary Programs of IAIP

IAIP administers the (1) Administrative and Outreach Program; (2) Intelligence and Warning Program; (3) Homeland Security Operations Center; and (4) Protecting Critical Infrastructure and Key Assets Program. Baseline personnel and funding statistics as provided by IAIP are reported in the following table.

Table 1 – Projected, authorized personnel and funding statistics for FY 2004

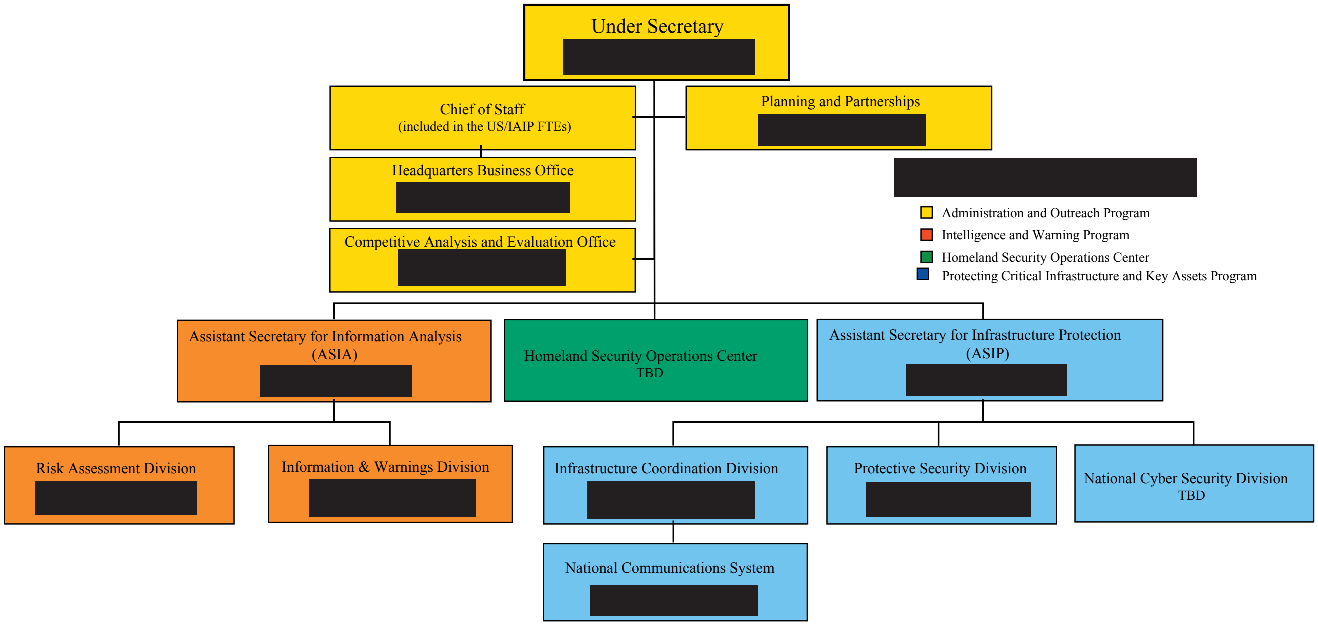
Programs/Operations Center	FTEs	Budget ($000)
Administrative and Outreach Program	[redacted]	[redacted]
Homeland Security Operations Center	[redacted]	[redacted]
Intelligence and Warning Program	[redacted]	[redacted]
Protecting Critical Infrastructure and Key Assets Program	[redacted]	[redacted]
Total	692	$1,032,000

These three programs and one operations center can be traced generally to specific offices and divisions within IAIP. The Administrative and Outreach Program is roughly equivalent to the Office of the Under Secretary and the personnel assigned to support the Under Secretary and administrative and outreach functions of IAIP. The Intelligence and Warning Program is roughly equivalent to the Office of Information Analysis (IA), and the Protecting Critical Infrastructure and Key Assets Program is roughly equivalent to the Office of Infrastructure Protection (IP).

Organizational Chart of IAIP

IAIP's organizational chart supplied, as of August 11, 2003, is presented below.

Chart 1 – The Information Analysis and Infrastructure Protection Directorate



Under Secretary
[redacted]
Chief of Staff
(included in the US/IAIP FTEs)
Planning and Partnerships
[redacted]
Headquarters Business Office
[redacted]
Competitive Analysis and Evaluation Office
[redacted]
[redacted]
🟨 Administration and Outreach Program
🟥 Intelligence and Warning Program
🟩 Homeland Security Operations Center
🟦 Protecting Critical Infrastructure and Key Assets Program
Assistant Secretary for Information Analysis (ASIA)
[redacted]
Homeland Security Operations Center
TBD
Assistant Secretary for Infrastructure Protection (ASIP)
[redacted]
Risk Assessment Division
[redacted]
Information & Warnings Division
[redacted]
Infrastructure Coordination Division
[redacted]
Protective Security Division
[redacted]
National Cyber Security Division
TBD
National Communications System
[redacted]

On March 1, 2003, when certain offices and functions of 22 agencies merged to create DHS, IAIP inherited elements from five legacy agencies, including:

- National Infrastructure Protection Center (Federal Bureau of Investigation)
- Critical Infrastructure Assurance Office (Department of Commerce)
- Federal Computer Incident Response Center (General Services Administration)
- National Communications System (Department of Defense)
- Office of Energy Assurance (Department of Energy)

Merging these five legacy elements into a fully functioning directorate is an ongoing process. Since merging, IAIP has made several changes to its organizational structure. One of the more significant changes involved the placement of the Homeland Security Operations Center (HSOC) within IAIP. Previously, the HSOC was assigned to the Office of the Secretary and was budgeted under the Management and Administration Program of DHS. Another significant change was the establishment of a National Cyber Security Division (NCSD). Both of these changes are reflected in the current organizational chart. However, as IAIP streamlines processes and refines communication among internal offices, divisions and external partners, the OIG understands that additional changes in the current organizational structure may be necessary. In fact, the OIG has learned that additional changes in the organizational structure are under consideration. These changes are intended to enhance the ability of IAIP to meet the 19 responsibilities assigned to it by the HSA. Such changes could involve converting the Information and Warnings Division (IWD) within the IA into the Information Management and Requirements Division (IMRD), moving the Planning and Partnerships Office (PPO) from the Office of the Under Secretary to the IP, and making the National Communications System (NCS) into a peer of the Infrastructure Coordination Division (ICD) rather than keeping it as a subordinate.

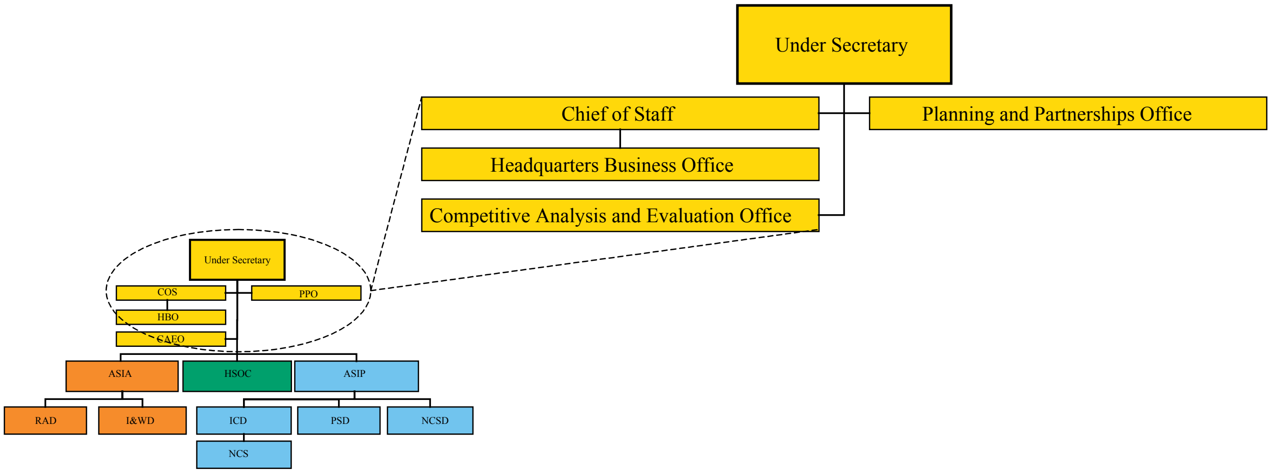
Under the current organizational structure, IA is responsible primarily for identifying and assessing current and future threats to the nation's critical infrastructures. The HSOC is responsible for communicating identified threats and issuing warnings to relevant federal, state, local, and private sector partners. The IP is responsible for implementing strategies to protect the nation's critical infrastructure. Of the 19 responsibilities assigned to IAIP by the HSA, 16 are to be carried out by IA and three are assigned to IP, with close collaboration between IA and IP on seven of these responsibilities (Appendix A.). One of the goals of executive management is for the IA and IP to function seamlessly regarding these assignments.

During non-crisis operations, information arrives through IAIP-watch, resident intelligence agency desks, resident law enforcement agency desks, and resident response agency desks within the HSOC, as well as through contacts among the 13 infrastructure sectors (Appendix B). Once information is processed within IAIP, warning and mitigation strategies are then communicated to relevant partners through the HSOC or through line-operational divisions (e.g., the Infrastructure Coordination Division) after coordination with HSOC to points of contacts among the 13 infrastructure sectors – an environment where IAIP listens with many ears and speaks with many mouths. During near-crisis or crisis operations, information flows through the HSOC and, in general, line-operational divisions will be discouraged from maintaining separate channels of communication with the contacts developed through the course of regular non-crisis operations. Line-operational divisions will still be able to communicate with their contacts in the sectors; however, they will be encouraged to do so through the HSOC so the message will be more controlled – an environment where IAIP listens with one ear and speaks with one mouth.

Administration and Outreach – Office of the Under Secretary

The Office of the Under Secretary is comprised of: (1) the Under Secretary; (2) the Chief of Staff; (3) Headquarters Business Office; (4) the Competitive Analysis and Evaluation Office; and (5) the Planning and Partnership Office. The following chart highlights the position of the Office of the Under Secretary within IAIP:

Chart 2 – The Office of the Under Secretary


Under Secretary
Chief of Staff
Planning and Partnerships Office
Headquarters Business Office
Competitive Analysis and Evaluation Office
Under Secretary
COS
PPO
HBO
CAEO
ASIA
HSOC
ASIP
RAD
I&WD
ICD
PSD
NCSD
NCS

- **Chief of Staff (COS)**
  The primary responsibility of the COS is to administer and manage IAIP's staff. Embodied within this responsibility is the coordination of the directorate's offices and line-operational divisions, assuring that they are integrated and operating in full collaboration with the HSOC. However, several issues appear to be inhibiting this integration process. One of the more obvious involves the 499 Full Time Equivalents (FTEs) that IAIP inherited from legacy agencies. Of these 499 FTEs, only 174 were filled by personnel who actually left their legacy agency and made the transition into IAIP. The other 325 have remained vacant for the first six months of IAIP's existence. The element that contributed the most to this personnel shortage was the National Infrastructure Protection Center (NIPC). When NPIC transferred into IAIP, personnel who actually left the FBI filled only 18 of the 307 FTEs targeted for transfer. The other 289 were vacant. Other complicating issues include turnover of key leadership positions, slower than anticipated consolidation of administrative functions, and logistical problems caused by IAIP's multiple office locations spread throughout the Washington metropolitan area.

- **Headquarters Business Office (HQBO)**
  The HQBO was established to provide IAIP components with the necessary planning, financial, facilities, and acquisition support required to satisfy their mission objectives and to ensure compliance with all federal and DHS regulatory and policy requirements. The Director of Business Operations is responsible for administering, managing, and overseeing all activities in the HQBO; coordinating business operations functions and activities across the IAIP; and reporting progress to its primary customers, the Under Secretary, the COS, and the assistant secretaries for IA and IP.

  One of the high priority challenges facing the HQBO, as well as the COS, is IAIP's immediate need to fill its ranks with sufficiently trained and appropriately cleared staff to meet the needs of IAIP senior management and all IAIP divisions. Further, it is anticipated that within next five years, the IAIP will experience tremendous growth in terms of acquiring additional highly skilled staff as well as services, technologies, and tools that will enable the IAIP to refine its mission. The HQBO and the COS face the challenge of identifying issues and factors that influence the size and shape of IAIP's budget, staffing, and technology.

- **Competitive Analysis and Evaluation Office (CAEO)**
  The mission of the CAEO is to reduce the risk and consequences of terrorist attacks on the homeland by helping to ensure that IAIP products and services are tested, and of the highest quality and value.

  The CAEO helps DHS anticipate terrorist actions -- and thus improve DHS threat warnings, collection requirements, and mitigation measures - - by organizing DHS "strategic red cell" sessions. During these sessions, the CAEO brings in outside experts from private industry, the military, the intelligence and law enforcement communities, and elsewhere to provide an independent assessment of where, how, and when terrorist may attempt to strike.

  The CAEO plans to test and validate risk assessments on infrastructure through physical and cyber "red teaming." By emulating terrorist mindsets, doctrines, and tactics, CAEO red teams will provide its customers, mainly IP, with a snapshot of critical infrastructure and cyber security vulnerabilities, categorize them according to risk, and identify safeguards to mitigate the vulnerabilities.

  In addition, the CAEO:

  - Develops, coordinates, and conducts interagency and IAIP exercises to test and improve procedures for managing terrorist threats and attacks, as well as organizes conferences and seminars.
  - Conducts impartial in-house and outside reviews of IAIP products, services, and processes -- including measuring customer feedback on these products -- and works with IAIP components to develop quality standards.

- **Planning and Partnership Office (PPO)**
  At the core of IAIP's mission is the need to build and maintain strong, strategic relationships with critical infrastructure sectors and key asset industries. This task is assigned to IAIP's PPO. The PPO is responsible for developing and supporting the development of partnerships for IAIP divisions with state and local government, private industry, and international communities for national planning, outreach and awareness, information sharing, and protective actions. Specifically, the PPO:

- Develops, coordinates and supports partnerships for IAIP divisions with international communities, state and local government and other federal agencies, public sector, and academic institutions for outreach and awareness, information sharing and protective action programs;
- Develops, coordinates, and implements national outreach and awareness programs for IAIP divisions;
- Manages and provides executive agent support to advisory councils and cross-sector partnerships; and,
- Develops, maintains and reports progress against national integrated strategies and implementation plans for critical infrastructure protection.

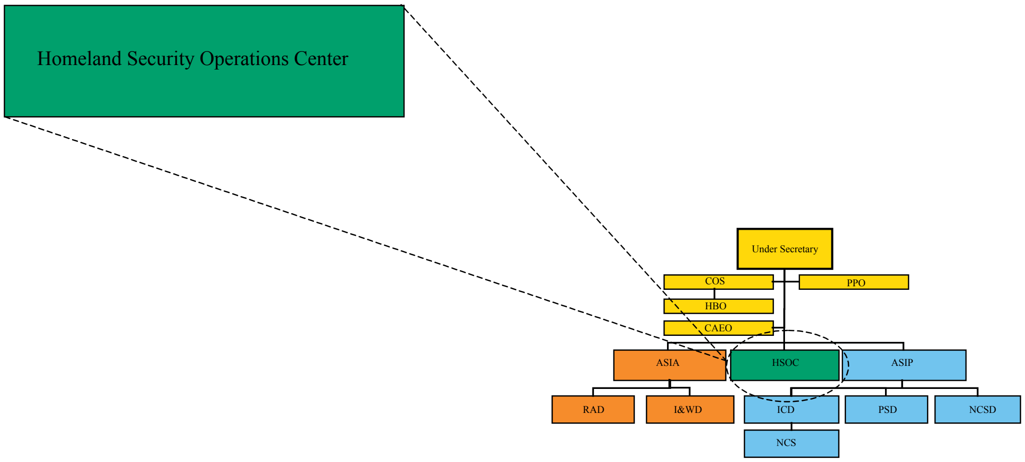
Successfully implementing productive partnerships requires expertise in information analysis and infrastructure protection processes and policies, the interest of potential partners, and skills in creating mutual benefits among an array of stakeholders. Before the PPO can become fully functional, offices and divisions within IAIP must understand the benefits of their interaction with each other as well as external participants. The PPO must also develop standardized protocols and processes as they apply to entities inside and outside IAIP.

Homeland Security Operations Center

The Homeland Security Operations Center (HSOC) is the nation's single point for tracking federal, state, local and private sector terrorist threat information to secure the homeland. It operates 24 hours per day, seven days a week. It maintains and shares domestic situational awareness; coordinates security operations; detects, prevents, and deters terrorist incidents; and facilitates the response to all critical threats. During a crisis, [redacted]

The following chart highlights the HSOC's position within IAIP:

Chart 3 – The Homeland Security Operations Center



Under the operational control of IAIP, the HSOC houses staff from various elements of the intelligence and law enforcement communities such as the CIA, National Security Agency, Secret Service, and FBI, as well as elements from organizations such as the Department of State, Department of Energy and the National Emergency Management Association.[3] In addition, an IAIP cell or "IAIP-watch" is located in the HSOC. IAIP-watch serves as a channel for the flow of threat information to and from the divisions within IAIP.

[redacted]

[redacted]

[3] The National Emergency Management Association is a professional organization for state emergency management directors. Its mission is to provide leadership and expertise in emergency management, serve as an information and assistance resource, and to advocate continuous improvement in emergency management procedures.

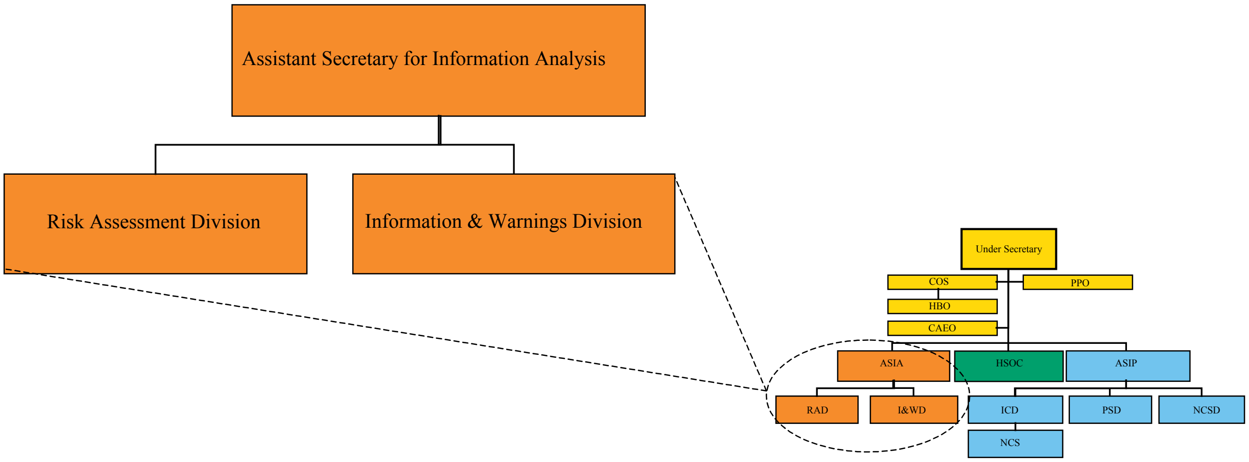
[redacted]

Intelligence and Warning – Office of Information Analysis

The Office of Information Analysis (IA) is comprised of two divisions:the Risk Assessment Division and the Information and Warnings Division. The primary mission of IA is to provide a full range of intelligence support to components within DHS, as well as relevant partners outside of DHS. IA provides this support by serving two roles: first, as an information "fusion center," and, second, as an information "dissemination manager." As an information fusion center, IA gathers and integrates threat information from the intelligence and law enforcement communities, as well as from other components within DHS. Once the information has been gathered and integrated, it is then analyzed and processed into a usable format for distribution. As an information dissemination manager, IA ensures that threat information is shared appropriately by issuing threat advisories, bulletins, and warnings to relevant partners both internal and external to DHS. Finally, IA supports the administration of the HSAS, by providing independent analysis of threat information in support of decisions to raise or lower the national threat condition.

The following chart highlights IA's position within IAIP:

Chart 4 – The Office of Information and Analysis



- **Risk Assessment Division (RAD)**
  RAD is charged with becoming the most authoritative source in the federal government for assessing the overall threat that terrorists pose to homeland

security. It is also charged with mapping these threats against vulnerabilities and providing actionable advisories to relevant partners both internal and external to DHS. The RAD is considered to be an intelligence *gatherer*, rather than an intelligence *collector*. The difference is the RAD accumulates and analyzes information passed to it by sources whose mission is to seek out raw intelligence.[4] The RAD does not participate in activities such as recruiting informants or intercepting communications.

The RAD accomplishes its core intelligence mission by integrating and analyzing threat information primarily from the intelligence and law enforcement communities and DHS operational and intelligence components. The RAD is also authorized to establish a two-way exchange of information with its state, local, and private sector partners. [redacted]

[redacted] The HSOC is the lead operations center within DHS that is responsible for monitoring and conducting a first level assessment of incoming threat information and any appropriate response. The HSOC is staffed with representatives from the intelligence and law enforcement communities, Department of Defense (DoD), and various civilian agencies. [redacted]

The Terrorist Threat Integration Center (TTIC), a joint venture among the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), the DoD, Department of State, and DHS, serves as another important

[4] Raw intelligence is a colloquial term meaning collected information that has not yet been converted into finished intelligence.

[redacted]

source of information for the RAD. In contrast to the HSOC, the director of TTIC does not report to the IAIP Under Secretary but to the Director of Central Intelligence as the head of the entire U.S. intelligence community. The TTIC's mission is to integrate and analyze terrorist-related information to form the most comprehensive threat picture possible, whether it pertains to threats overseas or to the homeland. In many respects, the missions of the TTIC and the RAD overlap. However, the TTIC's mission is more specific than the analytic mission performed within DHS by the RAD in that TTIC primarily focuses on threats developing overseas.[6]

By contrast, the RAD has both a more focused and overarching mission in defending the homeland than TTIC. The RAD, as a division of IA, has the statutory mandate to analyze all incoming threats to homeland security and then to assess their credibility [redacted] Another important difference is that the RAD has the mandate to communicate these assessments in a timely manner to state, local, and private sector partners. The RAD does this through its close relationships with the HSOC, IP, and the state and local office of DHS. The importance and uniqueness of the RAD's relationships with its counterpart divisions within the IP cannot be overstressed. The TTIC does not have the mandate to communicate or interact with state, local, and private sector partners, nor does it have a direct relationship with divisions within the IP that implement protective measures.

The TTIC is reported to be a willing partner in the exchange of threat information.[7] However, the OIG was told during senior executive interviews that DHS must weigh in more heavily with TTIC, particularly in its corporate ownership of analytic products produced for the President, Secretary of Homeland Security, and other senior officials. According to these interviews, the intelligence product coming out of the TTIC would benefit

[6] In a letter to Senator Joseph I. Lieberman, dated June 17, 2003, Secretary Ridge, attempting to clarify the difference between TTIC and the analytical work being performed within DHS, wrote, "Other agencies have specific analytic functions that relate to the war on terrorism performed to support their respective and specialized mission. …Information pertaining to threats overseas [primarily collected by the CIA and analyzed by TTIC] is an important part of the overall analytic mosaic supporting the global war on terrorism."

[7] On July 22, 2003, at a joint oversight hearing with the Committee on the Judiciary and Select Committee on Homeland Security, Acting Assistant Secretary for IA confirmed that TTIC has provided IA all the threat information that he has requested since he assumed that position.

from the expertise and unique information access which RAD analysts have. Furthermore, DHS and the TTIC should share staffing strategies to ensure that they build compatible skill sets and missions rather than compete for the same personnel resources and missions. [redacted]

[redacted]

- **Information and Warnings Division (IWD)**
  Initially, the IWD was assigned two critical responsibilities. One of these responsibilities was managing the entire internal and external information requirements process of IAIP. As part of this process, the IWD "pushes" information to relevant internal and external partners by coordinating the IAIP-watch within the HSOC and disseminating open-source[9] warnings to state, local, and private sector partners -- functioning much like an information traffic cop. The IWD "pulls" information from relevant internal and external partners by developing information sharing and intelligence requirements designed to extract specific data that is necessary to obtain a more complete and comprehensive threat picture. The IWD works closely with the RAD and counterpart divisions within the IP to determine information sharing and intelligence requirements.

[redacted]

[9] Information that is publicly available through such media as newspapers, television, and the Internet.

The IWD also is responsible for administering the HSAS. Once the Secretary, in consultation with members of the Homeland Security Council (HSC), decides to raise or lower the national threat condition, the IWD is charged with coordinating the actual notification of relevant partners about the change in threat condition. The IWD fulfills this role by maintaining a call list of contacts among key media outlets and state, local, and private sector officials. The IWD works closely with the HSOC throughout the notification process. In addition to administering the HSAS, the IWD is expected to produce information bulletins and warnings, coordinate the Secretary's morning summary, and have input in the overnight development briefing and the President and Secretary's monthly report.[10]

The OIG has been told that the IWD may be disbanded in favor of a division that would focus almost exclusively on IAIP's information requirements. The new division most likely will be called the "Information Management and Requirements Division" (IMRD) and will transfer old IWD elements responsible for watch and warning functions to the HSOC. Now that the HSOC has been moved into IAIP consolidating all watch and warning functions in the HSOC would eliminate the need to maintain two different entities within IAIP with the same functions. The future success of the IMRD will depend on how well organizations within the intelligence and law enforcement communities respond to the information requirements it sets. IAIP officials told the OIG that the IMRD's utility would be strongly influenced by the responsiveness of agencies such as the FBI and the CIA when tasked by the IMRD to collect certain intelligence or conduct specific investigations.

Protecting Critical Infrastructure and Key Assets – Office of Infrastructure Protection

The mission of the IP is to implement protective measures to reduce vulnerabilities in the nation's critical infrastructure.[11] According to the "National Strategy for the Physical Protection of Critical Infrastructures," dated February

[10] The President or other officials in the White House, as well as the Secretary, receive a report that outlines trends in suspicious incidents. Initially, this report was distributed on a weekly basis and then eventually on a bi-weekly basis. Currently, it is distributed on a monthly basis.

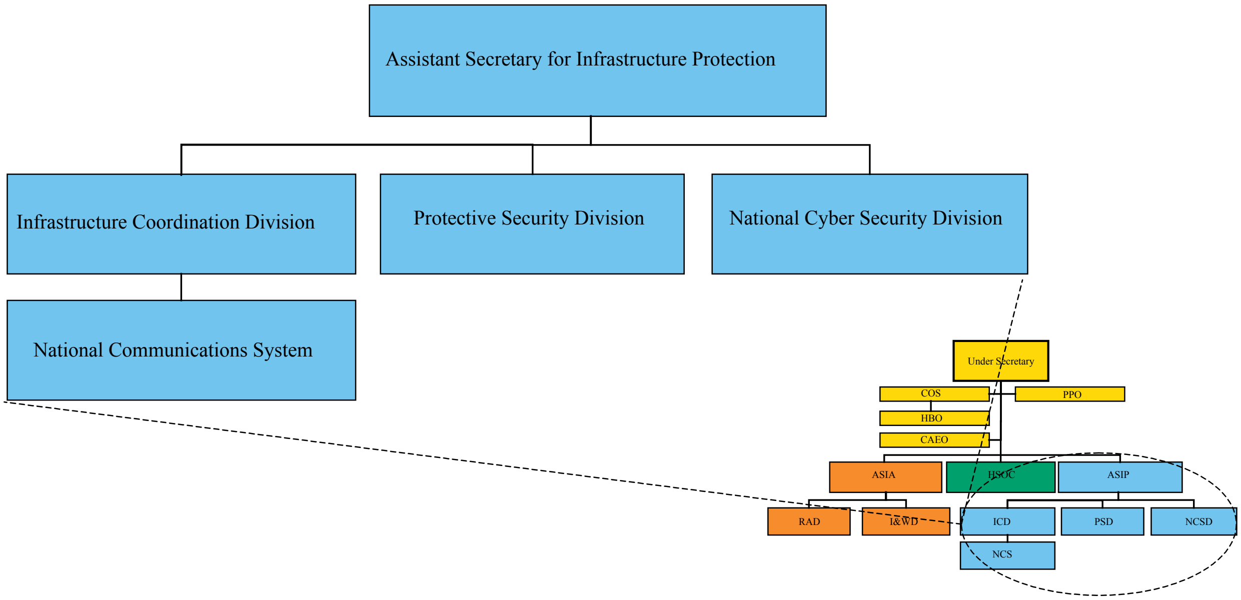
[11] The Patriot Act defines critical infrastructure as "those systems and assets, whether physical or virtual [cyber], so vital to the United States that the[ir] incapacity or destruction... would have a debilitating impact on the security, national economic security, national public health or safety, or any combination of those matters."

2003, critical infrastructure can be categorized into 13 infrastructure sectors and five key assets. There are eight federal lead departments and agencies, including DHS, which have a role in coordinating protection activities and cultivating long-term collaborative relationships with counterparts from each of the 13 infrastructure sectors and five key assets (Appendix B). However, as authorized in the HSA, only DHS has the overarching responsibility to be the primary liaison and facilitator for cooperation among all federal departments and agencies, as well as state, local and private sector partners.

As the primary liaison and facilitator within DHS during non-crisis operations, the IP takes a broad approach to protecting the nation's critical infrastructure by working closely with: (1) the IA and other organizations within DHS; (2) federal lead departments and agencies responsible for protecting infrastructure sectors and key assets that do not fall under the immediate control of DHS; (3) state, local, and private entities; and (4) international entities to reduce infrastructure vulnerabilities and deny the use of the infrastructure as a weapon to attack Americans. Within the context of a national approach, the IP is increasing the nation's capability to secure critical infrastructure and key assets, as well as high profile events [redacted] Second, based on assessed vulnerabilities, the IP will provide training and plans for protective measures to assist owners and operators in securing the critical infrastructure and key assets within their control. The IP's goal is to mitigate quickly vulnerabilities and risks, while simultaneously helping state, local, and private sector partners develop the capability to mitigate vulnerabilities and risk themselves. By building these capabilities into national partners, the IP intends to reduce the nation's vulnerability to terrorist attacks through a sector-wide approach.

The following chart highlights IP’s position within IAIP:

Chart 5 – The Office of Infrastructure Protection


Assistant Secretary for Infrastructure Protection
Infrastructure Coordination Division
Protective Security Division
National Cyber Security Division
National Communications System
Under Secretary
COS
HBO
CAEO
PPO
ASIA
HSOC
ASIP
RAD
I&WD
ICD
PSD
NCSD
NCS

- **Infrastructure Coordination Division (ICD)**
  ICD provides core expertise in all the nation’s infrastructure sectors and key assets; monitors the operational status of those infrastructure sectors and key assets; supports the two-way sharing of critical infrastructure information between DHS and other federal, state, local, and private sector partners; and supports infrastructure incident/event response, mitigation, and recovery. Additionally, the ICD is charged with protecting proprietary and business sensitive data, implementing and executing the Critical Infrastructure Information program[12], and executing National Security Emergency Preparedness (NS/EP) programs.

  To accomplish its mission and functions, the ICD works closely with the RAD, Protective Security Division (PSD), and eventually with the National Computer Security Division (NCSD) to provide analyses across all infrastructure sectors and key assets. After assessing current trends in terrorist threats to the nation’s critical infrastructure, the ICD determines the requirements for protective measures and then actively pursues partnerships

[12] Based on the authority of the HSA, the Critical Infrastructure Information program provides for tracking receipt, validation, protection against unauthorized disclosure, and destruction of infrastructure information.

with other government and private sector entities to safeguard [redacted]

- **National Communications System (NCS)**
  NCS is the lead IAIP element for developing and maintaining collaborative relationships to support the critical infrastructure sector on communications. To do this, the NCS: (1) monitors the vulnerabilities of the telecommunications industry; and (2) coordinates national security and emergency preparedness communications for the federal government during non-terrorism related emergencies, terrorist attacks, and recovery and reconstitution operations. Organizationally, the NCS reports to the ICD. The NCS is the only organization that merged into IAIP without losing its legacy name or mission assignment.

  The NCS combines the assets of 23 federal departments and agencies to address the full range of national security and telecommunications emergency preparedness issues. The NCS applies its interagency planning efforts in developing NS/EP special telecommunications services to support IAIP and national security missions.

  The NCS also provides a means of collaborating with executives from the communications and information technology industries who are part of the President's National Security Telecommunication Advisory Committee (NSTAC).[13] The NSTAC provides industry based advice and expertise to the President on issues and problems related to implementing national security and emergency preparedness. Additionally, through its relationships with other federal departments and agencies and the NSTAC, the NCS serves as another conduit for receiving information about potential terrorist attacks against the nation's critical infrastructure.

- **Protective Security Division (PSD)**
  PSD is to coordinate strategies for protecting the nation's critical, *physical* infrastructure. The PSD works closely with the ICD. The ICD identifies critical infrastructure elements and passes the information to the PSD. The PSD uses this information to conduct risk assessments and determine remediation plans for identified vulnerabilities.

[13] The NSTAC is composed of up to 30 executives representing the major communications and network service providers and information technology, finance, and aerospace companies, such as Verizon, Bell South, Lockheed Martin, The Boeing Company, and Electronic Data Systems.

The PSD receives terrorist threat information and analysis from the RAD and other open sources, such as state and local governments. Based on this information, the PSD formulates terrorist capability disruption and remediation strategies. By implementing disruption strategies, the objective of PSD is to upset the ability of terrorists to establish the means for attack. By implementing remediation strategies, [redacted] the objective of the PSD is to deter or disrupt terrorist attacks, or minimize their impact if they occur.

The PSD also has an important advisory and training function. Advisory and training services will be delivered to state, local, and private sector partners by a network of protective security specialists as well as Protective Security Advisors posted throughout the country. Based upon identified critical assets, threats, and incidents, the PSD may provide an advisory team to work with state and local public safety officials and infrastructure owners and operators to make assets within their control more secure. Additionally, the PSD has been working with its state, local, and private sector partners to identify and list critical infrastructure assets [redacted]

- **National Cyber Security Division (NCSD)**
  The mission of the NCSD is to implement the *National Strategy to Secure Cyberspace* which includes identifying, analyzing and reducing cyber threats and vulnerabilities; disseminating cyber-threat warning information; coordinating incident response; providing technical assistance in continuity of

operations and recovery planning; and outreach, awareness, and training. The newly formed NCSD is to be a fusion point of expertise for cyber security. The NCSD also is to use the expertise of various law enforcement, defense, and intelligence agencies to provide multi-layered cyber security protection. Furthermore, the NCSD is to serve as a single point of contact for the public and private sectors for addressing cyber security issues in the United States. The NCSD is to work closely with other IAIP offices and divisions and maintain contacts with other federal, state and local governments, and the private sector to fulfill its mission.

Issues for Inspections/Evaluations

As we studied IAIP in order to understand its mission and how its offices and divisions operate, we identified several issues that could be impeding the ability of IAIP to become fully operational. Consequently, these issues may be suitable for future inspections.

Hiring Personnel to Work in a Classified Environment Takes a Substantial Amount of Time

Because of its close interaction with the intelligence and law enforcement communities, IAIP handles some of the most sensitive work within DHS. To work in this environment, most IAIP personnel require access to information that is classified at the Top Secret level or higher. Obtaining the necessary clearance can be a time consuming process for new employees. In some cases, it can take a year or more before a background investigation can be completed and the new employee is deemed suitable for a clearance. Even when the person hired already has a security clearance, a full background investigation may still be necessary because clearances are not universally accepted by other agencies within the intelligence and law enforcement communities. For these reasons, a majority of IAIP executives interviewed by the OIG identified hiring personnel who can work quickly within a classified environment as one of the major obstacles impeding the directorate's ability to become fully operational.

The time necessary to obtain a clearance is also an impediment for state, local, and private sector personnel. The delay affects both the general distribution of threat information and the actual participation of state, local, private sector, and contract support personnel on IAIP analytical teams or in the HSOC. A recent executive order granted the Secretary authority to set the standard for security clearances going to state, local, and private sector personnel.[14] Despite this authority, many state and local law enforcement personnel are experiencing significant delays in getting clearances to obtain information from federal sources. A future inspection could focus on whether the clearance process for DHS new hires and personnel from state and local governments, the private sector, and contractor support can be shortened without sacrificing security. Such an inspection could examine the feasibility of utilizing state and local police officers to augment the background investigative process. It may also examine the reasons agencies reject other agencies' decisions granting clearances and why there is no universally accepted clearance process.

The Ability of IAIP to Exchange Threat Information Electronically with Partners is Necessary to Fulfill its Mission

One of the keys to the success of DHS is establishing connectivity with both its internal and external partners. Having the capability to send and receive timely, accurate, and reliable information, is necessary if IAIP is to fulfill its mission as the lead intelligence gathering and warning directorate within DHS. In fact, the HSA requires DHS to establish procedures that facilitate the free exchange of threat information among agencies at all levels of government and the private sector. The HSA also requires DHS to report to congressional committees on how well it shares information with its partners.[15]

To establish connectivity among its partners that is compatible, IAIP must have the necessary resources, including:

- personnel with the necessary security clearances and technical experience to operate and maintain information systems;
- facilities to receive and store intelligence data; and
- networks and messaging systems within IAIP that allow for secure electronic communication with internal, other federal, state, local, and private sector partners.

IAIP has already begun to identify its top priorities for sharing and processing information. [redacted]

[14] "Bush Greenlights Ridge on Security Clearances Outside Beltway," Congressional Quarterly, by Jim McGee, July 30, 2003.

[15] These requirements are found in the Homeland Security Act, Section 892 (b)(1) & (2), and Section 893.

[redacted] A future inspection could identify [redacted] IAIP's methodology for developing connectivity with its partners and make recommendations for corrective action.

Maintaining Close Partnerships that Facilitate Unobstructed Information Flows is Crucial to the Success of IAIP

DHS is now the cabinet-level department responsible for coordinating the protection of American citizens and infrastructure from terrorist attacks. The Secretary charged IAIP with carrying out this responsibility. Therefore, IAIP is accountable for transmitting terrorist threat information to its federal counterparts, as well as to state and local law enforcers -- our nation's first line of defense against terrorist attacks. IAIP also maintains channels to receive threat-related information. Information IAIP receives may originate from federal, state, local, private sector or any other sources. Since IAIP is an intelligence gatherer rather than an intelligence collector, its success is largely dependent on its federal, state and local, and private sector partnerships.

The acting Assistant Secretary for IA expressed his satisfaction with the manner in which information flows both vertically (i.e., between IAIP and its state, local, and private sector partners), and horizontally (i.e., between IAIP and its federal partners such as the CIA, FBI, and other members of the intelligence community). However, in a recent congressional hearing,[16] a member of the House Select Committee on Homeland Security stated, "It is nearly two years since the attacks of September 11th, and information sharing on the terrorist threat to America is still dangerously disconnected between different agencies of the federal government and between the federal government and state and local law enforcement officials."

A future inspection could document the impact of security clearance issues on information sharing, particularly at the state, local, and private sector levels and connectivity and electronic data sharing issues among IAIP's federal partners. In addition, the study should chronicle the existence of conflicting or duplicative information channels within IAIP or among its state, local, and private sector or federal partners and how such alternative channels might be integrated. This

[16] Subcommittee on Intelligence and Counter-Terrorism to the House Select Committee on Homeland Security, " Improving the Department of Homeland Security's Information Sharing Capabilities," July 24, 2003.

review could complement a planned, internal IAIP study that will be conducted jointly with the Border and Transportation directorate.[17]

The Extent of IAIP's Involvement With the Homeland Security Advisory System is Not Clear

The purpose of HSAS is to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist attacks to federal, state, and local authorities and to the American people. This advisory system characterizes appropriate levels of vigilance, preparedness, and readiness in a series of graduated threat conditions. As previously mentioned, the Secretary, in consultation with the HSC, determines the threat condition. IAIP supports the management of the HSAS by providing analysis of threat information in support of decisions to raise or lower the national threat level and for coordinating the actual notification of a threat condition change.

Although IAIP participates in analyzing threat information in support of the HSAS, it is not clear what information is specific enough to act upon. The intelligence requirements for the different threat conditions are unclear. Also, as noted previously in the RAD discussion, not all threat information that could affect the threat condition is vetted through IAIP.

Therefore, the OIG could initiate an inspection of how IAIP interacts with the Secretary and others involved in making the decision to elevate or lower the threat condition. Also, such an inspection could evaluate the adequacy and timeliness of information used for authorizing changes in the threat level.

IAIP Needs to Develop a Prioritized List of Critical Infrastructure and Assets

Identifying critical infrastructure is a critical step in implementing a national infrastructure protection plan. Once identified and validated, these critical infrastructure and key assets are catalogued into a prioritized national list that assigns the appropriate security level based on a comprehensive risk analysis of all assets identified on the list. It is expected that this national prioritized list will serve as a baseline for making decisions on which critical infrastructure and key assets to safeguard first. In line with this expectation, Congress has requested that

[17] July 31, 2003 memorandum from IAIP Under Secretary and the Border and Transportation Security Under Secretary, "Invitation to Participate in Joint Studies."

IAIP provide a detailed program plan outlining a proposed scope, total estimated costs, and schedule for completing a comprehensive risk analysis and assessment of vulnerabilities of the critical infrastructure by December 15, 2003.

The Protective Security Division (PSD) is responsible for maintaining a prioritized national list of critical infrastructure and key assets. Through interviews, the OIG has learned that PSD has solicited data from state and local partners on certain critical infrastructure and key assets. [redacted]

Appendix A
Summary of IAIP Statutory Functions

Summary of IAIP Statutory Functions

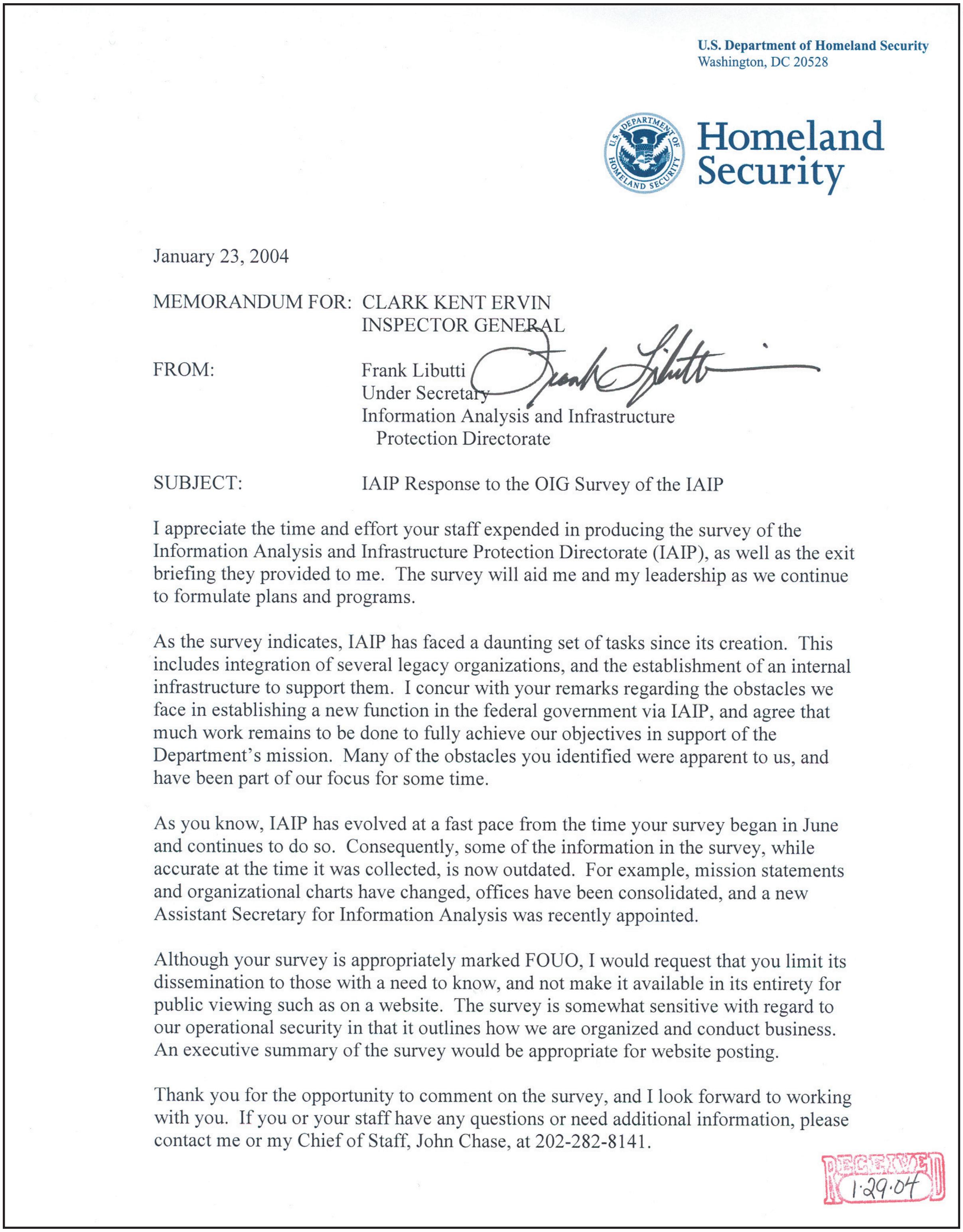
No.	Statutory Function	
1	Vulnerability Assessment	IP
2	National Plan to Secure Infrastructure	IP
3	“Map” Threats against vulnerabilities	IP
4	Recommend Infrastructure Protective Measures	IA/IP
5	Ensure timely and efficient access to DHS of all homeland security information	IA
6	Administer the Homeland Security Advisory System	IA
7	Make recommendations for homeland security information sharing policies	IA
8	Disseminate information analyzed by DHS to other federal, state, and local government entities and the private sector	IA
9	Consult with appropriate federal Intelligence Community and law enforcement officials to establish collection priorities and strategies and represent DHS in all “requirements” processes.	IA
10	Consult with state and local governments and the private sector to ensure appropriate exchanges of terrorist threat-related information	IA
11	Ensure that information received is protected from unauthorized disclosure and used only for the performance of official duties	IA/IP
12	Request additional information from other federal, state, local government agencies and the private sector	IA/IP
13	Establish and use secure information technology infrastructure	IA/IP
14	Ensure that information systems/databases are compatible with one another and other federal agencies and treat information in accordance with applicable Federal privacy law	IA/IP
15	Coordinate training and other support to DHS and other agencies to identify and share information	IA/IP
16	Coordinate with IC elements and federal, state, and local law enforcement agencies “as appropriate”	IA
17	Provide intelligence analysis and other support to the rest of DHS	IA
18	Perform such other duties as the Secretary may provide	IA/IP
19	Identify, Detect, and Assess Terrorist Threats to Homeland	IA

	Lead Agency	Critical Infrastructure Sectors [18]
1	Department of Homeland Security	Emergency Services
2	Department of Homeland Security	Information and Telecommunications
3	Department of Homeland Security	Transportation
4	Department of Homeland Security	Postal and Shipping
5	Department of Homeland Security All departments and agencies	Government
6	Department of Agriculture	Agriculture
7	Department of Agriculture Department of Health & Human Services	Food
8	Environmental Protection Agency	Water
9	Department of Health & Human Services	Public Health
10	Department of Defense	Defense Industry Base
11	Department of Energy	Energy
12	Department of the Treasury	Banking and Finance
13	Environmental Protection Agency	Chemical Industry & Hazardous Materials

	Key Assets
1	Commercial Assets
2	Government Facilities
3	Dams
4	Nuclear Power Plants
5	National Monuments

[18] Source: National Strategy for the Physical Protection of Critical Infrastructures dated February 2003.

Appendix C
IAIP Response to OIG



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

Homeland
Security

January 23, 2004

MEMORANDUM FOR: CLARK KENT ERVIN
INSPECTOR GENERAL

FROM: Frank Libutti
Under Secretary
Information Analysis and Infrastructure
Protection Directorate

SUBJECT: IAIP Response to the OIG Survey of the IAIP

I appreciate the time and effort your staff expended in producing the survey of the Information Analysis and Infrastructure Protection Directorate (IAIP), as well as the exit briefing they provided to me. The survey will aid me and my leadership as we continue to formulate plans and programs.

As the survey indicates, IAIP has faced a daunting set of tasks since its creation. This includes integration of several legacy organizations, and the establishment of an internal infrastructure to support them. I concur with your remarks regarding the obstacles we face in establishing a new function in the federal government via IAIP, and agree that much work remains to be done to fully achieve our objectives in support of the Department's mission. Many of the obstacles you identified were apparent to us, and have been part of our focus for some time.

As you know, IAIP has evolved at a fast pace from the time your survey began in June and continues to do so. Consequently, some of the information in the survey, while accurate at the time it was collected, is now outdated. For example, mission statements and organizational charts have changed, offices have been consolidated, and a new Assistant Secretary for Information Analysis was recently appointed.

Although your survey is appropriately marked FOUO, I would request that you limit its dissemination to those with a need to know, and not make it available in its entirety for public viewing such as on a website. The survey is somewhat sensitive with regard to our operational security in that it outlines how we are organized and conduct business. An executive summary of the survey would be appropriate for website posting.

Thank you for the opportunity to comment on the survey, and I look forward to working with you. If you or your staff have any questions or need additional information, please contact me or my Chief of Staff, John Chase, at 202-282-8141.

Bradley J. Harp, Program Analyst, Department of Homeland Security, Office of Inspections, Evaluations, and Special Reviews

Carlton I. Mann, Program Analyst, Department of Homeland Security, Office of Inspections, Evaluations, and Special Reviews

Frank A. Parrott, Program Analyst, Department of Homeland Security, Office of Inspections, Evaluations, and Special Reviews

Department of Homeland Security

Under Secretary, Information Analysis and Infrastructure Protection Directorate, Department of Homeland Security

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG), Office of Inspections, Evaluations, and Special Reviews at (202) 254-4205 or 4208, or fax your request to (202) 254-4304.

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 the OIG Hotline at 1-800-323-8603 or write to Department of Homeland Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.