GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

November 6, 2008

Congressional Committees

Subject: *National Applications Office Certification Review*

Since the 1960s, classified satellite information collected by intelligence agencies[1] has been used, from time to time, by federal civilian agencies and other non-intelligence entities for civil, scientific, and environmental purposes (such as mapping, disaster relief, and environmental research). These uses have historically been coordinated by the Civil Applications Committee (CAC) led by the U.S. Geological Survey, a component of the Department of the Interior.

Following the events of September 11, 2001, attention has turned to information sharing as a key element in developing comprehensive and practical approaches to defending against potential terrorist attacks. Having information on threats, vulnerabilities, and incidents can help an agency better understand the risks and determine what preventive measures should be implemented. The ability to share such terrorism-related information can also unify the efforts of federal, state, and local government agencies, as well as the private sector in preventing or minimizing terrorist attacks. Exchanging terrorism-related information continues to be a significant challenge for federal, state, and local governments—one that we recognize is not easily addressed. Accordingly, since January 2005, we have designated information sharing for homeland security a high-risk area.[2]

Citing a growing need to use classified satellite information for civil or domestic purposes, in 2005, an independent study group reviewed the future role of the CAC and concluded that although the civil domestic users were well supported through the CAC, homeland security and law enforcement users lacked a coherent, organized, and focused process to access classified satellite information.[3]

---

[1] For purposes of this report, the term "classified satellite information" will be used to refer to all information derived from intelligence community sources that is expected to be made available through the National Applications Office (NAO). Based on discussions with NAO officials, a substantial part—but not all—of this information is derived from sensors mounted on classified government satellites.

[2] For more information, see GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007), p. 47; *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.: Mar. 17, 2006).

[3] Independent Study Group, *Civil Applications Committee Blue Ribbon Study*, (September 2005).

In 2007, the Office of the Director of National Intelligence designated the Department of Homeland Security (DHS) as the executive agency and home of a newly created National Applications Office (NAO), whose mission would be to process requests for classified satellite information from, among others, nontraditional users of intelligence for civil, homeland security, and law enforcement purposes. DHS established a process whereby potential requesters for classified satellite information annually submit memorandums generally describing the information they plan to ask for, followed by a more detailed review of each actual request to ensure legal compliance.

The Consolidated Appropriations Act, 2008, prohibited funds from being made available to commence operations of the NAO until the Secretary of Homeland Security certified that the program complies with all existing laws, including all applicable privacy and civil liberties standards, and that certification was reviewed by GAO.

On April 9, 2008, in a letter to Members of Congress, the Secretary of the Department of Homeland Security certified that the NAO complies with all existing laws, including all applicable privacy and civil liberties standards. The Secretary also provided a charter for the office, privacy and civil liberties impact assessments, and NAO standard operating procedures.

Our objectives were to determine the extent to which DHS justified its certification that the NAO complies with (1) all applicable laws, (2) privacy standards, and (3) civil liberties standards.

To assess DHS's certification of compliance with all applicable laws, we reviewed the certification documents to determine the extent to which DHS evaluated and addressed laws applicable to NAO operations. We interviewed agency officials from the NAO program office and the DHS Office of General Counsel to identify all available analysis conducted on applicable laws and to determine the extent to which mechanisms for ensuring compliance had been established.

To assess DHS's certification of compliance with privacy standards, we reviewed two versions of the privacy impact assessment developed for the program (one completed in connection with the April 2008 certification and a revised version developed in July 2008 in response to discussions with us) and interviewed officials from the program office and the DHS Privacy Office. In addition, we analyzed the system-of-records notices identified within the certification documentation and by DHS to determine whether they provided public notice regarding NAO's planned operations and potential use of personal information.

To assess DHS's certification of NAO compliance with civil liberties standards, we reviewed the civil liberties impact assessment to identify concerns raised about civil liberties and recommendations made to address them. We also interviewed officials from the program office and the DHS Office of Civil Rights and Civil Liberties to determine the extent to which DHS had instituted measures to address the concerns raised by the impact assessment

We conducted this performance audit in the Washington, D.C., area from April 2008 to September 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

On September 15, 2008, we provided the staff of cognizant committees with sensitive but unclassified briefing slides on the results of this review. Subsequently, we coordinated with DHS officials to review the sensitivity of the slides and determine what contents could be publicly released. This report summarizes the results of our review, provides the public version of the slides, and officially transmits our recommendations to the Secretary of Homeland Security. The slides, including details on our scope and methodology, are reprinted in enclosure I.

DHS Has Not Fully Justified Its Certification That the NAO Complies with Applicable Laws

Although the department has established procedures for legal review, it has not yet fully addressed all outstanding issues regarding how the planned operations of the NAO, as described in the department's certification documents, are to comply with legal requirements. Specifically, DHS has not resolved legal and policy issues associated with NAO support for law enforcement. The NAO charter states that requests for law enforcement domain uses (i.e., activities relating to enforcing criminal or civil laws or investigating violations thereof) will not be accepted by the NAO until interagency agreement is reached on unresolved legal and policy issues. An independent study group had determined that the legality of using satellite imagery of domestic subjects for law enforcement purposes raised difficult issues that had not been fully settled. Work has begun to address these issues, and the department now plans to recertify the NAO's compliance with all laws before accepting requests related to law enforcement. Recertification following the resolution of legal and policy concerns will be an important element in providing assurance that NAO operations are in compliance with all applicable laws.

In addition, DHS has taken steps to develop a legal review procedure for classified satellite information requests but has not yet fully established management controls to ensure that it will be effective. DHS has developed a multistage process for reviewing potential requests to address any legal or policy concerns. This process represents a reasonable approach for ensuring that decisions are reviewed on a case-by-case basis, to the extent that law enforcement requests are not accepted. However, the NAO charter leaves it unclear what types of requests will be initially rejected as being in the law enforcement domain and what types will be accepted as homeland security requests, because the distinctions between the two domains are not clear.

Further, other important details have not yet been fully addressed. The process for developing and approving annual memorandums, which set expectations about planned customer uses of NAO data, has not yet been established for all categories of

classified satellite information. In addition, procedures for monitoring the legal review process to ensure that it is making appropriate determinations about the legality of requests have not yet been established. Without clarifying these details of the planned legal review process, DHS will have limited assurance that the process is effective at ensuring compliance with applicable laws.

DHS Has Taken Steps to Justify Its Certification of Compliance with Privacy Standards

The DHS Privacy Office worked with NAO program officials to define privacy protections for the program and prepared a privacy assessment that discussed high-level privacy protections. Further, DHS has recently taken additional steps to justify its certification of compliance with privacy standards.

Specifically, DHS originally did not fulfill agency requirements to identify privacy risks and control mechanisms but recently has taken steps to do so. At the time of NAO certification, DHS did not fully explain how the office would comply with widely accepted privacy standards, such as the need for personally identifiable information to be accurate, secure, and used only for limited purposes. Specifically, the NAO's original privacy assessment did not identify or analyze the risks that NAO operations might not meet these standards, nor did it specify measures to mitigate such risks. In response to discussions with us regarding these shortcomings, the Privacy Office developed a revised assessment that represented a substantial improvement in identifying privacy risks and mitigating controls to address them, such as providing appropriate oversight and building a process to identify and correct inaccurate information. However, differences between the review procedures outlined in the revised privacy impact assessment and those in the standard operating procedures raise questions about whether the specifics of the NAO's privacy protection controls have been clearly established.

In addition, the public notices cited by DHS did not provide a public explanation of the privacy protections associated with planned NAO operations. One key privacy standard requires that the public be notified about the existence of systems containing personal information and the privacy protections associated with them. However, publicly available privacy notices (called system-of-records notices under the Privacy Act of 1974) cited by DHS as applying to the NAO did not provide information specifically about the NAO, its planned uses of personal information, or the privacy protections that are to be established. In response to discussions with us regarding this lack of public notice, DHS updated NAO information on the department's public Web site to reflect the relationship between the NAO and the applicable system-of-records notice. The updated information better informs the public about how personal information is to be processed, analyzed, and distributed by the NAO.

DHS Identified Civil Liberties Concerns Associated with NAO Operations but Has Not Yet Fully Addressed Them

The NAO civil liberties impact assessment identified a number of areas of potential concern regarding civil rights and civil liberties. Although the NAO program office

addressed several of these issues—such as the need to develop and conduct training on civil liberties issues—the department has not indicated how the NAO would address other significant issues, including the potential for improper use or retention of intelligence information by customers and the potential for overly broad annual memorandums about customers' planned uses, which may facilitate the acceptance of requests that should be rejected.

In a July 2008 letter to the DHS Undersecretary of Intelligence and Analysis, the acting NAO program director outlined plans to address several issues raised by the assessment. However, specific measures have not yet been developed to address the potential for improper use or retention of information provided by the NAO and the potential for impermissible requests to be accepted as a result of a reliance on broad annual memorandums as justifications. Certifying the readiness of the NAO without fully addressing the concerns outlined within the assessment—including establishing internal controls for mitigating identified risks—provides only limited assurance that the office is in compliance with civil liberties standards and will take appropriate measures to protect civil liberties.

Recommendations for Executive Action

To ensure that the NAO is in compliance with applicable laws, including privacy and civil liberties standards, we recommend that the Secretary of Homeland Security more fully justify the department's certification by taking the following actions:

1. Given that the NAO is to operate before law enforcement issues are resolved and operations are recertified, establish clear definitions for law enforcement and homeland security requests to better ensure that law enforcement requests will not be accepted until legal and policy issues are resolved.

2. Direct the NAO to address remaining issues about its processes and procedures, including
    - defining procedures for developing and approving annual memorandums for all categories of classified satellite information,
    - establishing procedures for monitoring the legal review process to ensure it is achieving its objectives,
    - ensuring that specific privacy controls outlined in the revised privacy assessment are clearly established in NAO standard operating procedures, and
    - establishing specific procedures to fully address issues raised within the civil liberties impact assessment: the potential for improper use or retention of information provided by the NAO and the potential for impermissible requests to be accepted as a result of a reliance on broad annual memorandums as justifications.

Comments from the Department of Homeland Security and Our Evaluation

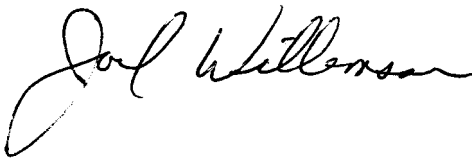
In responding to our request for comments on a draft of this letter, the NAO program director stated that the comments provided by DHS in September 2008 regarding our briefing slides were to be considered the department's official response to our certification review.

In those written comments, (reprinted in enclosure II) the DHS Deputy Undersecretary for Mission Integration described steps that DHS has taken or plans to take to address our recommendations. Regarding our first recommendation, the Deputy Undersecretary stated that the definitions for law enforcement and homeland security requests outlined in the charter were sufficiently clear for the NAO to operate in an effective and lawful manner. However, we believe that clearer definitions are essential to ensuring that law enforcement requests are effectively and consistently excluded from consideration by the NAO. The Secretary's certification of compliance depends critically on the assertion that requests for law enforcement domain uses will not be accepted by the NAO until interagency agreement is reached on unresolved legal and policy issues. Without clearer definitions that unambiguously distinguish the law enforcement and homeland security domains, the NAO runs the risk that requests may be accepted without a complete analysis of how the NAO will ensure compliance with applicable laws.

Regarding our second recommendation, the Deputy Undersecretary highlighted steps the agency is taking to update its processes and procedures, including updating its internal procedures to address civil liberties issues and focusing resources on training NAO staff and customers, particularly with respect to the collection, use, and retention of personally identifiable information. We agree that these steps, once completed, should provide DHS with better assurance that NAO's processes and procedures are effective in ensuring the program's compliance with applicable laws, privacy and civil liberties standards.

We are sending copies of this report to interested congressional committees, the Secretary of Homeland Security, and other interested parties. We will also make copies available to others upon request. In addition, this product will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions concerning this report, please contact me at (202) 512-6253 or willemssenj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributions to this report were made by Linda Koontz, Director, Information Management Issues; John de Ferrari, Assistant Director; Matthew Grote; Nick Marinos; Lee McCracken; and David Plocher.



Managing Director, Information Technology

Enclosure

The Honorable Robert C. Byrd
Chairman
The Honorable Thad Cochran
Ranking Member
Subcommittee on Homeland Security
Committee on Appropriations
United States Senate

The Honorable Joseph I. Lieberman
Chairman
The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Daniel K. Akaka
Chairman
Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable John D. Rockefeller IV
Chairman
The Honorable Christopher S. Bond
Vice Chairman
Select Committee on Intelligence
United States Senate

The Honorable David E. Price
Chairman
The Honorable Harold Rogers
Ranking Member
Subcommittee on Homeland Security
Committee on Appropriations
House of Representatives

The Honorable Bennie G. Thompson
Chairman
The Honorable Peter T. King
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Silvestre Reyes
Chairman
The Honorable Peter Hoekstra
Ranking Member
Permanent Select Committee on Intelligence
House of Representatives

(311119)

GAO

Accountability * Integrity * Reliability

NATIONAL APPLICATIONS OFFICE

Certification of Compliance With Legal, Privacy, and Civil Liberties Standards Needs to Be More Fully Justified

Briefing for Congressional Staff

September 15, 2008

1

Contents

Introduction

Since the 1960s, classified satellite information collected by intelligence agencies[1] has been used, from time to time, by federal civilian agencies and other non-intelligence entities for civil, scientific, and environmental purposes (such as mapping, disaster relief, and environmental research). These uses have historically been coordinated by the Civil Applications Committee (CAC) led by the U.S. Geological Survey (USGS), a component of the Department of the Interior.

Following the events of September 11, 2001, attention has turned to information sharing as a key element in developing comprehensive and practical approaches to defending against potential terrorist attacks. Having information on threats, vulnerabilities, and incidents can help an agency better understand the risks and determine what preventative measures should be implemented. The ability to share such terrorism-related information can also unify the efforts of federal, state, and local government agencies, as well as the private sector in preventing or minimizing terrorist attacks.

Citing a growing need to use classified satellite information for civil or domestic purposes, in 2005, an independent study group reviewed the future role of the CAC and concluded that although the civil domestic users were well supported through the CAC, homeland security and law enforcement users lacked a coherent, organized, and focused process to access classified satellite information.

[1] For purposes of this briefing, the term "classified satellite information" will be used to refer to all information derived from intelligence community sources that is expected to be made available through the National Applications Office (NAO). Based on discussions with NAO officials, a substantial part—but not all—of this information is derived from sensors mounted on classified government satellites.

Introduction

In 2007, the Office of the Director of National Intelligence (ODNI) designated the Department of Homeland Security (DHS) as the executive agency and home of a newly created National Applications Office (NAO), whose mission would be to process requests for classified satellite information from, among others, non-traditional users of intelligence for civil, homeland security, and law enforcement purposes. DHS established a process whereby potential requesters for classified satellite information annually submit memorandums generally describing the information they plan to ask for, followed by a more detailed review of each actual request, to ensure legal compliance.

The Consolidated Appropriations Act, 2008, prohibited funds from being made available to commence operations of the NAO until the Secretary of Homeland Security certified that the program complies with all existing laws, including all applicable privacy and civil liberties standards, and that certification was reviewed by GAO.

GAO
Accountability * Integrity * Reliability

Objectives

On April 9, 2008, in a letter to members of Congress, the Secretary of the Department of Homeland Security certified that NAO complies with all existing laws, including all applicable privacy and civil liberties standards. The Secretary also provided a charter for the office, privacy and civil liberties impact assessments, and NAO standard operating procedures.

Our objectives were to determine the extent to which DHS justified its certification that the NAO complies with (1) all applicable laws, (2) privacy standards, and (3) civil liberties standards.

5

Scope and Methodology

To assess DHS certification of compliance with all applicable laws, we reviewed the certification documents to determine the extent to which DHS evaluated and addressed laws applicable to NAO operations. Specifically, we reviewed DHS' assessment of applicable laws such as the Posse Comitatus Act—which generally prohibits the use of U.S. military personnel to enforce civilian laws, unless otherwise authorized by law—and the 4th Amendment to the Constitution, which guards against unreasonable searches and seizures. We also reviewed related executive branch directives, including Executive Order 12333, which limits how federal agencies in the intelligence community collect information concerning U.S. persons.[2] We interviewed agency officials from the NAO program office and the DHS Office of General Counsel to identify all available analysis conducted on applicable laws and to determine the extent to which mechanisms for ensuring compliance had been established.

[2] Executive Order 12333 defines a U.S. person as a U.S. citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government(s).

Scope and Methodology

To assess DHS certification of compliance with privacy standards, we reviewed two versions of the privacy impact assessment developed for the program (one completed in connection with the April 2008 certification and a revised version developed in July 2008 in response to discussions with us) and interviewed officials from the program office and the DHS Privacy Office. To identify DHS privacy responsibilities, we reviewed the Privacy Act of 1974, Homeland Security Act of 2002, and E-Government Act of 2002. We compared the original and revised NAO privacy impact assessments with DHS privacy impact assessment guidance as well as the Fair Information Practices, a widely accepted set of standards for protecting the privacy and security of personal information. In addition, we analyzed the system-of-records notices identified within the certification documentation and by DHS to determine whether they provided public notice regarding the NAO's planned operations and potential use of personal information.

To assess DHS certification of NAO compliance with civil liberties standards, we reviewed the civil liberties impact assessment (CLIA) to identify concerns raised about civil liberties and recommendations made to address them. We compared the content of the CLIA to a set of standard civil liberties assessment criteria developed by DHS for analyzing a program's potential civil liberties impact, including questions about the impact on particular groups or individuals, such as racial or ethnic groups; the impact on the influence of government in its relationship with private citizens; and whether alternatives and safeguards have been considered to address potential concerns. We also interviewed officials from the program office and the DHS Office of Civil Rights and Civil Liberties to determine the extent to which DHS had instituted measures to address the concerns raised by the CLIA.

We interviewed officials at the USGS and National Geospatial-Intelligence Agency (NGA) to obtain information on how requests for information from classified satellites are currently processed for federal civilian agencies. This information pertained to compliance with applicable laws as well as privacy and civil liberties standards.

We conducted this performance audit in the Washington, D.C., area from April 2008 to September 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

DHS has not fully justified its certification that the NAO complies with applicable laws.

Although the department has established procedures for legal review, it has not yet fully addressed all outstanding issues regarding how the planned operations of the NAO, as described in the department's certification documents, are to comply with legal requirements. Specifically:

- DHS has not resolved legal and policy issues associated with NAO support for law enforcement. The NAO charter states that requests for law enforcement domain uses (i.e., activities relating to enforcing criminal or civil laws or investigating violations thereof) will not be accepted by the NAO until interagency agreement is reached on unresolved legal and policy issues. The Independent Study Group had determined that the legality of using satellite imagery of domestic subjects for law enforcement purposes raised difficult issues that had not been fully settled. Work has begun to address these issues, and the department now plans to re-certify the NAO's compliance with all laws before accepting requests related to law enforcement. Recertification following the resolution of legal and policy concerns will be an important element in providing assurance that NAO operations are in compliance with all applicable laws.

- DHS has taken steps to develop a legal review procedure for classified satellite information requests but has not yet fully established management controls to ensure that it will be effective. DHS has developed a multi-stage process for reviewing potential requests to address any legal or policy concerns. This process represents a reasonable approach for ensuring that decisions are reviewed on a case-by-case basis, to the extent that law enforcement requests are not accepted. However, the NAO charter leaves it unclear what types of requests will be initially rejected as being in the law enforcement domain and what types will be accepted as homeland security requests, because the distinctions between the two domains are not clear.
- In addition, other important details have not yet been fully addressed. The process for developing and approving annual memorandums, which set expectations about planned customer uses of NAO data, has not yet been established for all categories of classified satellite information. In addition, procedures for monitoring the legal review process to ensure it is making appropriate determinations about the legality of requests have not yet been established. Without clarifying these details of the planned legal review process, DHS will have limited assurance that the process is effective at ensuring compliance with applicable laws.

DHS has taken steps to justify its certification of compliance with privacy standards.

The DHS Privacy Office worked with NAO program officials to define privacy protections for the program and prepared a privacy assessment that discussed high-level privacy protections. Further, DHS has recently taken additional steps to justify its certification of compliance with privacy standards.

- DHS originally did not fulfill agency requirements to identify privacy risks and control mechanisms but recently has taken steps to do so. At the time of NAO certification, DHS did not fully explain how the office would comply with widely accepted privacy standards, such as the need for personally identifiable information to be accurate, secure, and used only for limited purposes. Specifically, NAO's original privacy assessment did not identify or analyze the risks that NAO operations might not meet these standards, nor did it specify measures to mitigate such risks. In response to discussions with us regarding these shortcomings, the Privacy Office developed a revised assessment that represents a substantial improvement in identifying privacy risks and mitigating controls to address them, such as providing appropriate oversight and building a process to identify and correct inaccurate information. However, differences between the review procedures outlined in the revised PIA and those in the standard operating procedures raise questions about whether the specifics of NAO's privacy protection controls have been clearly established.

Results in Brief

- The system-of-records notices cited by DHS do not provide a public explanation of the privacy protections associated with planned NAO operations. One key privacy standard requires that the public be notified about the existence of systems containing personal information and the privacy protections associated with them. However, publicly available privacy notices (called system-of-records notices under the Privacy Act of 1974) cited by DHS as applying to NAO do not provide information specifically about the NAO, its planned uses of personal information, or the privacy protections that are to be established. In response to discussions with us regarding this lack of public notice, DHS updated NAO information on the department's public Web site to reflect the relationship between the NAO and the applicable system-of-records notice. The updated information better informs the public about how personal information is to be processed, analyzed, and distributed by the NAO.

DHS identified civil liberties concerns associated with NAO operations but has not yet fully addressed them.

The Department's assessment of the civil liberties impact of NAO operations identified a number of areas of potential concern regarding civil rights and civil liberties. Although the NAO program office addressed several of these issues—such as the need to develop and conduct training on civil liberties issues—the department has not indicated how NAO would address other significant issues, including the potential for improper use or retention of intelligence information by customers, and the potential for overly broad, annual memorandums about customers' planned uses that may facilitate the acceptance of requests that should be rejected.

In a July 2008 letter to the DHS Undersecretary of Intelligence and Analysis, the acting NAO program director outlined plans to address several issues raised by the assessment. However, specific measures have not yet been developed to address the potential for improper use or retention of information provided by NAO and the potential for impermissible requests to be accepted as a result of a reliance on broad annual memorandums as justifications.

Certifying the readiness of the NAO without fully addressing the concerns outlined within the assessment—including establishing internal controls for mitigating identified risks—does not provide assurance that the office is in compliance with civil liberties standards and will take appropriate measures to protect civil liberties.

Without fully justifying its certification, DHS lacks assurance that NAO operations will comply with applicable laws and privacy and civil liberties standards. To help ensure that NAO is in compliance with such laws and standards, we recommend that the Secretary of Homeland Security more fully justify the department's certification by

1. establishing clear definitions for law enforcement and homeland security requests to better ensure that law enforcement requests will not be accepted until legal and policy issues are resolved, and
2. directing NAO to address remaining issues regarding its processes and procedures, including:
   - defining procedures for developing and approving annual memorandums in all categories,
   - establishing procedures for monitoring the legal review process,
   - ensuring that privacy controls outlined in the revised privacy impact assessment are clearly established in standard operating procedures, and
   - establishing specific procedures to fully address issues raised by the civil liberties impact assessment.

In written comments provided on a draft of this briefing, the DHS Deputy Undersecretary for Mission Integration described steps that DHS has taken or plans to take to address our recommendations. Regarding our first recommendation, the Deputy Undersecretary stated that the definitions for law enforcement and homeland security requests outlined in the charter were sufficiently clear for the NAO to operate in an effective and lawful manner. However, we believe that clearer definitions are essential to ensuring that law enforcement requests are effectively and consistently excluded from consideration by the NAO. The Secretary's certification of compliance depends critically on the assertion that requests for law enforcement domain uses will not be accepted by the NAO until interagency agreement is reached on unresolved legal and policy issues. Without clearer definitions that unambiguously distinguish the law enforcement and homeland security domains, the NAO runs the risk that requests may be accepted without a complete analysis of how the NAO will ensure compliance with applicable laws.

Regarding our second recommendation, the Deputy Undersecretary highlighted steps the agency is taking to update its processes and procedures, including updating its internal procedures to address civil liberties issues and focusing resources on training NAO staff and customers, particularly with respect to the collection, use, and retention of personally identifiable information. We agree that these steps, once completed, should provide DHS with better assurance that NAO's processes and procedures are effective in ensuring the program's compliance with applicable laws, privacy and civil liberties standards.

Since the 1960's, federal civilian agencies have used classified satellite information for civil, scientific, and environmental purposes. In 1975, the U.S. President's Commission on Central Intelligence Agency Activities within the United States recommended that an interagency committee of federal civil agencies be established to oversee the use of classified satellites for imaging domestic areas and to allay concerns about improper or illegal uses of such imaging capabilities. In response to the Commission's recommendations, the Civil Applications Committee (CAC) was established in 1976 to serve as a mechanism for reviewing and prioritizing the needs of civilian agencies for classified satellite information.

In response to the events of September 11, 2001, information sharing has been identified as a key element in developing comprehensive and practical approaches to defending against potential terrorist attacks. Having information on threats, vulnerabilities, and incidents can help an agency better understand the risks and determine what preventative measures should be implemented. The ability to share such terrorism-related information can also unify the efforts of federal, state, and local government agencies, as well as the private sector in preventing or minimizing terrorist attacks. Exchanging terrorism-related information continues to be a significant challenge for federal, state, and local governments—one that we recognize is not easily addressed. Accordingly, since January 2005, we have designated information sharing for homeland security a high-risk area.[3]

[3] For more information, see GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007), p.47, and GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.: Mar. 17, 2006).

The mission of the CAC has been to facilitate the appropriate civil uses of data collected by classified government satellites. Led by the U.S. Geological Survey (USGS), the CAC includes representatives from the Departments of Agriculture, Commerce, Health and Human Services, Homeland Security (DHS), the Interior, and Transportation; the U.S. Army Corps of Engineers; the Environmental Protection Agency; the Federal Emergency Management Agency; the National Science Foundation; the U.S. Coast Guard; and the National Aeronautics and Space Administration.

According to its charter, the CAC's responsibilities include, among other things:

- assisting in ensuring the effective application of classified satellite information to support the appropriate worldwide production, analysis, and research programs of federal civil agencies;
- facilitating the use of such data to derive basic information for civil applications, including mapping, disaster assessments, monitoring environmental changes, and for deriving other information to support national policies and objectives; and
- overseeing federal civil agencies' requests for the collection of classified satellite information to ensure the constitutional and other legal rights of U.S. persons are not violated and that such requests and the use of such data are consistent with the authorities and responsibilities of the agencies and are in accordance with authorized programs.

Citing a growing need for domestic uses of information collected by intelligence agencies, in May 2005, the Office of the Director of National Intelligence (ODNI) and USGS chartered an Independent Study Group to conduct a review of the future role of the CAC for the facilitation, management, and oversight of classified satellite information for civil or domestic use.[4] The group, composed of former senior government and military officials and consultants, concluded in its report (known as the Blue Ribbon Study) that although civil users were well supported through the CAC, homeland security and law enforcement users lacked a coherent, organized, and focused process to access classified satellite information.[5] Further, the report stated that most of these users did not understand how classified satellite information could be applied to support their missions and functions and, likewise, that intelligence agencies lacked a comprehensive understanding of the needs of those users.

[4] Independent Study Group, Civil Applications Committee Blue Ribbon Study (September 2005).

[5] The report discussed the use of intelligence capabilities, which include the technical and analytic assets of intelligence agencies. For purposes of this report, we are focusing on the use of classified satellite information.

As a result of its findings, the study group recommended the establishment of a domestic applications program to provide a focal point and act as a facilitator between intelligence agencies and their potential customers, such as homeland security and law enforcement users. The study group recommended that the office be informed by working groups from three domestic user domains: civil, homeland security, and law enforcement, and be modeled after the operations of the CAC. The group also recommended that the establishment of the office be informed by a comprehensive review of legal and policy issues.

Responding to the study group's recommendations, ODNI began planning the National Applications Office (NAO) in September 2006 and, in May 2007, designated DHS as its executive agent. Following the August 2007 DHS publication of the NAO's mission, a congressional hearing was held in September 2007 to examine the privacy and civil liberties implications of using classified satellite information for domestic purposes.

The Consolidated Appropriations Act, 2008, prohibited funds provided in the act from being available to commence NAO operations until the Secretary of DHS certified that the program complies with all existing laws, including all applicable privacy and civil liberties standards, and that certification was reviewed by GAO.

On April 9, 2008, in a letter to members of Congress, the DHS Secretary certified that the NAO, as described in its charter and standard operating procedures, complies with all existing laws, including all applicable privacy and civil liberties standards. The Secretary also provided the following supporting documentation:

- The **NAO Charter** – The charter defines the mission of the NAO and the responsibility of its members. The charter was approved in February 2008 by the Attorney General, Director of National Intelligence, Secretary of the Interior, Secretary of Homeland Security, and Secretary of Defense.
- A **Privacy Impact Assessment** (PIA) –The PIA was reviewed and approved by the DHS Privacy Office, which is responsible for ensuring PIAs are conducted to identify specific privacy risks and controls needed to mitigate those risks.[6] The PIA describes how the NAO plans to address the Fair Information Practices—a set of widely-accepted principles for protecting the privacy and security of personal information that include such things as limiting the collection and use of such information and ensuring that it is accurate for its intended purpose. The PIA concludes that privacy risks have been minimized by the institution of multi-layered protection mechanisms involving personnel management, IT system security, and business processes.

[6] As directed by section 222 of the Homeland Security Act, the DHS Privacy Office is responsible for, among other things, ensuring that the department is in compliance with federal laws that govern the use of personal information by the federal government. Further, the E-Government Act of 2002 requires agencies to conduct PIAs before developing or procuring information technology that collects, maintains, or disseminates information in an identifiable form. The E-Government Act specifically exempts national security systems from its privacy provisions. However, DHS policy requires PIAs to be completed for intelligence programs but, consistent with the E-Government Act, does not make these PIAs public.

- A **Civil Liberties Impact Assessment** (CLIA) – The DHS Civil Rights and Civil Liberties Office conducts these assessments to help ensure that civil liberties are considered as the department develops or implements laws, regulations, policies, procedures, and guidelines related to efforts to protect the nation against terrorism.[7] The NAO CLIA discusses potential civil liberties impacts, identifies safeguards in place, and makes recommendations for additional measures. It concludes that due to the nature of the NAO mission, rigorous oversight of the office, and existing safeguards, the NAO is unlikely to impact on individuals' civil liberties in a substantial way.
- **Standard Operating Procedures** – These procedures cover the required steps involved in the submission, approval, and processing of information requests in support of civil, homeland security, and law enforcement purposes when such requests are submitted through the NAO.

[7] The responsibilities of the Civil Rights and Civil Liberties Office include overseeing DHS compliance with constitutional, statutory, regulatory, policy, and other requirements relating to the civil rights and civil liberties of individuals affected by the agency's programs and activities.

According to its charter, the mission of the NAO is to serve as an independent advocate for the use of, and facilitate access to, classified satellite information by, among others, non-traditional users of intelligence in the following three domains:

- **Civil Applications** includes entities involved with domestic and international research, analysis, and operations designed to support the assessment and management of environmental issues and natural resources, evaluating socioeconomic conditions, producing maps and charts, and assessment, preparation and response to disasters.
- **Homeland Security** includes those government agencies and activities involved in the prevention and mitigation of, preparation for, response to, and recovery from natural or man-made disasters, including terrorism, and other threats to the homeland.
- **Law Enforcement** includes government law enforcement entities when they are seeking to enforce criminal or civil laws or investigate violations thereof.

For each of the three domains, NAO's function is to

- review, coordinate and advocate for requests from government entities for classified satellite information (agencies may also directly contact the intelligence community for access to intelligence capabilities);
- advocate future technology needs to the intelligence community;
- educate potential users about intelligence capabilities and how and when they might be leveraged to support their needs within the existing policy and legal frameworks;
- if necessary, analyze data received from providers to meet the needs of the requesters; and
- promote information sharing through the effective and efficient use of intelligence capabilities.

In carrying out these functions, NAO's goal is to

- protect privacy, civil rights, and civil liberties;
- lawfully and appropriately use intelligence capabilities; and
- protect the confidentiality of the sources and methods used to collect the information.

Three categories of classified satellite information are to be provided through the NAO:[8]

- **Geospatial intelligence (GEOINT)** – GEOINT is defined as "the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information."
- **Measurement and signature intelligence (MASINT)** – MASINT is defined as intelligence "derived from measurements of physical phenomena intrinsic to an object or event." These phenomena can include the following types: "electro-optical, infrared, laser, spectral, radar, polarimetric, high-power or unintentional radio frequency emanations, geophysical, chemical, biological, radiological, or nuclear."
- **Electronic intelligence (ELINT)** – ELINT is defined as "technical and geolocation intelligence derived from non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. It does not include oral or written communications." Thus, ELINT could include intelligence based on signals from machines, such as computers, but not telephone conversations or other communications between individuals.

[8] Department of Homeland Security, National Applications Office Charter, pp. 13-14 (February 2008), National Applications Office Standard Operating Procedures Requirements Process for Electronic Intelligence, p. 1 (March 2008), National Applications Office Standard Operating Procedures Requirements Process for Measurement and Signature Intelligence, p. 7 (March 2008).

In addition, according to the charter, NAO may provide open source intelligence information, derived from publicly available information that anyone can lawfully obtain by request, purchase, or observation. For example, DHS officials stated that certain requests might be most easily filled with publicly available mapping imagery.

According to its charter NAO will not accept any requests that fall within the law enforcement domain when it begins operations.[9] Such requests will not be accepted until legal and policy issues are resolved. For all other requests, NAO acceptance of requests for classified satellite information relies on a two-phased process:

Filing of annual memorandums

As a first phase, potential requesters (i.e., agencies within the civil and homeland security domains) are to annually submit memorandums that generally describe the information they plan to request and its intended use.

Processing of individual requests

In the second phase of the process, NAO has defined a six-step review procedure for individual information requests.

[9] In addition, according to the charter, prior to the establishment of the law enforcement applications domain committee, the NAO will not accept any requests from state, local, tribal, and territorial law enforcement entities, even if the subject of such requests properly resides in the homeland security domain.

DHS has not resolved legal and policy issues associated with NAO support for law enforcement operations.

The NAO is intended to support law enforcement as a key element of its mission. Its charter states that the office is to be an advocate for the use of intelligence community capabilities by civil, homeland security, and law enforcement communities, and DHS officials have said that the NAO will eventually process law enforcement requests. Further, the Independent Study Group, which was an impetus to the creation of the NAO, cites assistance to law enforcement as a major reason to establish the NAO.

The Independent Study Group determined that the legality of using satellite imagery of domestic subjects for law enforcement purposes was a difficult issue that had not been fully settled. For example, it stated that no case regarding the use of military, civil, or commercial satellites has been brought to court. The study group also stated that appropriate safeguards were needed to ensure that classified satellite information would be used lawfully and with full consideration of the rights of U.S. persons.

DHS Certification of Compliance with Applicable Laws

The NAO certification documents include discussions of the applicability of certain laws, such as the 4th Amendment to the Constitution, and executive branch directives, such as Executive Order 12333—which limits how federal agencies in the intelligence community collect information concerning U.S. persons. For example, the CLIA includes a discussion of the Posse Comitatus Act, which generally prohibits the use of U.S. military personnel to enforce civilian (civil or criminal) laws, unless otherwise authorized by law. The CLIA concludes that there is little likelihood that NAO activities will raise Posse Comitatus Act issues.

However, DHS analysis of these laws did not resolve the legal issues of using intelligence community capabilities for law enforcement purposes. For example, regarding the 4th Amendment to the Constitution, which guards against unreasonable searches and seizures, the CLIA notes that NAO's involvement in law enforcement uses "remains under consideration and thus its ultimate contours are not known at this time." The document states that the Civil Rights and Civil Liberties Office will update its assessment and assist in constructing polices and procedures for law enforcement use. This indicates that, with respect to issues related to law enforcement, NAO certification is not yet complete.

29

DHS Certification of Compliance with Applicable Laws

DHS certification recognizes that law enforcement issues have not been resolved and, in response, states that law enforcement requests will not be accepted until such issues are resolved. The NAO charter established a Policy and Legal Working Group to develop responses to the legal and policy concerns. The group plans to conduct analyses and make recommendations regarding potential changes in policy and law regarding permissible access to classified satellite information for law enforcement purposes. At the time of our review, the working group had begun its work but had yet to complete its analysis or make recommendations.

According to the acting NAO director, it was an agency priority to begin operations at the NAO as soon as possible and thus a decision was reached to set unresolved law enforcement issues aside and proceed with certification of legal compliance for the rest of the NAO's planned operations.

In responding to our questions regarding law enforcement issues, the DHS Deputy Undersecretary for Mission Integration, who oversees NAO, stated that the agency will provide an additional certification before the law enforcement domain becomes operational. Recertification following the resolution of legal and policy concerns will be an important element in providing assurance that NAO operations are in compliance with all applicable laws.

DHS took steps to develop a legal review procedure for requests but has not yet established sufficient management controls to ensure that it will be effective.

The DHS Secretary's certification letter states that NAO's charter and standard operating procedures were carefully crafted to ensure compliance with all applicable laws. The charter also states that a primary function of the office will be to ensure that its procedures are in accordance with laws, policies, and procedures that protect privacy, civil rights, and civil liberties.

Given the need to ensure compliance with all laws, it is important that NAO establish management controls to ensure that only requests that meet established criteria are accepted. According to government standards, management controls (or internal controls) are the policies, procedures, techniques, and mechanisms that help ensure that management's directives are carried out.[10] Management controls can include a wide range of diverse activities, such as approvals and authorizations, which vary depending on agency missions, organization, complexity and other factors, and should be clearly documented in agency directives, policies, and other guidance. Further, processes need to be established to monitor management controls on a regular basis to ensure they are achieving their objectives.

[10] GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999), p.11.

DHS Certification of Compliance with Applicable Laws

As its management control to ensure compliance with applicable laws, DHS developed a multi-stage legal review process for all requests submitted to NAO. According to the charter and standard operating procedures, assurance that information requests are consistent with applicable laws and official policy will occur through the review of requests by the NAO staff, the legal staff of the relevant collecting agencies, and, as appropriate, other federal agencies. As previously described, this will involve interagency review when "special uses," such as the use of U.S. person data or law enforcement functions, are being requested, as well as review by the DHS Secretary or Deputy Secretary of uses that involve novel or significant homeland security uses, or where the use of a new technology has 4th Amendment implications.

This process represents a reasonable approach for ensuring that decisions are reviewed on a case-by-case basis to the extent that law enforcement requests are not accepted, which is a critical element of the process. As the Office for Civil Rights and Civil Liberties has pointed out in the CLIA, the impact on NAO operations of 4th Amendment and other law enforcement issues cannot yet be evaluated because "the ultimate contours [of NAO support for the Law Enforcement Domain] are not known at this time."

However, NAO has not established clear definitions of the homeland security and law enforcement domains to guide decisions by NAO and other agency officials and to ensure that law enforcement requests are not accepted.

As previously discussed, the NAO charter describes three civilian customer domains that could use intelligence capabilities in support of their missions—civil applications, homeland security, and law enforcement. Homeland security includes those government agencies and activities involved in the prevention and mitigation of, preparation for, response to, and recovery from natural or man-made disasters, including terrorism and other threats to the homeland. Law enforcement includes law enforcement entities when they are seeking to enforce criminal or civil laws or investigate violations thereof. However, the charter further states that when law enforcement entities are “not so focused,” their activities may fall within the homeland security domain.

The domain definitions are unclear because they describe functions that could overlap. For example, law enforcement entities would likely be involved in seeking to enforce homeland security laws, such as the USA PATRIOT Act or the Intelligence Reform and Terrorism Prevention Act. It is not clear whether that function would be interpreted as falling under the homeland security or law enforcement domain, because elements of both domains are involved.

Likewise many other types of homeland security functions have the potential to overlap with law enforcement functions, thus leaving it unclear how they would be categorized. For example, border security involves closely interrelated law enforcement and homeland security functions. A request for imagery along the U.S. border might be interpreted as a law enforcement matter (e.g., surveillance of suspected criminal activity), in which case it is not to be accepted by the NAO under the office's initial operating procedures. However, alternatively, the request might be considered a homeland security matter (e.g., serving a broader objective of protecting the border). In that case, the request might be accepted.

This lack of clarity is exacerbated by the fact that while NAO does not plan to accept law enforcement requests initially, it will accept requests from federal law enforcement agencies for homeland security purposes.

DHS officials acknowledged the overlap between the two domains, but stated that they expect that the review process for requests outlined in the NAO charter, along with communication between NAO and the requester, will provide sufficient clarity for distinguishing between law enforcement and homeland security requests.

However, the review process outlined within the charter relies upon the domain definitions included in that document. Without clear domain definitions, DHS cannot be certain that requests related to law enforcement are being effectively and consistently excluded from consideration. And because law enforcement issues have not yet been analyzed and resolved, the NAO therefore runs the risk that requests may be accepted without a complete analysis of how the NAO will ensure compliance with applicable laws.

Other important details of how the legal review process is to be implemented have also not yet been determined. For example,

- The process for developing and approving annual memorandums for MASINT and ELINT has not been delineated. Such procedures are an important control in assuring that access, retention, and sharing of information is properly constrained.
- Specific processes have not yet been established for monitoring the legal review process on a regular basis to ensure it is achieving its objectives. Monitoring the NAO's operations will be important to ensure that planned privacy and civil liberties protections are being implemented as intended.

NAO officials stated that they are in the process of developing these procedures. For example, they stated that MASINT and ELINT procedures will be developed that mirror existing GEOINT procedures. They also stated that it would be up to the Privacy Office, Civil Rights and Civil Liberties Office, and Office of the Inspector General to determine how they will monitor the program to ensure it is achieving its objectives.

However, officials did not provide milestones for completing procedures that are in process or state when monitoring procedures will be developed. Until the procedures are adequately defined, DHS will have limited assurance that the process is effective at ensuring compliance with applicable laws.

DHS originally did not fulfill agency requirements to identify privacy risks and control mechanisms but recently has taken steps to do so.

Under law, Office of Management and Budget guidance, and DHS guidance, DHS is to conduct privacy impact assessments (PIA) to ensure that the technology used by DHS sustains and does not erode privacy protections. Specifically, DHS guidance states that a PIA should be completed for any program, system technology, or rulemaking that involves personally identifiable information.

The guidance also states that a PIA should accomplish two goals:

- determine the risks and effects of collecting, maintaining and disseminating information in identifiable form via an electronic information system; and
- evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

In order to accomplish these goals, PIAs are required to include “privacy impact analysis” sections that assess privacy risks and identify specific steps to be taken to mitigate those risks.

DHS Certification of Compliance with Privacy Standards

PIAs can serve as an analysis of adherence to the Fair Information Practices. These practices, first proposed in 1973 by a U.S. government advisory committee, are now widely accepted as principles for protecting the privacy and security of personal information. The DHS Privacy Office defines these principles as follows:

- *Transparency* - DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).
- *Individual participation* - DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS use of PII.
- *Purpose specification* - DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- *Data minimization* - DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose and only retain PII for as long as is necessary to fulfill the specified purpose.

DHS Certification of Compliance with Privacy Standards

- *Use limitation* - DHS should use PII solely for the purpose specified in the notice. Sharing PII outside the department should be for a purpose compatible with the purpose for which the PII was collected.
- *Data quality and integrity* - DHS should, to the extent practical, ensure that PII is accurate, relevant, and timely, within the context of each use of the information.
- *Security* - DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- *Accountability and auditing* - DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

40

The original NAO PIA was divided into sections that correspond to the Fair Information Practices. For each principle, a planned course of action was described. For example, the principle of purpose specification was to be addressed through the use of annual memorandums, which state requesters' intended uses. Based on the discussions in these sections, the PIA concluded that privacy risks had been minimized by instituting multi-layered protection mechanisms involving personnel management, information technology (IT) system security, and business processes.

The PIA further stated that the NAO did not anticipate routinely collecting, storing, and disseminating personally identifiable information and that, in those instances when it did, the information would be maintained and disseminated in accordance with applicable laws, regulations, and polices. In discussing the original PIA, DHS Privacy Office officials noted that NAO's adherence to privacy standards was assured in part because it was expected to be staffed with individuals who would be trained in privacy protection standards and who would be required to adhere to authorities such as Executive Order 12333, which includes limits on the extent and manner in which information about U.S. persons is collected by intelligence agencies. In addition, they stated that the NAO's planned multi-stage review process for requests would also help ensure that privacy standards are met. For example, that review process could include consultation with the Privacy Office if it is deemed necessary. Because these broad measures were in place, Privacy Office officials believed that NAO operations would meet privacy standards.

However, although it described privacy protections in general terms, the original PIA did not fully analyze privacy risks or identify specific ways to mitigate them.

For example:

- *Data quality and integrity* – DHS guidance requires agency information on U.S. persons to be accurate, relevant, and timely. However, the original PIA did not discuss this risk or other specific risks regarding the accuracy of personal information to be processed by the NAO. The PIA asserted that the office would follow "appropriate policies and procedures" to ensure data quality but did not identify the polices and procedures. Thus, the document did not identify the risks associated with use of inaccurate data or discuss how specific controls would mitigate these risks.
- *Security* – DHS guidance requires agency information on U.S. persons to be protected by proper safeguards and security measures; however, the original PIA did not identify the specific security risks. The PIA asserted the office would follow applicable security policies and procedures, including the use of password-protected storage of information. However, these statements only referred generically to the use of standard security controls. They did not discuss how such techniques addressed the specific security risks.

- *Use limitation* – DHS guidance requires agency information on U.S. persons to be used only for the purposes for which it was originally collected. The original PIA stated that the "NAO will use a multi-layer system of protection to ensure that information passing through or stored by the NAO is in compliance with privacy and civil liberties laws and policies of the United States." It also stated that the NAO would adhere to NGA policies related to proper use of information. However, the PIA did not discuss specific risks associated with inadequately limiting the use of personal information that NAO might be distributing. For example, by broadly sharing information with non-federal users, who are not bound by the Privacy Act, personal information could be at risk of being used in ways not specified when it was originally collected. The PIA did not discuss control mechanisms for mitigating risks such as this.

DHS Certification of Compliance with Privacy Standards

In discussions with us, the DHS Director of Privacy Compliance acknowledged these shortcomings in the original PIA. In response, the Privacy Office developed and issued a revised PIA on July 28, 2008, that more fully addressed risks and mitigating controls. The revised document identifies four overall privacy risks associated with the operation of the NAO:

1. An individual may be unaware that personally identifiable information will be collected about him or her in response to a request processed by the NAO.
2. Personally identifiable information may be collected, analyzed, or disseminated in a manner that makes the information inaccurate.
3. Personally identifiable information may be misused by a requestor.
4. Associated technology may improve so dramatically that qualitatively new capabilities will enable the gathering of personally identifiable information in ways that are impossible today, thus creating new potential privacy risks.

The PIA states that these risks can be mitigated by providing appropriate oversight, building a process to identify and correct inaccurate information, and ensuring that the DHS Privacy Office and DHS Office for Civil Rights and Civil Liberties remain critical components of all review processes as new and improved technology is developed.

The revised PIA also identifies specific privacy risks associated with several of the individual Fair Information Practices and outlines measures taken by the NAO to address them. For example, regarding Use Limitation, the assessment identifies the risk that users of NAO-provided information may distribute NAO products inappropriately. The PIA states that the review processes for annual memorandums and requests, along with a process for educating potential and actual customers, are to mitigate the risk of improper use of information.

However, several of the mitigating techniques identified in the revised PIA include specifics that differ from the standard operating procedures. For example, to address risks associated with the data quality and integrity of NAO-provided information, the PIA stated that NAO will implement several internal quality reviews conducted by officials not cited in NAO program documentation.

DHS Certification of Compliance with Privacy Standards

According to the DHS Director of Privacy Compliance, the DHS Privacy Office plans to meet with NAO officials to discuss the revised PIA and their plans to implement the controls that will be required to address the identified risks.

The revised PIA represents a substantial improvement over the original PIA in identifying privacy risks and mitigating controls to address them. However, the differences between the review procedures outlined in the revised PIA and those in the standard operating procedures raise questions about whether the specifics of NAO's privacy protection controls have been clearly established.

The system-of-records notices cited by DHS do not provide a public explanation of the privacy protections associated with planned NAO operations.

A key DHS privacy principle states that the agency should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information. In addition, the Privacy Act requires agencies to notify the public, via a notice in the *Federal Register* known as a system-of-records notice (SORN), when they create or modify systems of records. This requirement is in place to protect the public's right to know about the government's collection of its personal information.

The certification documents state that DHS complies with the Privacy Act notice requirement through the publication of the Homeland Security Operations Center (HSOC) Database SORN, issued in April 2005. The HSOC opened in 2004 to serve as a center for real-time threat monitoring, domestic incident management, and information sharing efforts.

The HSOC Database SORN stated that the HSOC Database "serves as the technological platform to receive threat information, integrate it and disseminate it." According to the notice, the HSOC Database contains law enforcement information, intelligence information, and other information for identifying and assessing the threats to the homeland,[11] and the HSOC Database will disclose information to "a Federal, state, local, joint, tribal, foreign, international or other public agency or organization, or to any person or entity in either the public or private sector, domestic or foreign, where such disclosure may promote assist or otherwise serve homeland or national security interests."

However, the SORN does not identify the NAO or specifically describe its potential uses of personal information.

[11] The notice states that "the HSOC database includes intelligence information and other information received from agencies and components of the Federal Government, foreign governments, organizations or entities, international organizations, state and local government agencies (including law enforcement agencies), and private sector entities, as well as information provided by individuals, regardless of the medium used to submit the information or the agency to which it was submitted. This system also contains: information regarding persons on watch lists with possible links to terrorism; the results of intelligence analysis and reporting; ongoing law enforcement investigative information, information systems security analysis and reporting; historical law enforcement information, operational and administrative records; financial information; and public-source data such as that contained in media reports and commercial databases as appropriate to identify and assess the nature and scope of terrorist threats to the homeland, detect and identify threats of terrorism against the United States, and understand such threats in light of actual and potential vulnerabilities of the homeland."

According to DHS officials, the HSOC Database SORN had broad applicability to programs within the Office of Intelligence and Analysis, including NAO.

Further, after the NAO certification was made, DHS issued a new SORN for the Office of Intelligence and Analysis Enterprise Records System on May 15, 2008. According to DHS officials, this notice replaced the HSOC Database SORN as the relevant notice for NAO. The new notice states that the Intelligence and Analysis Enterprise Records System is the single system of records to support all Intelligence and Analysis operations, including analysis and information sharing. Like the previous document, the new notice does not identify the NAO or specifically describe its potential uses of personally identifiable information.

In response to discussions with us regarding the lack of public notice, DHS officials stated that a more extensive public notice would not be appropriate for intelligence activities but that they would update NAO information on the department's public Web site to note that the privacy protections described in the Intelligence and Analysis Enterprise Records System notice apply to NAO. Explicitly linking NAO to the existing notice better informs the public about how personal information is to be processed, analyzed, and distributed by the NAO.

DHS identified civil liberties concerns associated with NAO operations but has not yet fully addressed them.

The DHS Office of Civil Rights and Civil Liberties is responsible for, among other things, assisting the Secretary of DHS and agency offices in developing, implementing, and periodically reviewing agency policies and procedures to ensure that the protection of civil rights and civil liberties is appropriately incorporated into the department's programs and activities. According to officials, civil liberties impact assessments (CLIA) serve as a tool to assist in protecting civil rights and civil liberties as DHS programs are developed.

The CLIA discussed efforts by DHS to take into consideration civil rights and civil liberties during the development of the NAO program. For example, the CLIA discussed various safeguards, including establishment of a training program regarding duties and responsibilities to protect civil rights and civil liberties. In addition, the CLIA highlighted the program office's working relationship with the Office of Civil Rights and Civil Liberties and the DHS Privacy Office in developing the charter and standard operating procedures. The CLIA also stated that the NAO had benefited from significant input from the DHS Office of General Counsel. The assessment concluded that due to the nature of the NAO mission, rigorous oversight of the office, and existing safeguards, the NAO is unlikely to impact on individuals' civil liberties in a substantial way.

DHS Certification of Compliance with Civil Liberties Standards

Officials from the Civil Rights and Civil Liberties Office told us that they had provided feedback to NAO as they conducted their review and that measures had been added to the program to address their concerns.

Although the CLIA discusses how many of the issues it raises will be resolved and concludes that sufficient safeguards are in place, two significant issues related to civil liberties risks were raised that NAO has not responded to with a clear indication of how they are to be resolved. These issues are

- the potential for improper use or retention of information provided by NAO, and
- the potential for impermissible requests to be accepted as a result of a reliance on broad annual memorandums as justifications.

Potential for Improper Use or Retention of Information Provided by NAO

The CLIA raised concern regarding improper use and retention of requested information by NAO's customers and its impact on U.S. persons' civil liberties. Specifically, the CLIA stated that "the manner in which information is accessed, used, and shared between the requester, the facilitator (NAO), the originating agency, and any information sharing partners has civil liberties implications." Although information may be lawfully collected and is being used lawfully by the end user, "it is unclear [after the authorized use is complete] what will happen to the U.S. person information lawfully collected."

The CLIA recommended that two specific actions be taken to mitigate this risk:

- NAO should vet all requests to amend access, retention, and sharing instructions contained in annual memorandums; and
- procedures and/or a system for tracing dissemination and access of products should be extended beyond NAO to customers as a condition of service.

In response, NAO inserted a footnote into its standard operating procedures stating that it would vet all requests to amend access, retention, and sharing instructions contained in the original annual memorandum. The footnote also stated that access, retention, and sharing provisions were already included in existing proper use memorandums that govern requests to NGA. Finally, the footnote stated that procedures and/or a system for tracing dissemination and access of products will be extended beyond NAO to the requesters as a condition of service. However, no specific procedures have been developed regarding how such actions are to be implemented by NAO, and thus it is unclear whether the risk identified in the CLIA has been adequately addressed.

In a July 2008 letter to the DHS Undersecretary for Intelligence and Analysis regarding plans to address recommendations identified within the CLIA, the acting NAO program director stated that NAO staff would continue to work with other intelligence agencies to explore additional ways to monitor and enable appropriate dissemination and access of products, including a discussion of how technology may assist in this process.

Such a dialogue could assist the NAO in determining how best to implement these controls. However, until the NAO establishes specific procedures for vetting amendments to existing annual memorandums and tracing dissemination and access of products, it is uncertain whether this risk has been adequately addressed.

Potential For Impermissible Requests as a Result of Broad Annual Memorandums

The CLIA stated that annual memorandums will be used as the primary method of categorizing the nature of multiple, recurring requests. While the CLIA indicated that such a process provides certain safeguards against the improper dissemination of personally identifiable information, it also stated that such agreements could potentially be formulated so broadly that they result in requests that could lead to a violation of civil liberties. For example, state and local agencies might group together by region to submit requests under a single annual agreement created by a regional information sharing center. The CLIA stated that allowing multiple customers to use a single annual memorandum could result in requests being made by individuals who lack the proper authority to do so.

The CLIA recommended placing limits on what can be requested at the outset of the process to prevent potential mission creep, improper sharing, and improper requests. Further, it stated that failing to establish such limits increased the risk that improper requests would be received and could slip through the NAO's review process.

The certification documents generally outlined NAO's annual memorandum process, but they did not set the recommended limits or identify controls to enforce them.

NAO officials stated that civil liberties controls, such as those necessary to address the civil liberties risks identified in the CLIA, were not fully identified in the certification documentation because the NAO is in the early stages of its development and has not yet documented many of its internal controls.

Prior to the NAO certification, DHS indicated that it planned to address certain civil liberties concerns outlined in the assessment. On April 8, 2008, the DHS Undersecretary for Intelligence and Analysis stated in a memorandum to the Civil Rights and Civil Liberties Office that he concurred with the report and that elements were already being incorporated into NAO management.

The acting NAO program director's July letter outlining plans for implementing several of the CLIA recommendations demonstrates the agency's commitment to addressing civil liberties concerns. However, specific measures to address the potential for improper use or retention of information provided by NAO and the potential for impermissible requests to be accepted as a result of a reliance on broad annual memorandums as justifications have not yet been developed.

Certifying the readiness of the NAO without fully addressing the concerns outlined within the assessment does not provide assurance that the office is fully in compliance with civil liberties standards and will take appropriate measures to protect civil liberties.

Conclusions

DHS has taken positive steps to ensure that NAO operations will comply with applicable laws, including developing a legal review procedure for requests for classified satellite information. However, DHS has not yet fully justified that the planned operations of the NAO comply with applicable laws and standards. While the agency plans to provide an additional certification before the law enforcement domain becomes operational, the department has not provided clear definitions that show how law enforcement requests will be excluded from consideration before legal and policy issues associated with NAO support for law enforcement are resolved. Without clear definitions, DHS cannot be certain that requests related to law enforcement are being effectively and consistently excluded from consideration, and therefore runs the risk that requests may be accepted without a complete analysis of how the NAO will ensure compliance with applicable laws. In addition, procedures for developing and approving memorandums in the MASINT and ELINT categories have yet to be defined, and a specific process for monitoring the legal reviews has not yet been established. Given the sensitivity of NAO's mission, it is important that these specific procedures be documented in the program's implementing instructions. Without clarifying these details, DHS will have limited assurance that the legal review process is effectively ensuring compliance with applicable laws.

DHS has recently taken steps to address privacy standards, including fulfilling agency requirements to identify privacy risks and control mechanisms to mitigate them. However, differences between the review procedures outlined in the revised NAO PIA and those in the standard operating procedures raise questions about whether the specifics of NAO's privacy protection controls have been clearly established.

GAO
Accountability * Integrity * Reliability

Conclusions

Furthermore, DHS initially did not provide a public explanation of the privacy protections associated with planned NAO operations but has recently taken steps to do so. In response to discussions with us regarding the lack of public notice, DHS updated its publicly available information about the NAO to show its relationship with the applicable system-of-records notice, better informing the public about how personal information is to be processed, analyzed, and distributed by the NAO.

Finally, DHS also completed a CLIA that identifies and assesses civil liberties risks associated with NAO, and discusses how most of them will be mitigated. However, measures to address the potential for improper use or retention of information provided by NAO and the potential for impermissible requests to be accepted as a result of a reliance on broad annual memorandums as justifications have not yet been fully addressed. Certifying the readiness of the NAO without fully addressing these concerns does not provide assurance that it is fully in compliance with civil liberties standards and will take appropriate measures to protect civil liberties.

Recommendations

To ensure that NAO is in compliance with applicable laws, including privacy and civil liberties standards, we recommend that the Secretary of Homeland Security more fully justify the department's certification by taking the following actions:

1. Given that NAO is to operate before law enforcement issues are resolved and operations are re-certified, establish clear definitions for law enforcement and homeland security requests to better ensure that law enforcement requests will not be accepted until legal and policy issues are resolved.
2. Direct NAO to address remaining issues about its processes and procedures, including
   - defining procedures for developing and approving annual memorandums in the MASINT and ELINT categories,
   - establishing procedures for monitoring the legal review process to ensure it is achieving its objectives,
   - ensuring that specific privacy controls outlined in the revised privacy assessment are clearly established in NAO standard operating procedures, and
   - establishing specific procedures to fully address issues raised within the CLIA: the potential for improper use or retention of information provided by NAO and the potential for impermissible requests to be accepted as a result of a reliance on broad annual memorandums as justifications.

Agency Comments and Our Evaluation

In written comments provided on a draft of this briefing, the DHS Deputy Undersecretary for Mission Integration stated that the department had taken or would take steps to ensure that our recommendations are incorporated in to the functioning of the NAO.

However, with respect to our recommendation regarding the definitions of law enforcement and homeland security requests, the Deputy Undersecretary stated that the definitions outlined in the charter were sufficiently clear for the NAO to operate in an effective and lawful manner. He also noted that DHS "acknowledge[s] that overlap between these two general areas is possible," and that "to the extent overlap between domains is conceivable, communication between the NAO and the requester will provide sufficient clarity."

However, we believe that without clearer domain definitions, DHS cannot be certain that requests related to law enforcement are being effectively and consistently excluded from consideration. The Secretary's certification of compliance depends critically on the assertion that requests for law enforcement domain uses will not be accepted by the NAO until interagency agreement is reached on unresolved legal and policy issues. Because these law enforcement issues have not yet been analyzed and resolved, the NAO runs the risk that requests may be accepted without a complete analysis of how the NAO will ensure compliance with applicable laws.

Regarding our recommendation to direct NAO to address remaining issues about its processes and procedures, the Deputy Undersecretary stated that NAO is taking several steps to incorporate the recommendation, including

- working with the intelligence community to establish more detailed procedures for requesting ELINT and MASINT, which are to be patterned after the GEOINT process;
- developing a metrics program to help assess its effectiveness and maintain its customer focus;
- updating its standard operating procedures to conform to the recently revised PIA; and
- updating its internal procedures to address issues raised in the CLIA, focusing resources on educating and training NAO staff and customers, particularly with respect to the collection, use, and retention of personally identifiable information.

These actions have not yet been completed. However, we agree that completing these steps should provide DHS with better assurance that NAO's processes and procedures will be effective in ensuring the program's compliance with applicable laws, privacy and civil liberties standards.

The Deputy Undersecretary also commented that the title of the briefing was misleading because it suggested that the NAO had failed to comply with all existing laws. We disagree that the title makes such a suggestion. The purpose of our review was not to make an independent determination of compliance, but to assess the completeness of DHS' justification for certifying its compliance. Our conclusion was that additional justification was needed.

In addition, the Deputy Undersecretary stated that some of the matters addressed in our briefing were, in DHS' view, beyond the scope of what Congress authorized and that some of our recommendations point out programmatic or policy differences between GAO and DHS. Specifically, the Deputy Undersecretary stated his position that GAO's tasking was limited to reviewing legal compliance. However, our scope and methodology were established on the basis of the language within the congressional mandate, and, in addition, we reached agreement with relevant Congressional appropriations, authorization, and oversight committees on the scope of our review prior to initiating our work. Further, we based our evaluation of the Secretary's certification of compliance with privacy and civil liberties standards on the agency's own policies and standards, including the DHS version of the Fair Information Practice Principles.

Finally, the Deputy Undersecretary stated that our briefing constituted the completion of the review required by the Appropriations Act, and that the NAO is preparing to commence its operations in the civil applications and homeland security communities.

Enclosure II: Comments from the Department of Homeland Security

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

Homeland Security

August 29, 2008

Gene Dodaro
Acting Comptroller General
Of the United States
Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Dodaro,

Thank you for your thorough review of the Secretary's certification of the National Applications Office (NAO), as required by the 2008 Omnibus Appropriations Act.[1] We have carefully considered your draft recommendations and, as described below, have taken or will take steps to ensure that these recommendations are incorporated into the functioning of the NAO.

As an initial matter, I must address the title of the report: *NATIONAL APPLICATIONS OFFICE, Certification of Compliance with Legal, Privacy and Civil Liberties Standards Needs To Be More Fully Justified.* GAO's report runs sixty pages and reflects a comprehensive and thoughtful review. The recommendations discussed below are focused on discrete and technical matters—and in no way suggest that the NAO fails to "comply with [any] existing laws." The title paints a very different picture. It is our view that the title is misleading because it does not accurately reflect the substance of the report.

GAO's first recommendation is that the NAO establish a clearer definition of law enforcement activity. The NAO Charter states that the law enforcement domain includes activities conducted by law enforcement entities "to the extent they are enforcing criminal or civil laws or investigating violations thereof". The homeland security domain includes activities conducted by any agency related to "the prevention and mitigation of, preparation for, response to, and recovery from natural or man-made disasters, including terrorism, and other threats to the homeland." As we explained in our letter dated

[1] Section 525 of the 2008 Omnibus Appropriations Act provides the following:

> None of the funds provided in this Act shall be available to commence operations of the National Applications Office…until the Secretary certifies that th[is] program[ ] compl[ies] with all existing laws, including all applicable privacy and civil liberties standards, and that certification is reviewed by the Government Accountability Office.

The Classified Annex to the Act further provides:

> (U) Included in the bill is a provision that restricts obligation of any funds to commence operations of [the National Applications Office] until the Secretary of Homeland Security certifies that all statutory privacy and civil liberties requirements have been met, and submits Standard Operating Procedures for [the] program[] to the Committees on Appropriations. The bill also requires the Government Accountability Office to review the Secretary's certification.

July 30, 2008, we believe that these definitions are sufficiently clear for the NAO to operate in an effective and lawful manner. A copy of that letter is attached.

GAO's second recommendation pertains to operational processes and procedures. The NAO is taking several steps to incorporate this recommendation. First, the NAO is working with the Intelligence Community's Functional Managers to establish more detailed procedures for requesting electronic intelligence (ELINT) and measurements and signatures intelligence (MASINT), which will be patterned after the geospatial intelligence (GEOINT) community's Proper Use Memorandum (PUM) process. As with the PUM process, these procedures will enhance individual privacy and civil rights protections. Second, the NAO is developing a metrics program to help assess the NAO's effectiveness and maintain its customer focus. Among other benefits, this will allow the NAO to ensure that it is adequately safeguarding individuals' civil rights and privacy. Third, the NAO is updating its Standard Operating Procedures (SOPs) to conform to the recently revised Privacy Impact Assessment (PIA). During the review process, GAO identified several concerns with the PIA for the NAO. DHS has worked closely with the DHS Privacy Office to address these concerns and in August 2008 the Privacy Office issued a revised PIA. Finally, to address the issues raised in the Civil Liberties Impact Assessment (CLIA) for the NAO, the NAO is updating its internal procedures. It will focus resources on educating and training NAO staff and customers, particularly with respect to the collection, use and retention of Personally Identifiable Information (PII).

Notwithstanding the steps DHS has taken to incorporate GAO's recommendations, some of the matters addressed in GAO's report are, in our view, beyond the scope of what Congress authorized. GAO's task was to review the Secretary's certification, which states only that the NAO, as contemplated, satisfies all existing laws, including statutory privacy and civil liberties standards. The classified portion of the Appropriations Act clarified and narrowed the scope of this review, providing that it is to focus on whether "all statutory privacy and civil liberties requirements have been met." Yet some of GAO's recommendations point out programmatic or policy differences between it and the Department, and thus are beyond the review contemplated in the Appropriations Act.

Since GAO's report constitutes the completion of the review required by the Appropriations Act, the NAO is preparing to commence operations in the civil applications and homeland security communities.

Sincerely,

James M. Chaparro
Deputy Under Secretary for Mission Integration
Office of Intelligence and Analysis

Attachment:
Letter to GAO dated July 30, 2008