

June 2005

TRANSPORTATION
SECURITY
ADMINISTRATION

Clear Policies and
Oversight Needed for
Designation of
Sensitive Security
Information





Highlights of [GAO-GAO-05-677](#), a report to congressional requesters

Why GAO Did This Study

Concerns have arisen about whether the Transportation Security Administration (TSA) is applying the Sensitive Security Information (SSI) designation consistently and appropriately. SSI is one category of “sensitive but unclassified” information—information generally restricted from public disclosure but that is not classified. GAO determined (1) TSA’s SSI designation and removal procedures, (2) TSA’s internal control procedures in place to ensure that it consistently complies with laws and regulations governing the SSI process and oversight thereof, and (3) TSA’s training to its staff that designate SSI.

What GAO Recommends

GAO recommends that the Secretary of Homeland Security direct TSA to establish clear guidance and procedures for using the TSA regulations to determine what constitutes SSI; establish clear responsibility for the identification and designation of SSI information; establish internal controls monitoring compliance with its SSI regulations, policies, and procedures, and communicate that responsibility for implementing the controls throughout TSA; and provide specialized training to those making SSI designations on how information is to be identified and evaluated for SSI status. The Department of Homeland Security generally concurred with our recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-05-677.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Laurie E. Ekstrand at (202) 512-8777 or ekstrandl@gao.gov.

TRANSPORTATION SECURITY ADMINISTRATION

Clear Policies and Oversight Needed for Designation of Sensitive Security Information

What GAO Found

TSA does not have guidance and procedures, beyond its SSI regulations, providing criteria for determining what constitutes SSI or who can make the designation. Such guidance is required under GAO’s standards for internal controls. In addition, TSA has no policies on accounting for or tracking documents designated as SSI. As a result, TSA was unable to determine either the number of TSA employees actually designating information as SSI or the number of documents designated SSI. Further, apart from Freedom of Information Act (FOIA) requests or other requests for disclosure outside of TSA, there are no written policies and procedures or systematic reviews for determining if and when an SSI designation should be removed.

TSA also lacks adequate internal controls to provide reasonable assurance that its SSI designation process is being consistently applied across TSA. Specifically, TSA has not established and documented policies and internal control procedures for monitoring compliance with the regulations, policies, and procedures governing its SSI designation process, including ongoing monitoring of the process. TSA officials told us that its new SSI Program Office will ultimately be responsible for ensuring that staff are consistently applying SSI designations. This office, which was established in February 2005, will also develop and implement all TSA policy concerning SSI handling, training, and protection. More detailed information on how this office’s activities will be operationalized was not yet available. Specifically, TSA officials provided no written policies formalizing the office’s role, responsibilities, and authority.

TSA has not developed policies and procedures for providing specialized training for all of its employees making SSI designations on how information is identified and evaluated for protected status. Development of such training for SSI designations is needed to help ensure consistent implementation of the designation authority across TSA. While TSA has provided a training briefing on SSI regulations to certain staff, such as the FOIA staff, it does not have specialized training in place to instruct employees on how to consistently designate information as SSI. In addition, TSA has no written policies identifying who is responsible for ensuring that employees comply with SSI training requirements.

Contents

Letter		1
	Background	2
	Results	3
	Conclusions	7
	Recommendations	7
	Agency Comments and Our Evaluation	7
Appendix I	Briefing Slides	13
Appendix II	Comments from the Department of Homeland Security	52

Abbreviations

ATSA	Aviation and Transportation Security Act
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FOIA	Freedom of Information Act
SBU	Sensitive But Unclassified
SSI	Sensitive Security Information
TSA	Transportation Security Administration

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



United States Government Accountability Office
Washington, DC 20548

June 29, 2005

The Honorable David Obey
Ranking Minority Member
Committee on Appropriations
House of Representatives

The Honorable Martin Olav Sabo
Ranking Minority Member
Subcommittee on Homeland Security
Committee on Appropriations
House of Representatives

The security of our transportation system is of vital importance to the nation. In line with keeping our transportation safe, some information that is related to threats to or protection of the transportation system must be held out of the public domain. On the other hand, the government must always be mindful of the public's legitimate interest in, and need to know, information related to threats to the transportation system and associated vulnerabilities.

Sensitive Security Information (SSI) is a specific category of information related to transportation security that is deemed to require protection against public disclosure. Although it is not classified national security information, SSI is a category of sensitive but unclassified information that, along with protected critical infrastructure information, is specifically exempted by statute from release under the Freedom of Information Act (FOIA), and that it is to be disclosed only to covered persons on a need to know basis. While the Transportation Security Administration (TSA), through its SSI authority, may share SSI with regulated entities, it generally prohibits the public disclosure of information obtained or developed in the conduct of security activities, which would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential commercial or financial information, or be detrimental to the security of transportation.

Questions have been raised about TSA's practices and procedures for determining whether information should be protected as SSI. For example, certain written responses to questions submitted by TSA to the House Appropriations Homeland Security Subcommittee were designated as SSI. However, 1 month earlier, the agency had not treated this same

information as sensitive. Further, in an October 2004 memorandum, TSA itself recognized that the handling and identification of SSI had become problematic.

In response to your request concerning TSA's handling of SSI, we are reporting on (1) TSA's procedures for determining whether information should be protected under the SSI designation, as well as procedures for determining if and when the designation should be removed, (2) internal control procedures in place to ensure that TSA consistently complies with laws and regulations governing the designation of information as SSI and how TSA oversees the procedures to ensure that they are consistently applied, and (3) TSA's training to its staff who designate SSI.

To address our objectives, we reviewed applicable federal laws and regulations, Department of Homeland Security (DHS) and TSA policies and procedures, and other documents related to the SSI designation, and oversight and training processes. We also interviewed TSA and DHS officials involved in the SSI designation, oversight and training processes. GAO's *Standards for Internal Control in the Federal Government* provided benchmarks and standards against which we assessed TSA's SSI designation policies and procedures.¹ Our work was conducted from January 2005 through April 2005 in accordance with generally accepted government auditing standards.

On April 29, 2005, we provided your offices a briefing on the results of our work. The briefing slides are included in appendix I.

Background

In the aftermath of the terrorist attacks of September 11, 2001, TSA was created to take responsibility for the security of all modes of public transportation. Included in the responsibilities of this new agency was the authority to designate information as SSI. Originally housed in the Department of Transportation, TSA was transferred to DHS as a result of the Homeland Security Act of 2002.²

¹GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: November 1999).

²The Homeland Security Act of 2002 established 49 U.S.C. § 114(s) as TSA's SSI authority. TSA codified its SSI regulations at 49 C.F.R. part 1520.

According to TSA officials, SSI designated information is created by TSA and by airports, aircraft operators, and other regulated parties when they are establishing or implementing security programs or documentation to address security requirements. Information that is designated SSI can be shared with those who have a need to know in order to participate in or oversee the protection of the nation's transportation system. Those with a need to know can include persons outside of TSA, such as airport operators, aircraft operators, foreign vessel owners, and other persons. SSI cannot be shared with the general public, and it is exempt from disclosure under FOIA.

There are 16 categories of SSI. TSA has distinguished these 16 categories into 3 types of SSI. Four categories are termed "categorical" and automatically designated SSI. Eleven categories require a judgment or analysis to determine if the SSI designation is warranted. One category requires a written determination by an office with determination authority to be deemed SSI. This category is "other information," which is a catchall exemption for information that TSA may wish to designate SSI that does not fit into the other 15 categories.³

Additional background information on the SSI regulatory authority, including a list of the 16 categories, is included in appendix I.

Results

TSA does not have written policies and procedures, beyond its SSI regulations, providing criteria for determining what constitutes SSI. Written guidance for decision making such as this is a key element included in GAO's *Standards for Internal Control in the Federal Government*. Lack of such guidance could result in errors and inconsistencies in determining the SSI designation. Indeed, in October 2004, TSA's Internal Security Policy Board concluded that TSA must establish a framework to identify, control, and protect SSI. The board concluded that essential elements of the framework should include, among other things,

"... exacting specificity with respect to what information is covered and what is not covered. This specificity could be documented in a classification guide type format because imprecision in this area causes a significant impediment to determining SSI. Experience

³A subset of one of the judgment categories, 49 C.F.R. § 1520.5(9)(iii), also falls within this determination category.

has shown that employees unsure as to what constitutes SSI may err on the side of caution and improperly and unnecessarily restrict information, or may err inappropriately and potentially disastrously on the side of public disclosure.”

In addition to lacking written guidance concerning SSI designation, TSA has no policies and procedures specifying clear responsibilities for officials who can designate SSI.⁴ TSA’s regulations allow anyone within TSA to designate information SSI. Further, TSA has no policies on accounting for or tracking documents designated as SSI. While TSA officials told us that only a limited number of employees routinely make SSI designations, they were unable to provide documentation to confirm this. One consequence of a lack of control of personnel able to designate documents as SSI is that TSA is unable to determine the number of employees designating information as SSI or the volume of documents designated SSI.

Once a document is designated SSI, it can remain designated as SSI in perpetuity unless a FOIA request or other request for disclosure outside of TSA results in removal of its SSI status. If a FOIA request is received for an SSI designated document, or a document that contains some SSI designated material, the SSI Program Office works in conjunction with the FOIA Office to review its initial designation. If TSA officials determine that the document should no longer be considered SSI, it can be released to the FOIA requester. If TSA officials feel that the SSI designation should remain but some portions of the document are not SSI, the FOIA Office can determine whether it is appropriate to release the document without the SSI material, or not to release the document at all.⁵ Other than the FOIA process, no procedures exist for the review of allegations that a document has been erroneously designated as SSI. If there is no FOIA request for a particular document, according to TSA, documents marked as SSI are reviewed for continued applicability upon any request for disclosure outside of TSA. However, TSA officials provided us with no information

⁴TSA identified two categories of information—§§ 1520.5(b)(9)(iii) and 1520.5(b)(16)—that require a written determination by an office with determination authority to be designated SSI.

⁵ According to a TSA official, TSA processed 99 FOIA requests involving or related to SSI in 2003 and 129 requests in 2004. The TSA official said that, of the total requests processed in 2003, no requests were granted in whole, 63 requests were granted in part, and 36 requests were denied in full. The official also said that, of those 129 requests processed in 2004, no requests were granted in whole, 92 requests were granted in part, and 37 requests were denied in full.

on the number of documents released as a result of these requests for public disclosure. TSA's SSI regulations indicate that TSA may determine in writing that information should no longer be designated as SSI because it no longer meets SSI criteria, but TSA has not done this to date.

TSA lacks adequate internal controls to provide reasonable assurance that its SSI designation process is being consistently applied across TSA and for monitoring compliance with the regulations governing the SSI designation process, including ongoing monitoring of the process. GAO's Standards for Internal Control call for (1) areas of authority and responsibility to be clearly defined and appropriate lines of reporting established, (2) transactions and other significant events to be documented clearly and documentation to be readily available for examination, and (3) controls generally to be designed to ensure that ongoing monitoring occurs in the course of normal operations. In addition, the standards also require that information be communicated within an organization to enable individuals to carry out their internal control responsibilities. However, our review of TSA's oversight activities noted weaknesses in each of these areas.

First, TSA has not clearly defined responsibility for monitoring compliance with regulations, policies and procedures governing the SSI designation process and communicated that responsibility throughout TSA. Without clearly identifying the responsibility for monitoring compliance with regulations governing its SSI designation, this function may not receive adequate attention, leaving TSA unable to provide reasonable assurance that those making SSI designations within TSA are designating documents properly.

In an October 14, 2004, memorandum designed to centralize the administration of SSI within the agency, TSA's Internal Security Policy Board recognized that the handling and identification of SSI had become problematic:

"Lacking a central policy program office for SSI has led to confusion and unnecessary classification of some materials as SSI. Adherence to handling requirements within TSA has been inconsistent, and there have been instances where SSI has been mishandled outside of TSA. Identification of SSI has often appeared to be ad-hoc, marked by confusion and disagreement depending on the viewpoint, experience, and training of the identifier. Strictures on the release of SSI and other SSI policy or handling-related problems have occasionally frustrated industry stakeholders, Congress, the media, and our own employees trying to work within the confines of the restrictions. Significant time and effort

has been devoted to SSI issues, and it is not likely that the current approach to addressing such issues can be sustained.”

TSA officials told us that its new SSI Program Office will ultimately be responsible for ensuring that staff are consistently applying SSI designations. This office, which was established in February 2005, will also develop and implement all TSA policies concerning SSI handling, training, and protection. Officials said that TSA is also currently drafting a summary that provides a definition and brief overview of the SSI authority and is designing materials that will further educate all TSA employees on policies, procedures, responsibilities, and guidance for identifying and designating SSI. More detailed information on how this office’s activities will be operationalized was not yet available. Specifically, TSA currently does not have written policies formalizing the office’s role, responsibilities, and authority.

Second, TSA has not yet established policies and procedures for how it will monitor compliance with the regulations governing the SSI designation process. Without written policies and procedures documenting how it plans to monitor compliance with the regulations governing the SSI designation process, TSA is unable to demonstrate evidence of its monitoring activities.

Third, TSA has no formally defined policies or procedures for ongoing monitoring reviews to assess compliance with the laws and regulations governing the process for designating information as SSI. Without clearly defined policies and procedures for conducting periodic internal monitoring to assess compliance with the regulations governing the SSI designation process, TSA lacks structure to support continuous assurance that those employees making SSI designations within TSA are designating documents properly.

TSA has not developed policies and procedures for providing specialized training for all of its employees making SSI designations on how information is to be identified and evaluated for protected status. Development of specialized training for SSI designations must be preceded by the establishment of guidance and associated policies and procedures so that an adequate training curriculum can be developed. It should also include written policies defining who is responsible for ensuring that employees comply with SSI training requirements. While TSA has provided a training briefing on SSI regulations to certain staff such as the FOIA staff and other units within TSA, it does not have specialized training in place to instruct employees on how to consistently designate information as SSI.

Conclusions

In order for TSA's SSI designation process to work effectively, there must be clarity, structure, and accountability to help ensure that information is not improperly and unnecessarily restricted or inappropriately disclosed, and that the SSI designation process is being applied consistently across TSA. The lack of clear and documented policies and procedures for determining what constitutes SSI and specifying who may make the designation could cause confusion and uncertainty for staff who must administer the SSI designation process without written guidance. Further, internal control policies and procedures for monitoring the compliance with regulations governing the SSI designation process, including internal controls for ongoing monitoring, communicated to all staff, would help ensure accountability and consistency in the implementation of TSA's SSI regulations. Specialized training designed to familiarize those who are making SSI designations on how information is to be identified and evaluated would reduce the likelihood that employees improperly exempt information from public disclosure or inappropriately disclose sensitive security information.

Recommendations

To help bring clarity, structure, and accountability to TSA's SSI designation process, we recommend that the Secretary of the Department of Homeland Security direct the Administrator of the Transportation Security Administration to take the following four actions

- establish clear guidance and procedures for using the TSA regulations to determine what constitutes SSI,
- establish clear responsibility for the identification and designation of information that warrants SSI protection,
- establish internal controls that clearly define responsibility for monitoring compliance with regulations, policies, and procedures governing the SSI designation process and communicate that responsibility throughout TSA, and
- establish policies and procedures within TSA for providing specialized training to those making SSI designations on how information is to be identified and evaluated for protected status.

Agency Comments and Our Evaluation

We obtained written comments on a draft of this report from the Department of Homeland Security. We have included a copy of the

comments in their entirety in appendix II. In addition, DHS provided technical comments, which we incorporated as appropriate.

In its June 14, 2005, comments, DHS generally concurred with our recommendations and stated that they are consistent with ongoing TSA efforts to improve sensitive security information program processes. In its comments, DHS discussed the actions it has already taken and will implement in response to the recommendations, including developing internal controls and audit functions, which will define responsibility for monitoring compliance with regulations, policies, and procedures governing the SSI designation process, and which will be communicated throughout TSA. However, as discussed below, DHS took exception to the report's analyses and conclusions. While we disagree with the thrust of DHS's comments, we believe we fairly and accurately characterize the implementation and monitoring of SSI at DHS. We made clarifying changes where appropriate.

DHS said that our report mischaracterized the nature of SSI by incorrectly applying concepts associated with classified information management to SSI information, which falls within a sensitive but unclassified information category. DHS said that this construct may lead the reader to fundamental misunderstandings regarding the issues surrounding SSI. Although mentioned as a basis for comparison, neither the GAO review nor its report was intended to apply concepts associated with classified information management to SSI. Rather, our analyses were intended to provide a factual summary of the key similarities and differences in the classified information and SSI processes. We compare the two processes only to help clarify the distinctions that exist and thereby avoid any misunderstandings by readers who are familiar with the processes for classified information. We included additional language in the report clarifying that SSI is a form of sensitive but unclassified information, rather than classified national security information.

DHS also stated that SSI is the only practical means for sharing security information with regulated parties and that the absence of a robust SSI program would degrade both the prompt distribution of security information to persons with a need to know and the free exchange of ideas. We agree that SSI is a practical means for sharing security information with regulated parties. In fact, the findings and recommendations in this report should help DHS improve the SSI process. That is, providing specific procedures and guidelines on how individual employees are to identify and evaluate information for SSI protected status is an intrinsic part of DHS's responsibility for effectively managing

its SSI process and should provide both DHS and the regulated parties with confidence that information is given the proper protective status.

DHS said that if a TSA employee incorrectly designates a document as SSI while it remains within TSA, there is no impact on the public's right to access because the FOIA review process will always result in an independent determination regarding the SSI designation and that TSA and DHS are committed to releasing as much information as possible. We view the management improvements discussed in this report as helping to ensure that information that should be withheld from the public is protected as well as helping to ensure that other information is available to the public. In addition, the fact that an incorrectly designated SSI document remains within TSA does not obviate the fact it is wrongfully exempted from disclosure. The potential lack of visibility to the public that SSI documents exist and the time and expense to the public and TSA involved in seeking disclosure of an SSI document through FOIA could inhibit the release of information that could and possibly should have been in the public domain but for an incorrect application of SSI.

DHS also states that we make no distinction between the obligation to "mark" information as SSI, held by all TSA employees, and the authority to "designate," held by only a very few high-level employees. It explains that all employees can "mark" documents that fall within 15 categories as SSI but only the high-level employees can "designate" the 16th category of "other information" by documenting the designation as SSI. As we point out in this report, the responsibility of all TSA employees goes beyond just marking a document as SSI and includes making judgments about what information should be marked as SSI. As we state on page 3, while TSA requires a written determination by an office with determination authority for information deemed SSI for 1 of its 16 SSI categories, according to TSA, only 4 of the remaining 15 categories automatically becomes SSI because of the type of document. The other 11 require a judgment or analysis to be made to determine if the SSI designation is warranted by any TSA employee. Therefore, we continue to believe that appropriate guidance and controls are needed to effectively manage the process.

In addition, DHS said that its SSI designation processes are consistent with every sensitive but unclassified system in the federal government. While we did not review these other systems, we believe that the management principles and controls discussed in this report are appropriate for the TSA system and would be appropriate for similar systems elsewhere.

DHS said that we made an implied suggestion to quantify and identify all documents that have been marked as SSI, and to identify all personnel who have marked such documents. We did note in our discussion of internal controls that TSA has no policies on accounting for or tracking documents designated as SSI. As DHS notes, we did not recommend that TSA provide an inventory of the titles or numbers of SSI documents. In terms of identifying staff that designate documents as SSI, since we are recommending training for all those who designate SSI, identification of all personnel who are going to be applying this designation would be needed to ensure that all are trained.

Further, DHS states that we obliquely criticize TSA's ability to protect SSI without a date by which the document automatically loses its SSI status based on time duration requirements similar to those applicable to classified information. We did not recommend that TSA should implement time limits for SSI information. Our review showed that TSA has no written policies and procedures or systematic reviews for determining if and when an SSI designation should be removed. Moreover, other than the FOIA request process and other requests for disclosure outside of TSA, no procedures exist for a review to determine whether a document has been appropriately designated as SSI. Such procedures would allow TSA to periodically review SSI designations and identify and correct erroneously marked SSI documents while still protecting those with valid reasons.

In commenting on our recommendation that DHS establish clear guidance and procedures for using the TSA regulations to determine what constitutes SSI, DHS said that TSA's SSI Program Office has already taken some steps in line with our recommendation by developing internal guidance that expands on the SSI regulation structure to provide examples of the types of information that should fall within each SSI category. It expects to publish the guidance for general use by TSA employees and regulated parties in identifying and handling SSI.

In commenting on our recommendation that DHS establish clear responsibility for the identification and designation of information that warrants SSI protection, DHS stated that limiting the number of individuals who may designate a document as SSI would lead to operational bottlenecks, could lead to inappropriate release of security information, and would not be operationally feasible. If it is properly done, we do not see how establishing clear responsibility for performing a governmental task would lead to these effects. We wish to make a distinction between a set of personnel who would have responsibility for SSI and a potentially much larger set of employees who would be able to

designate documents SSI. Those responsible for SSI would be accountable for ensuring that those in their domain of responsibility have appropriate training and are applying SSI appropriately. DHS would then be in a much better position to ensure that those responsible for SSI are held accountable, have appropriate training, and are applying SSI appropriately.

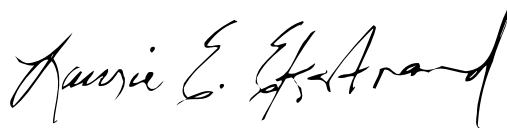
DHS agreed with our recommendation for DHS to establish internal controls that clearly define responsibility for monitoring compliance with regulations, policies, and procedures governing the SSI designation process and communicate that responsibility throughout TSA. DHS said it had already undertaken action to develop internal controls, including audit functions, which will define responsibility for monitoring compliance with regulations, policies, and procedures governing the SSI designation process and will communicate that responsibility throughout TSA.

In commenting on our recommendation that DHS establish policies and procedures within TSA for providing specialized training to those making SSI designations on how information is to be identified and evaluated for protected status, DHS said that it conducts specialized SSI training for the SSI Program Office and FOIA staff, and other TSA offices making SSI designations. In addition, it is expanding specialized training to those offices within the agency that create the majority of SSI. This is a good first step in addressing our recommendation, but falls short of its overall intent because SSI regulations extend the SSI designation authority to all TSA employees and does so without giving them specific procedures and guidance, beyond the regulations, upon which to base their judgments. Thus, policies and procedures for providing specialized training to all TSA employees authorized to make an SSI designation will still be needed. In this regard, in our report, we quote an October 14, 2004, TSA memorandum that says in part, “identification of SSI has often appeared to be ad-hoc, marked by confusion and disagreement depending on the viewpoint, experience, and training of the identifier.” We believe this statement speaks to the need for specialized training for all those who designate materials as SSI.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to other interested congressional committees and to the Secretary of the Department of Homeland Security and the Administrator of the Transportation Security Administration. We will also make copies

available to others upon request. In addition, the report will be available at no charge on GAO's Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-8777 or EkstrandL@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report were Glenn G. Davis, Vickie Miller, R. Rochelle Burns, Julian King, Thomas Lombardi, David Hooper, David Plocher, Dolores McGhee, Nikki Clowers, Kim Gianopoulos, David D'Agostino, Ann Borseth, William Cawood, Casey Keplinger, David Alexander, Katherine Davis, and Larry Harrell.



Laurie E. Ekstrand, Director
Homeland Security and Justice Issues

Appendix I: Briefing Slides



Transportation Security Administration's Designation Process and Oversight of Sensitive Security Information

**Interim Briefing to the
House Committee on Appropriations
April 29, 2005**

1



Objectives

Our objectives were to assess:

1. the Transportation Security Administration's (TSA) procedures for determining whether information should be protected under the Sensitive Security Information (SSI) designation, as well as procedures for determining if and when the designation should be removed;
 2. internal control procedures in place to ensure that TSA consistently complies with laws and regulations governing the designation of information as SSI and how TSA oversees the process to ensure that it is consistently applied; and
 3. TSA's policies and procedures for providing training to its staff who designate SSI.
-



Scope and Methodology

- To address the objectives, we:
 - reviewed applicable federal laws and regulations, Department of Homeland Security (DHS) and TSA policies and procedures, and other documents related to the SSI designation and oversight process, and
 - interviewed TSA and DHS officials involved in the SSI designation and oversight process.



Scope and Methodology (continued)

- Our review focused on TSA, which governs the administration of the SSI authority, and did not include the Department of Transportation (DOT), which also has statutory authority to use the designation.¹
- We reviewed and used as criteria, our *Standards for Internal Control in the Federal Government*.² The Comptroller General issued these standards to provide guidance to agencies to help them assess, evaluate, and implement effective internal controls that can be helpful in improving their operational processes, which would include the SSI designation process.

¹49 U.S.C. § 40119(b) and 49 C.F.R. part 15.

²GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).



Background

- After the terrorist attacks of September 11, 2001, the Aviation and Transportation Security Act (ATSA) was enacted on November 19, 2001, with the primary goal of strengthening the security of the nation's aviation system.
- ATSA created TSA as the agency responsible for securing all modes of transportation and transferred most civil aviation security responsibilities, including SSI authority, from the Federal Aviation Administration (FAA) to TSA.
- The Homeland Security Act of 2002 transferred TSA from DOT to DHS and established 49 U.S.C. § 114(s) as TSA's SSI authority.
- TSA codified its SSI regulations at 49 C.F.R. part 1520.



Background (continued)

- SSI constitutes one category of “Sensitive But Unclassified” (SBU) information—information generally restricted from public disclosure but that is not classified national security information.³
 - SSI is an SBU category specifically required by statute (other examples include Protected Critical Infrastructure Information and Privacy Act information).
 - Categories of SBU information not specifically mandated by statute include For Official Use Only and Law Enforcement Sensitive information.
- The Freedom of Information Act (FOIA) is the primary process for releasing (and for prohibiting the release of) SBU information to the public, as appropriate. SSI, by Statute, is exempt from disclosure under FOIA.

³Attachment I, contained in appendix I, illustrates differences between information designated SSI by TSA and classified national security information.



Background (continued)

- TSA, through its SSI authority, prohibits the public disclosure of information obtained or developed in the conduct of security activities that, for example, would be detrimental to transportation security.
- According to TSA, SSI is created by TSA and by airports, aircraft operators, and other regulated parties when they are establishing or implementing security programs or documentation to address security requirements.
- According to TSA, safeguarding information as SSI allows controlled information sharing with stakeholders to meet TSA's mission to protect the nation's transportation systems.
- SSI regulations allow for the sharing of SSI with covered persons (as defined in 49 C.F.R. § 1520.7) having a need to know—including airport operators, aircraft operators, foreign vessel owners, TSA employees, and other persons.



Background (continued)

- SSI falls into 1 (or more) of 16 categories, which TSA has divided into three types: categorical (automatically SSI), judgment (requires a judgment or analysis), and determination (requires written determination by an office with determination authority).⁴
- Additional background information on the SSI regulatory authority, including a list of the 16 categories, is included in attachment I, contained in appendix I.

⁴According to TSA officials, TSA determination authority only applies to SSI designated pursuant to 49 C.F.R. § 1520.5(b)(9)(iii), (16), and 1520.5(c).



Background (continued)

- Congressional concern has arisen about whether TSA is applying the designation criteria consistently and appropriately.
 - For example, certain written responses to questions submitted by TSA to the House Appropriations Homeland Security Subcommittee were designated as SSI. However, 1 month earlier, the agency had not treated this same information as sensitive.



Background (continued)

- In an October 14, 2004, memorandum designed to centralize the administration of SSI within the agency, TSA's Internal Security Policy Board⁵ recognized that the handling and identification of SSI had become problematic:
 - "Lacking a central policy program office for SSI has led to confusion and unnecessary classification of some materials as SSI. Adherence to handling requirements within TSA has been inconsistent, and there have been instances where SSI has been mishandled outside of TSA. Identification of SSI has often appeared to be ad-hoc, marked by confusion and disagreement depending on the viewpoint, experience, and training of the identifier. Strictures on the release of SSI and other SSI policy or handling-related problems have occasionally frustrated industry stakeholders, Congress, the media, and our own employees trying to work within the confines of the restrictions. Significant time and effort has been devoted to SSI issues, and it is not likely that the current approach to addressing such issues can be sustained."

⁵The board was established to oversee the coordination of multidisciplinary security activity and ensure that TSA maintains an acceptable level of security for its internal security programs, personnel, and facilities.



Results in Brief

- Lack of Clear Policies and Procedures for SSI Designations
 - TSA personnel make SSI designations based on SSI regulations. However, beyond these regulations, TSA does not have clear policies and procedures for determining what constitutes SSI, who can make the designation, or when an SSI designation should be removed.
 - Although TSA officials said that they believe that the number of staff making SSI designations is limited, TSA was unable to provide reasonable assurance of this because the number of staff designating information as SSI is not being tracked and is unknown to TSA.
-



Results in Brief (continued)

- Monitoring Controls Are Weak
 - TSA has not established and documented policies and internal control procedures for monitoring compliance with the regulations governing its SSI designation process.
 - Without clearly identifying responsibility for monitoring its SSI designation process, TSA is unable to provide reasonable assurance that the designation is being consistently applied across TSA.
-



Results in Brief (continued)

- SSI Training Policies and Procedures Are Insufficient
 - TSA does not have polices and procedures to provide reasonable assurance that those employees making SSI designations within TSA have received specialized training on how information is identified and evaluated for SSI status.



Objective 1—SSI Designation and Removal Process

- TSA does not have clear policies and procedures, beyond the SSI regulations, to provide to its employees for determining what constitutes SSI or who can make the designation.
 - The SSI regulations list 16 categories of information (see attachment I, contained in appendix I) that must be safeguarded as SSI. However, we found no written criteria beyond the regulations to guide those who must decide which items of information within these categories are appropriate for designation.
 - TSA officials said that additional guidance is under development.



Objective 1—SSI Designation and Removal Process (continued)

- TSA has acknowledged the need for greater clarity in the designation process--when to designate, when not to designate.
- In October 2004, TSA's Internal Security Policy Board concluded that TSA must establish a framework through a centralized policy program office for the identification, control, and protection of SSI that includes:
 - "... exacting specificity with respect to what information is covered and what is not covered. This specificity could be documented in a classification guide type format because imprecision in this area causes a significant impediment to determining SSI. Experience has shown that employees unsure as to what constitutes SSI may err on the side of caution and improperly and unnecessarily restrict information, or may err inappropriately and potentially disastrously on the side of public disclosure."



Objective 1—SSI Designation and Removal Process (continued)

- To provide some specificity with respect to what information is SSI and what is not, TSA has developed a training briefing on SSI regulations for certain staff such as the FOIA staff and other units within TSA.
- In accordance with GAO's internal control standards,⁶ those employees involved in designating information SSI should have written criteria or standards, beyond the regulations, upon which to base their judgments, and these standards should be consistent across TSA. In the case of SSI, TSA considers the SSI regulations to be the primary written criteria.

⁶GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).



Objective 1—SSI Designation and Removal Process (continued)

- Unlike original classification authorities for classified national security information, TSA has no policies and procedures limiting the number of persons who can designate information as SSI.
 - TSA’s SSI statute required the TSA Administrator to develop regulations governing the designation of SSI.
 - The SSI regulations require any covered person, which includes all TSA employees, to designate and protect appropriate information as SSI.
 - While the SSI regulations require all TSA employees to designate information SSI when appropriate, TSA officials told us that only a limited number of employees routinely designate information as SSI, and they provided a draft chart showing the organizational elements and program offices that most frequently designate information as SSI. However, they were unable to provide us documentation on the number of employees to support this assertion.



Objective 1—SSI Designation and Removal Process (continued)

- TSA has no policies on accounting for or tracking documents designated as SSI. TSA officials were unable to determine either the number of TSA employees actually designating information as SSI or the number of documents designated SSI.
 - TSA officials said that they estimate that about 15 of the 35 headquarters offices routinely encounter material that they designate as SSI.



Objective 1—SSI Designation and Removal Process (continued)

- There are no written policies and procedures or systematic reviews for determining if and when an SSI designation should be removed. Moreover, other than the FOIA request process and other requests for disclosure outside of TSA, no procedures exist for the review of allegations that a document has been erroneously designated as SSI.
- According to TSA officials, as a standard practice, all public requests are managed through the agency’s administration of FOIA. However, the only review that information with an SSI designation gets is one performed by its FOIA Office, in conjunction with the TSA SSI Program Office, after a request for this information has been submitted.



Objective 1— SSI Designation and Removal Process (continued)

- There is no provision providing a time frame for review or removal of an SSI designation.
 - If there is no FOIA request for a particular document, according to TSA, all documents marked as SSI are reviewed for continued applicability upon any request for disclosure outside of TSA.
 - SSI designations could remain in effect indefinitely without any further review.
- TSA officials said if someone makes a FOIA request for non-SSI information that is contained in an SSI record, the non-SSI information must be released if it is practical to extract the information.⁷
 - If it is not practical to extract the non-SSI information, the entire document will be withheld. In all cases, no SSI is to be released.

⁷According to a TSA official, TSA processed 99 FOIA requests involving or related to SSI in 2003 and 129 requests in 2004. The TSA official said that of the total requests processed in 2003, no requests were granted in whole, 63 requests were granted in part, and 36 requests were denied in full. The official also said that of those 129 requests processed in 2004, no requests were granted in whole, 92 requests were granted in part, and 37 requests were denied in full.



Objective 1—SSI Designation and Removal Process (continued)

- Under TSA’s SSI regulation, TSA may determine in writing that information or records do not constitute SSI because they no longer meet criteria in its SSI regulation, but this rule has not been invoked to date, according to TSA officials.



Objective 2—Monitoring Controls Are Weak

- TSA has neither established nor documented policies and internal control procedures for monitoring internal compliance with the laws and regulations governing its SSI designation process.
 - GAO's Standards for Internal Control call for
 - (1) areas of authority and responsibility to be clearly defined and appropriate lines of reporting established,
 - (2) transactions and other significant events to be documented clearly and documentation to be readily available for examination, and
 - (3) controls generally to be designed to ensure that ongoing monitoring occurs in the course of normal operations.
-



Objective 2—Monitoring Controls Are Weak (continued)

- However, our review of TSA’s oversight activities noted weaknesses in each of these areas:
- First, TSA officials told us that the new SSI Program Office will ultimately be responsible for ensuring that staff are consistently applying SSI designations. However, TSA currently does not have written policies formalizing the office’s role, responsibilities, and authority.
 - Without clearly identifying the responsibility for monitoring compliance with regulations governing its SSI designation, this function may not receive adequate attention, leaving TSA unable to provide reasonable assurance that those making SSI designations within TSA are designating documents properly.



Objective 2—Monitoring Controls Are Weak (continued)

- Second, TSA officials were unable to produce documentation of policies and procedures for conducting monitoring activities.
- Third, TSA officials were unable to provide any formal policy for conducting periodic internal monitoring activities to assess compliance with the laws and regulations governing the process for designating information as SSI.



Objective 2—Monitoring Controls Are Weak (continued)

- While TSA officials acknowledged that TSA has not yet established and documented policies and internal control procedures for monitoring compliance with regulations governing its SSI designation process, they said that those staff designating information as SSI are experienced in their application of the regulations.



Objective 2—Monitoring Controls Are Weak (continued)

- TSA implemented a new organizational structure in February 2005 and established the Sensitive Security Information (SSI) Program Office,⁸ within the Office of the Chief of Staff, to develop and implement all TSA policy with regard to SSI handling, training, and protection.
 - The SSI Program Office is currently developing a guide for handling SSI material. Additionally, it is drafting a summary that provides a definition and brief overview of the SSI authority. More detailed information on how this office’s activities will be operationalized was not yet available.
 - Specifically, no policies and procedures exist defining this office’s responsibilities for monitoring compliance with the regulations governing TSA’s SSI designation process.

⁸According to a TSA official, three full-time-equivalent (FTE) government positions have been allocated to the SSI Program Office. Of those three FTE positions, TSA officials said that two are filled. In addition to filling these FTE positions, TSA officials said that they hired seven contractors to review documents for SSI designation and determination and are pursuing options for detailing additional staff on an as needed basis.



Objective 2—Monitoring Controls Are Weak (continued)

- Since there are no written policies and procedures for conducting monitoring activities of its SSI designation process, we asked TSA officials what monitoring expectations they had and how they would be communicated to staff.
 - A TSA official told us that, among other things, the SSI Program Office has future plans to establish points of contact in each TSA program office to coordinate handling of SSI.
 - Because written documentation was not available on these future plans at the time of our review, we were not able to assess these efforts in addressing TSA's internal control issues.
-



Objective 3—SSI Training Policies and Procedures Are Insufficient

- While TSA employees receive training on how to safeguard and protect SSI information,⁹ TSA does not have policies and procedures to provide reasonable assurance that those employees designating information as SSI within TSA have received specialized training on how information is identified and evaluated for protected status. The absence of such training increases the risk of improperly designated SSI information. Moreover, TSA has no written policies identifying who is responsible for ensuring that employees comply with the SSI training requirements.
 - TSA has not effectively implemented a training program to instruct employees how to consistently designate information as SSI.
 - TSA officials said that they have developed a training briefing on SSI regulations for certain staff such as the FOIA staff and units within TSA.

⁹According to training statistics provided by TSA, 85 percent of its employees and contractors have successfully completed SSI awareness training. Completion of SSI awareness training is required within the first 30 days at the agency and the requirement is a one time training for employees.



Attachment I: Key Rulemakings Involving Sensitive Security Information (SSI) Authority

- December 1976: Federal Aviation Administration (FAA) prohibited the disclosure of security information in order to protect against acts of criminal violence and aircraft piracy.
- March 1997: FAA issued a final rule strengthening its existing rules protecting sensitive security information from unauthorized disclosure.
- February 2002: In accordance with the Aviation and Transportation Security Act, TSA issued a rule that implemented the transfer of the majority of FAA's security-related responsibilities, including the SSI authority, to TSA, clarified aviation-related SSI, and expanded SSI to encompass security information for other modes of transportation.
- May 2004: TSA revised its SSI regulations, expanding the existing framework to also govern information related to maritime security, in accordance with the Maritime Transportation Security Act, and clarifying pre-existing SSI provisions.



Attachment I: SSI Definition

- In general, TSA’s statute and implementing regulations prohibit the disclosure of information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA had determined would:
 - (1) constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);
 - (2) reveal trade secrets or privileged or confidential information obtained from any persons; or
 - (3) be detrimental to the security of transportation.¹⁰

¹⁰ U.S.C. § 114(s) and 49 C.F.R. § 1520.5(a).



Attachment I: Disclosure of SSI

- SSI can be disclosed or otherwise provided only to covered persons who have a need to know, unless disclosure is authorized in writing by TSA, the Coast Guard, or the Secretary of DOT.¹¹
- These covered persons include airport operators, aircraft operators, foreign vessel owners, indirect air carriers, DHS employees, and other persons who receive SSI.

¹¹TSA officials said that the Department of Homeland Security's Science and Technology Directorate and Office of Federal Air Marshal Service also use the SSI designation.



Attachment I: Disclosure of SSI (continued)

- TSA must provide SSI information to congressional committees authorized to have the information and the Government Accountability Office in conducting its congressionally requested work.
- SSI is exempt from disclosure under FOIA.



Attachment I: DHS Components Using SSI

- TSA
 - governs SSI authority at DHS.

 - US Coast Guard
 - has authority to designate information as SSI and seeks TSA's guidance as appropriate.

 - In addition to TSA and the US Coast Guard, TSA officials said that the following DHS components use the SSI designation:
 - U.S. Immigration and Customs Enforcement
 - Office of Federal Air Marshal Service

 - Science and Technology Directorate
-



Attachment I: General Comparison of SSI and Classified National Security Information

SSI

- Used only for information related to transportation security.
- Does not distinguish between risk levels of information.
- Does not set time limits for removing designation and release, and disclosure restrictions remain in force until revoked by TSA, the US Coast Guard, or DOT (e.g., after review for a FOIA request).
- Does not need security clearance.
- Covered persons, including anyone within TSA, must designate and protect appropriate information as SSI.
- TSA provides no written guidance, beyond the SSI regulations, for designating information SSI.

Classified

- Used for national security and defense, intelligence, and foreign relations.
- Protected generally at one of three risk levels—top secret, secret, and confidential.
- Sets specific date for declassification of protected national security information or, if no date, then 10-year limit.
- Does need a security clearance.
- Only individuals specifically authorized in writing may possess original classification authority.
- Agencies required to prepare a classification guide.



Attachment I: 16 Categories of SSI as Established by 49 C.F.R. § 1520.5(b)

1. Security programs and contingency plans
2. Security Directives
3. Information Circulars
4. Performance specifications
5. Vulnerability assessments
6. Security inspection or investigative information
7. Threat information
8. Security measures
9. Security screening information
10. Security training materials
11. Identifying information of certain transportation security personnel
12. Critical aviation or maritime infrastructure asset information
13. Systems security information
14. Confidential business information
15. Research and development
16. Other information determined to be SSI in accordance with the Statute



Attachment I: Types of SSI as Described by TSA

- TSA officials said that they find it useful to distinguish three types of SSI: categorical, judgment, and determination.
- Categorical material is automatically designated SSI as defined by the regulations, and includes
 - Security programs and contingency plans (1),¹²
 - Security Directives (2),
 - Information Circulars (3), and
 - Identifying information of certain transportation security personnel (11).

¹²Numbers correspond to the categories listed on slide 35.



Attachment I: Types of SSI as Described by TSA (continued)

- Judgment SSI requires a judgment or analysis, and includes
 - Performance specifications (4),¹³
 - Vulnerability assessments (5),
 - Security inspection or investigative information (6),
 - Threat information (7),
 - Security measures (8),
 - Security screening information (9)(i-ii),(iv, v, and vi),¹⁴
 - Security training materials (10),
 - Critical aviation or maritime infrastructure asset information (12),
 - Systems security information (13),
 - Confidential business information (14), and
 - Research and development (15).

¹³Numbers correspond to the categories listed on slide 35.

¹⁴According to TSA officials, category (9)(iii) is a determination type of SSI (requires written determination by an office with determination authority), since it states in the regulation that information may be protected under (9)(iii) "only if determined by TSA to be SSI."



Attachment I: Types of SSI as Described by TSA (continued)

- Determination material requires written determination by an office with determination authority for:
 - Security screening information (9)(iii)¹⁵, “Detailed information about the locations at which particular screening methods or equipment are used, only if determined by TSA to be SSI,” and
 - Other information (16) is a catchall exemption that TSA may use if the Administrator (or specific delegees) determines that information not otherwise captured in categories (1)–(15) should be withheld from public disclosure.

¹⁵Numbers correspond to those categories on slide 35.



Attachment I: Types of SSI as Described by TSA (continued)

- Category (16), other information, is handled differently by TSA. According to TSA officials:
 - The category has been used very rarely.
 - Only a small number of senior TSA officials with delegated authority from the TSA Administrator may designate material as in this category.
 - Such material must be documented with a determination memorandum.
 - Determination memorandums are not prepared for the other 15 SSI designation categories.

Appendix II: Comments from the Department of Homeland Security

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



**Homeland
Security**

June 14, 2005

Ms. Laurie E. Ekstrand
Director, Homeland Security and Justice Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Ms. Ekstrand:

RE: Draft Report GAO 05-677, Transportation Security Administration: Clear Policies and Oversight Needed for Designation of Sensitive Security Information (Job Code 440363)

Thank you for the opportunity to review and comment on the subject draft report. The Department of Homeland Security (DHS) generally concurs with the GAO recommendations, which are consistent with on-going Transportation Security Administration (TSA) efforts to improve Sensitive Security Information (SSI) program processes. However, we take strong exception with the analyses and conclusions. Specifically, the report mischaracterizes the nature of SSI by incorrectly applying concepts associated with classified information management to SSI information, which falls within a Sensitive But Unclassified (SBU) information category. SBU information includes such broadly used categories as For Official Use Only (FOUO) and Law Enforcement Sensitive (LES). This construct colors the entire report and may lead the reader to fundamental misunderstandings regarding the issues surrounding SSI. The SSI designation covers such information as airport and seaport security plans, screening procedures, operating parameters of screening equipment, vulnerability assessments, and other information that could be exploited by terrorists to harm the public and the nation's transportation systems.

The following discussion supports our position that GAO's analyses and conclusions are not valid because of how GAO evaluated the SSI program.

SSI is the Only Practical Means for Sharing Security Information with Regulated Parties.

SSI is primarily an information management tool that allows TSA to share information regarding transportation security with industry and foreign entities that have a need to know the information, but might not possess security clearances necessary for them to receive classified information. Sensitive information regarding transportation security can be shared with regulated parties without the limitations that would be imposed if the information were treated as

www.dhs.gov

a form of classified information. For example, TSA can distribute essential Security Directives and screening procedures in a timely manner to the multitude of airport and aircraft operators, both domestic and foreign, that transport the public. Detailed screening procedures can be provided to 45,000 TSA screeners without classified materials security clearances and without onerous handling limitations required for classified information including specifically approved safes and security logs. The absence of a robust SSI program would degrade both the prompt distribution of security information to persons with a need to know the information, and the free exchange of ideas among regulated parties to further transportation security.

SSI is also a mechanism for protecting transportation security information from indiscriminate release to those individuals who may seek to use government transparency as a means for obtaining information to harm the general public and the nation's transportation infrastructure. It has been widely reported that public source information has been specifically identified as an Al-Qaeda information resource.¹ Congress recognized the tension between this demonstrated need to protect certain information, and the mandate to support transparency in government operations, and concluded that SSI must be exempt from the Freedom of Information Act (FOIA), 5 U.S.C. §552.²

While the ability to protect SSI from release under FOIA is a critical component of SSI, it is ultimately a small part of the SSI system and subsumed within the overall purpose of sharing information with regulated parties that TSA would otherwise not be able to readily provide. It is through this protection under a statutory FOIA exemption that such information as Airport Security Plans, Security Directives, screening equipment limitations, vulnerability assessments, Federal Air Marshal deployment information, and other security information are protected from release to any person who files a request for documents under FOIA. Accordingly, TSA conducts a three-part SSI review of every document requested by the public to determine the appropriateness of any redaction that results in the withholding of SSI from the public. Through this process, TSA ensures that the public's right to access information about TSA operations is fully implemented. It is also through this process that TSA validates its identification of SSI documents, because it is only at this point that SSI restrictions most impact the public. If a TSA employee incorrectly marks a document as SSI while it remains within TSA, there is no impact on the public's right to access because the FOIA review process will always result in an independent determination regarding the SSI marking. Similar procedures exist for other avenues through which the public receives information, including Congressional, media, or litigation-related requests. In every case, TSA and DHS are committed to releasing as much information as possible.

SSI Designation Processes are Appropriate and Consistent with Every SBU Management System in Federal Government.

Like all SBU programs across the government, it is the obligation of every regulated person, whether TSA employee or employee of an entity covered by the SSI regulation, to mark as SSI

¹ On January 14, 2003, the Department of Defense reported that an Al Qaeda training manual recovered in Afghanistan stated that "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy." http://www.ioss.gov/docs/rumsfeld_14jan03.html.

² 49 U.S.C. §114(s).

those documents that clearly fall within defined SSI categories set out in the SSI regulation at 49 C.F.R. Part 1520, Protection of Sensitive Security Information. Thus, if an employee creates a vulnerability assessment of a transportation facility, there is no requirement for that employee to obtain permission from the equivalent of an original classification authority to mark and protect that document as SSI, because TSA has already designated vulnerability assessments as SSI in its published regulation. This marking obligation is no different from the obligation of any Federal employee in any Federal agency to mark as "FOUO" a sensitive document intended to be distributed for official use within the government. TSA is not aware of any examples of more effective or tightly tracked SBU systems within the Government.

The power to designate documents that may not clearly fall within the defined categories at 49 C.F.R. §§1520.5(b)(1)-(15), however, is limited to only seven TSA senior-level employees. That designation must be accompanied by a formal memorandum explaining the basis for designating the document as SSI. That form of designation, beyond the fifteen categories established by regulation, is used by TSA for only four items of information. GAO's report makes no distinction between the obligation to mark information as SSI, held by all employees, and the authority to designate, held by only a very few high level employees.³

It is for this reason that GAO's implied suggestion to quantify and identify (to GAO standards) all documents that have been marked as SSI, and all personnel who have marked such documents, is unworkable. The Government requires that agencies report the numbers and classification levels (Top Secret, Secret, or Confidential) of classified documents, but does not require reporting the titles of classified documents at any level, including Top Secret. We note that GAO did not recommend that TSA provide an inventory of the titles or numbers of SSI documents. Performing such inventories would impose enormous, administrative burdens that would require a vastly enlarged bureaucracy to implement. So long as the document falls within an SSI category established by regulation, it is the obligation of anyone who creates a document falling within that category to mark the document as SSI. In addition, SSI documents are created by non-TSA individuals including industry, Coast Guard, and the Federal Aviation Administration (FAA) personnel. Given that all documents that contain SSI created by any of these individuals must be marked and protected, developing a system to identify and track each potential and actual user, document, and title is not viable.

Similarly, limiting the number of personnel who mark a document SSI would also be unworkable. In a classified information system, an original classification authority uses a classification guide to determine whether a document should be classified. Within the SSI system, the SSI regulation serves a function similar to a classification guide by providing a framework for what should or should not be SSI. Since security information pervades TSA's mission and daily operations, limiting the ability to mark documents as SSI to a few individuals would create an information bottleneck without appreciably reducing the number of documents ultimately marked as SSI. Furthermore, it would risk the potentially inappropriate release of

³ Designation authority is currently limited to the Assistant Secretary for Transportation Security (TSA Administrator), Deputy Assistant Secretary, SSI Program Office Director, Chief Technology Officer, Assistant Administrator for Transportation Security Intelligence Service, Assistant Administrator for Intermodal Programs, and Assistant Administrator for Aviation Programs.

security information that should remain protected, as unmarked SSI documents are more difficult to protect and handle appropriately. The GAO report does not contest the substance of the SSI regulation covering the categories under which TSA appropriately marks SSI documents.

Finally, while the report does not recommend that TSA implement time limits for SSI information, GAO obliquely criticizes TSA's ability to protect SSI without a date by which the document automatically loses its SSI status. The reasons for designating information as SSI often remain valid for an indefinite period of time. While much classified information is time sensitive because it exists to protect sources of intelligence as much as the intelligence itself, SSI-designated operating procedures or screening equipment capabilities, for example, will remain sensitive so long as those procedures or that equipment remains in use, and do not become "stale" simply through the passage of time. Conversely, the SSI information may become obsolete much more rapidly than classified information if the procedures change substantially and could be de-designated before it would under a set schedule. As the GAO report acknowledges, the SSI regulation provides a mechanism for determining that a document should no longer be SSI. (49 C.F.R. §1520.5(c)).

GAO Recommendations and TSA Response

GAO Recommendation: *Establish clear guidance and procedures for using the TSA regulations to determine what constitutes SSI.*

TSA Response: TSA SSI regulations already provide a framework for determining what constitutes SSI. The TSA SSI Program office, created in February of this year within the Office of the Chief of Staff and assigned SSI policy and training functions, has also developed internal guidance that expands on the SSI regulation structure to provide examples of the types of information that should fall within each category. That guidance is an on-going effort that reflects the continued experience of the office with FOIA review, litigation support efforts, and general outreach with regulated parties. The SSI Program office expects to publish the guidance for general use by TSA employees and regulated parties in identifying and handling SSI.

GAO Recommendation: *Establish clear responsibility for the identification and designation of information that warrants SSI protection.*

TSA Response: Currently, only seven senior-level TSA employees have the authority to designate as SSI a document that does not fall within one of the fifteen categories specified in 49 C.F.R. §1520.5(b). Each covered person, including TSA employees, has an obligation to appropriately mark documents that fall within the fifteen categories. Those obligations are spelled out in the regulation, and in mandatory SSI training provided to every TSA employee.

Furthermore, limiting the number of individuals that may mark a document as SSI would lead to operational bottlenecks and to the potentially inappropriate release of security information that should remain protected. There would be no increase in the number of documents released to the public, since documents falling within the SSI regulation would ultimately still be marked SSI. Such a limitation impairs the utility of SSI as a system of shared, secure information, and would

not be operationally feasible. As noted earlier, GAO did not recommend that TSA provide an inventory of the titles or numbers of SSI documents. To reiterate, performing such inventories would impose enormous administrative burdens requiring a vastly enlarged bureaucracy. So long as the document falls within an SSI category established by regulation, it is the obligation of anyone who creates a document falling within that category to mark the document as SSI. In addition, SSI documents are created by non-TSA individuals including industry, Coast Guard, and FAA personnel. Because all documents that contain SSI created by any of these individuals must be marked and protected, developing a system to identify and track each potential and actual user, document, and title is not viable. The TSA SSI Program Office is currently designing materials that will further educate all TSA employees and other covered persons through clear policies, procedures, responsibilities, and guidance for identifying and marking SSI.

GAO Recommendation: *Establish internal controls that clearly define responsibility for monitoring compliance with regulations, policies, and procedures governing the SSI designation process and communicate that responsibility throughout TSA.*

TSA Response: TSA recognized shortcomings in SSI practices in the beginning of 2004 and charged the Internal Security Policy Board to make recommendations to improve TSA SSI practices. That Board recommended on October 14, 2004 that a central SSI Program Office be created and staffed, which has been accomplished. The SSI Program Office is currently developing internal controls, including audit functions, which will define responsibility for monitoring compliance with regulations, policies, and procedures governing the SSI designation process and will communicate that responsibility throughout TSA.

GAO Recommendation: *Establish policies and procedures within TSA for providing specialized training to those making SSI designations on how information is to be identified and evaluated for protected status.*

TSA Response: TSA already conducts specialized SSI training for SSI Program Office and FOIA staff, who review all FOIA requests prior to release to the public, and other TSA offices. TSA also has provided and is expanding specialized training to those offices within the agency that create the majority of SSI. TSA will continue to develop and provide more substantive training throughout TSA, including dramatically expanded guidance on identification and marking.

Thank you again for the opportunity to comment on this draft report. We are providing technical comments to your office under separate cover and trust that they will be considered for inclusion in the final report. We believe that most of the comments provide added context, background, and support for our position.⁴

Sincerely,



Steven J. Pecinovsky
Director, Departmental GAO/OIG Liaison Office
Office of the Chief Financial Officer

MMcP

⁴ In its technical comments, TSA addresses one incident that left a negative perception of TSA SSI practices. The GAO draft report noted an incident in which TSA prepared responses to questions submitted to the House Appropriations Homeland Security Subcommittee that were marked SSI, but that one month earlier had not been so marked. The incident was the result of an expedited review to accommodate a House Appropriations Committee schedule under which the normal SSI review process could not be accommodated. The result was that certain responses out of 373 questions were marked SSI because the materials fell within certain categories of the SSI regulation and there was no time to undertake a public source review that would have shown that the material was in the public domain. Once a review was undertaken, it was determined that 7 of the responses should not have been marked SSI. Given the unique circumstances of this particular request, where judgment had to be exercised quickly, favoring the preservation of security seemed the most appropriate course.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

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

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548