



Department of Homeland Security Office of Inspector General

TSA's Breach of Sensitive Security Information

(Redacted)





Homeland
Security

January 25, 2010

Preface

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

This report is in response to a request from the DHS Secretary. It addresses the circumstances, events, and actions surrounding the review, public posting, and discovery of unredacted Sensitive Security Information in a document on the internet, and identifies weaknesses in the department's policies and oversight for handling Sensitive Security Information. It is based on interviews with employees and officials of relevant components and offices; direct observations; and a review of applicable documents and databases.

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


Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

| | |
|--|----|
| Executive Summary | 1 |
| Background | 2 |
| Results of Review | 6 |
| Roundtable Discussion Used in Lieu of Three-Stage Review Process | 6 |
| OSSI Policies and Procedures do not Advise Employees on Handling and Releasing Redacted SSI Documents | 7 |
| Failure to Follow OSSI Procedures Resulted in an Improper Document Redaction ... | 8 |
| TSA Actions to Support the Montana Airport Solicitation Faced a Number of Challenges | 12 |
| SSI Security Breach Discovered..... | 15 |
| Conclusion | 17 |
| Recommendations, Management Comments, and OIG Analysis | 17 |

Appendices

| | |
|---|----|
| Appendix A: Scope, Purpose, and Methodology | 21 |
| Appendix B: TSA Comments to the Draft Report | 22 |
| Appendix C: Chief Privacy Officer Comments to the Draft Report | 26 |
| Appendix D: Evolution and History of the Redacted Screening Management SOPs | 28 |
| Appendix E: The SSI Review Analyst SOP Checklist and Style Guide | 29 |
| Appendix F: Office of SSI Transmission Email of Redacted Screening Management SOP to the Screening Partnership Program Office | 45 |
| Appendix G: Office of SSI Transmission Memorandum of Redacted Screening Management SOP to the Screening Partnership Program Office | 46 |
| Appendix H: Security Screening Standard Operating Procedures – Sensitive Security Information | 47 |
| Appendix I: Inventory of SSI Documents and Proper Handling Guidance | 49 |
| Appendix J: Major Contributors to this Report | 50 |
| Appendix K: Report Distribution | 51 |

Figures

| | |
|--|----|
| Figure 1: Visually Redacted and Redacted Document Creation | 10 |
| Figure 2: Chronology of Security Breach Discovery | 16 |

Table of Contents/Abbreviations

Abbreviations

| | |
|----------------|--|
| ACQ | Office of Acquisitions |
| DHS | Department of Homeland Security |
| FedBizOpps.gov | Federal Business Opportunities' website |
| OIG | Office of Inspector General |
| OIT | Office of Information Technology |
| OSO | Office of Security Operations |
| OSSI | Office of Sensitive Security Information |
| PDF | Portable Document Format Adobe® Acrobat® |
| PIA | Privacy Impact Assessment |
| R | Redacted |
| TSA | Transportation Security Administration |
| SOPs | Standard Operating Procedures |
| SPPO | Screening Partnership Program Office |
| SSI | Sensitive Security Information |
| STARS | SSI Tracking Audit and Review System |
| VR | Visually Redacted |

OIG

Department of Homeland Security
Office of Inspector General
Executive Summary

At the request of the Secretary for the Department of Homeland Security, we reviewed the events surrounding the release of Sensitive Security Information contained in the Transportation Security Administration's Screening Management Standard Operating Procedures. The Transportation Security Administration posted the document on March 3, 2009, and reposted it on March 16, 2009, to the Federal Business Opportunities, or FedBizOpps.gov, website, as part of a solicitation to privatize seven airports in the State of Montana. The objectives of our review were to determine how and why the release occurred, and whether management controls are in place and operational to ensure that a similar event would not recur. We determined that for the two documents in question, the redactions were not applied properly, and appropriate quality control procedures were not in place to protect against inadvertent disclosure. Consequently, Sensitive Security Information was visible in a public document posted on the internet. The Transportation Security Administration is conducting an internal vulnerabilities assessment of the effect of the standard operating procedures disclosure.

Transportation Security Administration officials received email messages on December 5, 2009, advising of a potential Sensitive Security Information breach. These notifications were made by a Transportation Security Administration employee to the Office of Sensitive Security Information, several Transportation Security Administration Sensitive Security Information Coordinators, the Transportation Security Administration Contact Center, as well as an external entity, the United States Computer Emergency Readiness Team. At this time, we are unaware of what actions TSA took in response to these notifications.

On December 6, 2009, at 4:28 p.m., the Transportation Security Administration Blog Team also received an email message indicating that unredacted Sensitive Security Information in its Screening Management Standard Operating Procedures was on the internet and visible to the public. Transportation Security Administration senior leadership did not receive notification until December 6, 2009, at 8:40 p.m. After receiving notification, the Acting Administrator took immediate actions and began intermediate and long-term measures to mitigate vulnerabilities. The Transportation Security Administration requested that the General Services Administration remove the website posting at 10:30 p.m. The

General Services Administration removed the solicitation, including the Screening Management Standard Operating Procedures from FedBizOpps.gov. Appendix D reflects the evolution and history of the redacted Screening Management Standard Operating Procedures.

We are making five recommendations, one to the department's Chief Privacy Officer, three to the Transportation Security Administration, and one is directed to both. In response to our draft report, the Transportation Security Administration and Chief Privacy Officer proposed plans and actions that, once implemented, will reduce a number of the deficiencies we identified. The Transportation Security Administration and the Chief Privacy Officer concurred with all of our recommendations.

Background

To comply with the *Aviation and Transportation Security Act of 2001*, the Transportation Security Administration (TSA) established pilot projects at five airports where employees of qualified private companies, under TSA's oversight, and in compliance with federal regulations, policies, guidance, and Standard Operating Procedures (SOPs), would perform passenger and baggage screening.¹ The law required that those contract screeners meet all the requirements applicable to federal screeners and the program be established no later than November 19, 2002. To satisfy the Act's requirement, TSA entered into contracts for pilot programs at the following airports:

- San Francisco International Airport
- Kansas City International Airport
- Greater Rochester International Airport
- Jackson Hole Airport
- Tupelo Regional Airport

To meet all the requirements applicable to federal screeners, private contract companies proposing to undertake and perform these duties would need information concerning airport Screening Management SOPs. These procedures contain Sensitive Security Information (SSI). SSI is a specific category of sensitive but unclassified information restricted from public disclosure. There are 16 categories of information relating to transportation security that constitute SSI. TSA's SSI regulation establishes certain requirements for the handling and dissemination of SSI,

¹Public Law 107-71, § 108.

including restrictions on disclosure, and also establishes that unauthorized disclosure is grounds for civil penalties and other enforcement action.² The Government Accountability Office said in its November 2007 letter report to Senators Byrd and Price that “According to TSA, SSI may be generated by TSA, other DHS agencies, airports, aircraft operators, and other regulated parties when they, for example, establish or implement security programs or create documentation to address security requirements.”³

Although the privatized screening pilot projects ended in November 2004, the Act includes a provision to expand the pilot program. As a result, other airport operators wanted to pursue privatized screening and TSA created the Screening Partnership Program Office (SPPO), within the Office of Security Operations (OSO), to perform and facilitate this function. Airport operators have been able to apply to SPPO to use private screeners since November 2004. As of January 2010, private contract screeners are in place at nine domestic airports.

Prior to a 2007 solicitation for requests for proposals to implement privatized screening at the Key West Airport, TSA required potential vendors to sign a nondisclosure agreement before providing the SSI Screening Management SOPs via its SPPO web-board. The web-board controlled access via login/password to vendor personnel who had submitted a signed nondisclosure agreement.

TSA officials reported to us that over time, TSA’s Office of Privacy and the Office of Chief Counsel’s Information Law branch informed SPPO and the Office of Acquisitions (ACQ) that the program’s prior process for vetting vendors, which included completion of a nondisclosure agreement, violated their privacy rights. TSA does not have a Privacy Impact Assessment (PIA) in place for the collection of personally identifiable information provided through the nondisclosure agreements. A PIA is a comprehensive process for determining the privacy, confidentiality, and security risks associated with the collection, use, and disclosure of personal information. It also defines the measures used to mitigate and, wherever possible, eliminate the identified risks. A PIA also communicates to the public how their privacy is protected and their information kept confidential and secure from unauthorized access.

²49 C.F.R. Part 1520.

³ GAO-08-232R Transportation Security Administration Processes for Designating and Releasing Sensitive Security Information, November 30, 2007.

Because of the concerns raised by the Offices of Privacy and Chief Counsel, TSA released the solicitation to implement privatized screening at the Key West Airport with limited information, did not have vendors sign a nondisclosure agreement, and did not release the SSI Screening Management SOPs. After the contract award, one vendor that had proposed to undertake and perform these duties at Key West Airport conveyed to TSA that not having access to SSI Screening Management SOPs placed them at a disadvantage, as other vendors had those documents through previously signed nondisclosure agreements.

In reviewing the Key West solicitation, the Offices of Chief Counsel and ACQ determined that TSA provided too little information and risked receiving an award protest. The expressed view was that incumbent contractors who already possessed the Screening Management SOPs would have an unfair advantage. To accommodate the information needs of potential vendors, and to discontinue the use of nondisclosure agreements, TSA officials we spoke with said that the Office of Sensitive Security Information (OSSI) suggested that SPPO include a redacted version of the Screening Management SOPs when releasing information in a request for proposal. We were told there was not a redacted version of the Screening Management SOPs at that time. In June 2008, SPPO requested that OSSI perform a review of the TSA Screening Management SOPs, Aviation Security Screening Management Standard Operating Procedures.⁴

Submission and Review of the Screening Management SOPs

SSI Review Request

OSSI is the SSI program manager for TSA. On June 23, 2008, SPPO submitted TSA's Screening Management SOPs to OSSI for review. In the SSI review request form, an SPPO official asked for "a review that identified specific SSI within the submitted record(s) so that the text can be either redacted (covered by black boxes) or visually redacted (highlighted)."

OSSI received and entered the SSI review request into its system on June 24, 2008. OSSI uses an automated system to process and track SSI review requests, called the SSI Tracking Audit and Review System (STARS). As noted on the request form, SPPO requested an expedited review of the Screening Management SOPs. Rather than the five to ten

⁴ Aviation Security, Screening Management Standard Operating Procedures; Revision 3; May 28, 2008, Implementation date: June 30, 2008. (SSI)

business days OSSI requires to complete a review, SPPO officials requested that OSSI complete the review by June 30, 2008, or four business days after OSSI entered the initial request into STARS.

Requests for Extension

After receipt of the initial review request, email correspondence between OSSI and SPPO indicate that OSSI twice communicated its inability to meet the expedited timeline of June 30, 2008. In an email message to SPPO dated June 26, 2008, OSSI program staff acknowledged that the office required an adjusted due date of July 3, 2008, because of the absence of key personnel.

On July 2, 2008, OSSI program staff again sent an email message to SPPO that indicated OSSI would be unable to meet the July 3, 2008, deadline. OSSI staff requested a readjusted timeline to perform their analysis. As explanation for this readjusted timeline, an OSSI senior official cited the need for a roundtable discussion, as well as additional support from OSSI subject matter experts on proposed redactions.

Three-Stage Review Process

According to *The SSI Review Analyst SOP Checklist and Style Guide*, located in Appendix E of this report, OSSI conducts most of its SSI reviews in a 3-stage review process. The first stage consists of a comprehensive SSI review of the material, including marking proposed redactions and providing accompanying citations to justify those redactions. These markings and citations are applied to the document by the first OSSI reviewer. Then the first reviewer's comments are subsequently reviewed by OSSI staff in the second and third stage reviews.

The second stage review requires a comprehensive review of the material as though it was the first review, except the OSSI analyst also critically examines the first reviewer's markings. The second reviewer can either agree with the first reviewer's proposed redactions, or mark corresponding sections in which redactions need adjustment. These markings and citations are also applied to the document by the second reviewer.

In the third and final stage, a senior OSSI analyst must perform the final review. As the final decision-making authority for the determination and review of SSI material in the document, the third OSSI reviewer resolves discrepancies in markings between the first and second reviewers. In addition, the third reviewer may choose to schedule a roundtable

discussion with relevant reviewers and subject matter experts to discuss proposed SSI redactions.

Results of Review

When TSA learned that SSI was publically available, it took immediate actions and began intermediate and long-term measures to mitigate vulnerabilities. In reviewing the events and circumstances surrounding the SSI release, we determined that OSSI's failure to follow its procedures resulted in an improper redaction of SSI. In addition, TSA actions to support the solicitation to privatize seven airports in the State of Montana faced a number of challenges, including several amendments to the solicitation, and concerns that the Screening Management SOPs attachment was not marked properly. Further, TSA and the department's internal controls for reviewing, redacting, and coordinating the protection of SSI are deficient.

Roundtable Discussion Used in Lieu of Three-Stage Review Process

OSSI officials described the roundtable discussion method as an exception to the 3-stage review process for reviewing documents for SSI content, but they contend that it is just as rigorous. OSSI uses it in limited circumstances, such as for complex documents or expedited review of documents not previously reviewed for redaction.

Due to the expedited nature of the review request, and because the Screening Management SOPs had not been reviewed for redaction of SSI before, at 1:00 p.m. on July 7, 2008, OSSI convened a roundtable discussion. In addition, the roundtable discussion allowed OSSI officials with subject matter expertise to collaborate on proposed redactions. During our review, we identified possible data integrity issues with the data contained in the STARS database. For example, according to STARS, there were four OSSI participants present at the roundtable discussion; however, evidence indicates that there may have only been three OSSI staff participants.

For the roundtable discussion, OSSI officials reviewed printed copies of the Screening Management SOPs and other relevant materials

During the roundtable discussion, the participants agreed upon the

redactions required in the Screening Management SOPs. At the conclusion of the meeting on July 7, 2008, the document was designated as having undergone final review. One participant in the roundtable discussion was tasked with completing the technical process of creating the redacted documents and delivering the documents to SPPO.

OSSI Policies and Procedures do not Advise Employees on Handling and Releasing Redacted SSI Documents

While TSA has policies and procedures for managing SSI, these policies and procedures do not include requirements for handling and releasing printed or electronically redacted documents. Each TSA Assistant Administrator and Federal Security Director must designate at least one SSI Coordinator for their functional area of responsibility. An SSI Coordinator assists OSSI with SSI matters, including assisting personnel with the appropriate use, application, and marking of SSI. TSA's policies and procedures should include detailed guidance as well as instruction on proper controls for the handling and release of redacted SSI material.

TSA officials reported to us that the TSA Online Learning Center features a *Sensitive Security Information (SSI) Awareness* course available to all TSA employees and is required as part of TSA's annual training requirements for employees who handle SSI documents. After our review of this training course, we determined that this training does not contain instruction on handling redacted SSI material, the process of consulting with SSI coordinators, or discussion of any other quality control steps prior to the release of redacted information outside of DHS.

The *Password Protection for Electronic Transmission and Storage of SSI Records* policy, dated September 29, 2006, requires authorization by the TSA Information Technology Security Office to post SSI material on secure portals, websites, or applications without passwords. The policy titled *Posting Material on the TSA Internet* pertains to information that is intended to be posted on TSA's website. Requirements include certification by an employee that the material does not contain SSI. Either OSSI or the employee's SSI Coordinator must review content that causes the employee uncertainty regarding its sensitivity. In addition, the employee must complete an Internet Posting Request form certifying that the material, whether a printed version of the electronic document or the html code posted on the internet, does not contain SSI. TSA should revise its SSI policies to advise employees on the creation of electronically redacted documents, and provide instructions on the proper posting of redacted information on unsecured internet sites.

An OSSI senior official told us that OSSI is not culpable for the release of SSI information by TSA employees. According to the OSSI senior official, current policies and procedures do not compel TSA employees to vet or request the assistance of OSSI in performing redactions and release of SSI. Should TSA agree with these statements, stronger internal controls are necessary.

Failure to Follow OSSI Procedures Resulted in an Improper Document Redaction

As described in *The SSI Review Analyst SOP Checklist and Style Guide*, SSI reviews can result in two types of products that are returned to requesting officials. On the SSI review request form, SPPO specifically requested the creation of both a visually redacted (VR) version as well as a redacted (R) version of the Screening Management SOPs. A VR version is a document in which SSI material has been identified and highlighted, and sensitive text is still visible to the requesting program official. An R version of a document contains the same redactions; however, in the R version the highlights are filled in so that sensitive material has been obscured from view. The R version of a final document is created directly from the VR version, and redactions in the two documents should be identical.

Redaction and Delivery of Document

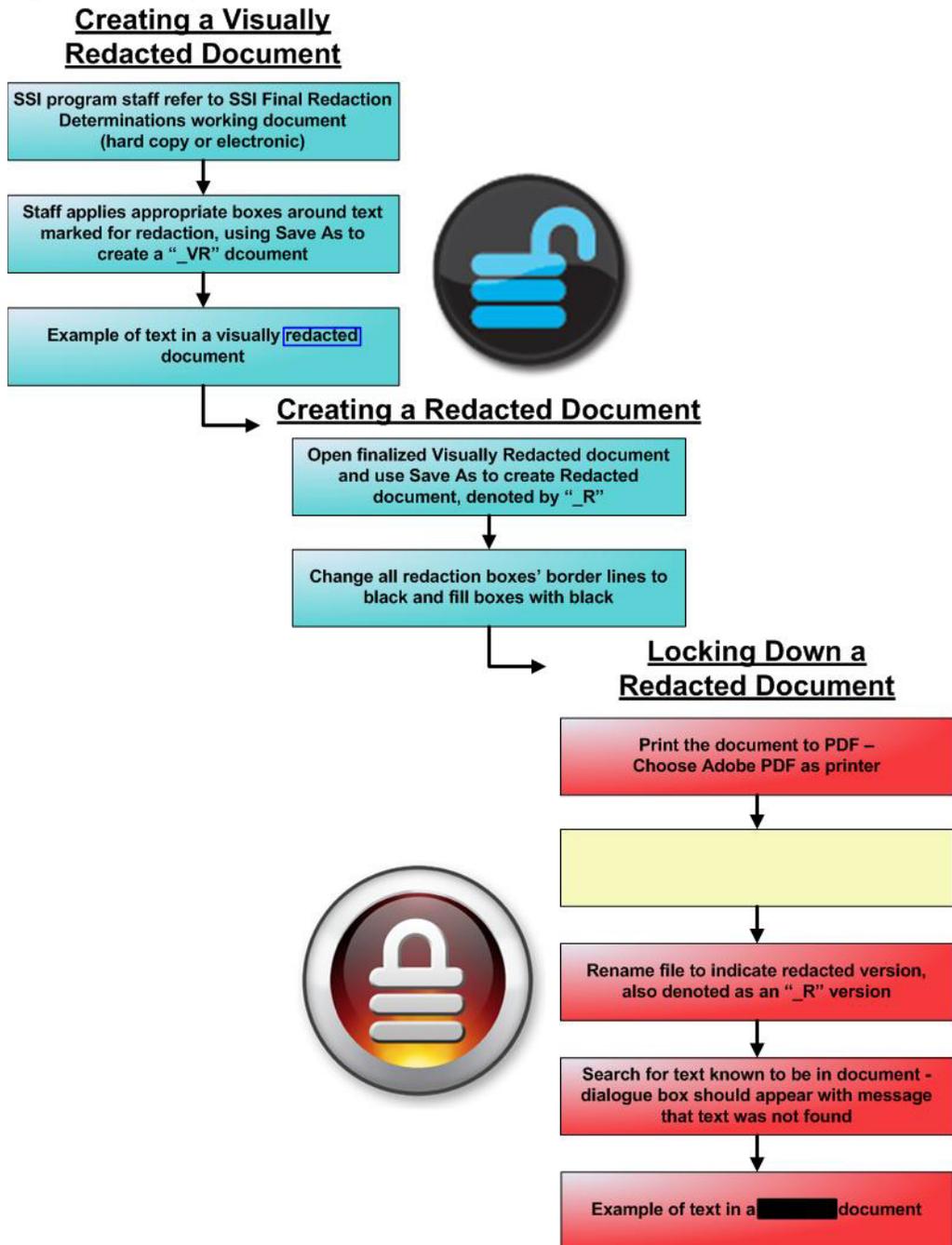
Following the roundtable discussion on July 7, 2008, the agreed upon redactions were applied to the documents. According to STARS, OSSI program staff finalized the documents at 2:47 p.m. At 3:03 p.m., OSSI delivered the documents to SPPO via an email. The email contained both the VR and R versions of the document as well as a transmittal memorandum describing the authority by which such information had been withheld. Refer to Appendices F and G for a copy of the email and memorandum. Even though OSSI redacts the SSI header and footer in the R version, these markings were still visible when transmitted to SPPO. The identified SSI content within the document, however, was covered by black redaction boxes.

In our discussions with senior OSSI staff, they believed that the OSSI guide's step-by-step directions would result in a secure or "locked down" image file, and that the text under the black redaction boxes is not visible or retrievable. By their account, the process of creating an R version of an SSI document allows TSA to share information publically and as broadly as possible without divulging SSI. OSSI used [REDACTED] to perform redaction of the Screening Management SOPs.

In [REDACTED] the key step to ensure that document contents cannot be either manipulated or retrievable is to check [REDACTED]. Officials from the Offices of OSSI and TSA's Office of Information Technology (OIT) reported to us that OSSI did not consult with OIT prior to the December 6, 2009, breach to ensure that the redaction process as written in *The SSI Review Analyst SOP Checklist and Style Guide* resulted in a locked down image of the document where text under the black redaction boxes is not visible or retrievable. The OSSI guide's step-by-step directions to create VR and R versions are depicted in Figure 1.

⁵ [REDACTED] software program, which views, creates, manipulates and manages files in [REDACTED] a file format that allows for cross-platform electronic information exchange.

Figure 1: Visually Redacted and Redacted Document Creation



Source: *OIG Analysis of The SSI Review Analyst SOP Checklist and Style Guide*

TSA officials said that for the redacted information in the Screening Management SOPs to be visible, OSSI staff did not check [redacted] for the R version. Further, OSSI staff should have realized the error upon performing the text search step, which serves as OSSI’s only quality control feature to ensure redactions are applied correctly. A

secondary check by another OSSI staff could have identified the error, but this procedure was not in place and did not occur prior to distribution of the VR and R documents from OSSI to SPPO.

As we depict in Figure 1, our review of the Screening Management SOPs determined the steps used to create a redacted document could lead to confusion. Instructions in *The SSI Review Analyst SOP Checklist and Style Guide* on redacted document naming are ambiguous and could lead to improper redaction and inadvertent SSI disclosure. Once OSSI personnel are finished creating the VR version, the instructions direct the creation of two R version documents that look identical, yet only one is properly redacted [REDACTED]. With two documents having the same nomenclature, OSSI could potentially send the R version that is not properly locked down [REDACTED] and the recipient would be unaware that redacted information is retrievable. Given OSSI's procedures, there is a high chance of failure to select the properly redacted version. OSSI could have eliminated this potential failure by restructuring the nomenclature into three distinct file names.

Sending the VR and R to the Requestor

The transmittal memorandum accompanying the two documents indicated both documents were password protected. The memorandum further instructed the recipient that for external distribution of these files, the recipient is to either use a printed copy or, in the case of the password protected file re-save the file with an idiosyncratic password that meets TSA's password requirements.⁶ The transmittal memorandum also advised SPPO of OSSI's availability to answer any questions related to the redacted documents. When we opened the same documents sent to SPPO, the VR version included password protection.

On August 15, 2008, SPPO staff returned the redacted Screening Management SOPs in an email message to an OSSI staff member stating that SPPO wants to release the SOPs. In this message the SPPO staff member also said that he or she believed that the "header footer" needed to be marked out. We have made a request for additional documentation to further analyze the communications between these two individuals. This was OSSI's first opportunity to realize the document was not properly redacted.

⁶ According to the TSA Sensitive Security Information Policy and Procedure Guide, to electronically transmit SSI material via email, all passwords must follow a prescribed standard format as determined in the policy.

Although not the focus of our review, when OSSI produces a locked down [REDACTED] document using its internal policy, these documents do not appear to be in compliance with DHS' Management Directive, *Section 508 Program Management Office & Electronic and Information Technology Accessibility*. To be 508 compliant, non-redacted text must be searchable, and OSSI's creation of a locked down [REDACTED] does not allow assistive technology to access non-redacted text. Because this issue is outside the scope of our review, once immediate concerns of the SSI breach have been resolved, TSA should conduct an analysis of OSSI's 508 compliance.

OSSI's Three-Stage Review Processes Warrant Further Review

OSSI's procedures instruct reviewers to use a color-coded system to distinguish the different levels of review for a document. Each level of review is assigned a distinctive color to use when marking SSI content identified in a document. Therefore, the third-stage reviewer could see two different colors marking which level of review identified particular SSI content.

According to some OSSI program staff, the application of color-coded boxes, used by analysts to distinguish the various review stages and redactions, may have been applied inconsistently in other OSSI redaction reviews. This potential inconsistency and confusion over procedures is outside of our current scope, but should be reviewed in the future to ensure the integrity, designation, and proper protection of SSI.

TSA Actions to Support the Montana Airport Solicitation Faced a Number of Challenges

Posting of Solicitation to Federal Business Opportunities Website

There was a significant time gap between the August 15, 2008, email and the initial posting of the request for proposal on February 7, 2009. Although we have been unable to determine the exact cause of the gap, several TSA officials told us there were organizational and staff changes in offices involved in the procurement during this timeframe, as well as delays in funding and program decisions.

On February 7, 2009, TSA's ACQ posted solicitation Number HSTS05-09-R-SPP061, on FedBizOpps.gov. FedBizOpps.gov lists notices of proposed government procurement actions, contract awards, sales of government property when the value is greater than \$25,000, and other procurement information. Solicitation HSTS05-09-R-SPP061 disclosed

that TSA intended to solicit industry to provide transportation security screening services at seven Montana airports, to include comprehensive screening of passengers and baggage. The initial posting did not include the Screening Management SOPs.

On February 13, 2009, ACQ staff posted Amendment 1 to FedBizOpps.gov. Amendment 1 provided industry with the time of the Pre-Proposal Conference at TSA headquarters and changed the date for potential bidders to submit questions. Amendment 1 did not include the posting of the Screening Management SOPs.

Concerns Surfaced that the Solicitation Did Not Include the Screening Management SOPs

As the posted solicitation on February 7, 2009, and Amendment 1 on February 13, 2009, did not include the Screening Management SOPs, there were discussions within TSA to get the SOPs posted. ACQ staff said they would have included the Screening Management SOPs as an attachment to the February 7, 2009 solicitation, but they had failed to do so because SPPO had not submitted it with other procurement documents. On February 26, 2009, ACQ and SPPO staff discussed whether to include the Screening Management SOPs with a new amendment to the solicitation.

These conversations resulted in a decision to provide a redacted Screening Management SOPs to ensure potential bidders had access to the necessary information to create meaningful proposals in response to the solicitation. SPPO coordinated with the OSO Procedures Branch on the afternoon of February 26, 2009, to determine whether the SOPs had undergone significant updates since the SSI review in July 2008. Shortly after SPPO's request, the Procedures Branch provided SPPO with a summary of updates between the current Screening Management SOPs and the redacted version provided by SPPO. As these changes were determined to be insignificant, the SPPO made the decision to move forward with the redacted version, and at 4:52 p.m. on February 26, 2009, SPPO forwarded what was thought to be a redacted Screening Management SOPs to ACQ. Our review of the document determined that the SSI header and footer markings on this document were not redacted, although the identified SSI content within the document was covered by black boxes.

ACQ staff posted Amendment 2 to FedBizOpps.gov on March 3, 2009. Amendment 2 replaced the existing Solicitation Table of Contents, changed the date for questions or requests for clarification submittals, changed the due date for proposal submissions, and added the Screening Management SOPs as attachment J-15. This is the first posting

of the Screening Management SOPs to FedBizOpps.gov. Interviews with staff from SPPO and ACQ revealed that neither SPPO nor ACQ performed any check of the electronic document to ensure the redactions were applied correctly. Both SPPO and ACQ staff believed it was OSSI's responsibility to provide a fully protected document.

Additional Concerns Raised That the Screening Management SOPs Attached to the Solicitation Was Improperly Marked

On March 10, 2009, SPPO staff received notification that the redacted Screening Management SOPs loaded to FedBizOpps.gov still had the SSI header and footer markings, even though the document was reportedly fully redacted. The SPPO personnel notified ACQ staff about the improperly marked SOP. ACQ personnel acknowledged that the markings were visible and should be blacked out. ACQ staff said that the visible marking would cause some concern even though there was no visible SSI in the document.

Dialogue continued between ACQ and SPPO personnel concerning adding a new amendment to the solicitation with a correctly marked version of the SOPs. ACQ personnel asked SPPO staff for a point of contact from the office that controls the SOPs to solicit guidance. The SPPO advised ACQ personnel to seek guidance from OSSI. OSSI senior staff instructed ACQ personnel to publish a new version of the document with the visible SSI header and footer markings blacked out, but stated that no harm was done. ACQ staff explained again that there did not appear to be any sensitive information in the document, and OSSI acknowledged their statement and thanked ACQ staff for the briefing.

Further evidence shows that on the afternoon of March 13, 2009, ACQ transmitted an electronic version of the July 7, 2008, redacted SOP for correction to OSSI. Later that afternoon, OSSI senior contract staff transmitted a modified version of the July 7, 2008, redacted SOP to ACQ. Our preliminary analysis of this modified SOP demonstrates that the SSI header and footer markings were redacted properly. However, the black box redactions were not properly locked down. Meaning the text under the black boxes would remain visible should the boxes be moved. Thus, OSSI did not perform their own quality control procedures to ensure the Screening Management SOPs were locked down. This was OSSI's second opportunity to realize the document was not properly redacted.

ACQ staff posted the modified July 7, 2008, redacted SOP as part of Amendment 3 to FedBizOpps.gov solicitation on March 16, 2009. Amendment 3 included changing the ACQ solicitation point of contact, and providing government responses to bidder's questions in PDF format;

government changes to request for proposal in response to bidder questions in PDF format; a slide presentation from Pre-Proposal Conference in PDF format; and a what was thought to be a fully redacted Screening Management SOPs document from Amendment 2 in PDF format.

SPPO Procurement Package Remains on Federal Business Opportunities After Contract Award

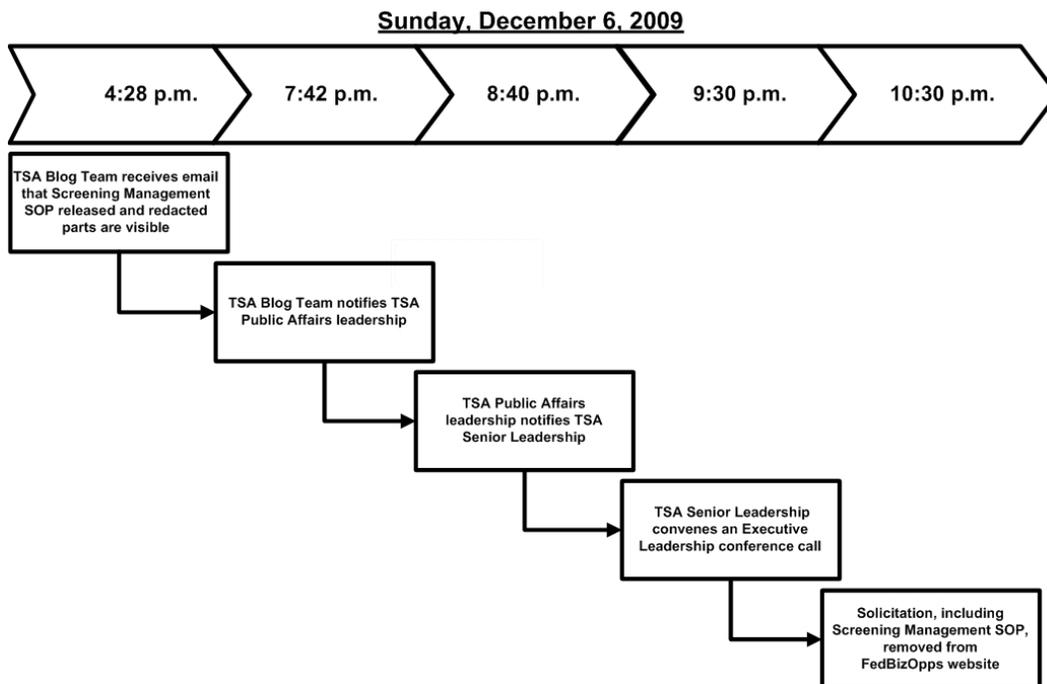
On August 24, 2009, TSA awarded the contract for screening management services at the seven Montana airports. According to FedBizOpps.gov personnel, after a procurement is complete, the information posted to support the solicitation is removed from active listings, but remains retrievable on the FedBizOpps.gov. The information remains on the website for historical purposes and allows individuals to conduct market research regarding past government purchases. ACQ staff stated that Amendments 2 and 3 to the solicitation included the Screening Management SOPs, but also administrative procurement related documents. ACQ staff told us they believed the contents of the documents were properly redacted, therefore there was no need to remove them from FedBizOpps.gov. As a result, the Screening Management SOPs were archived with the other procurement related documents.

SSI Security Breach Discovered

TSA officials received email messages on December 5, 2009, advising of a potential SSI breach. These notifications were made by a TSA employee to OSSI, several TSA SSI Coordinators, the TSA Contact Center, as well as an external entity, the United States Computer Emergency Readiness Team. At this time, we are unaware of what actions TSA took in response to these notifications.

On December 6, 2009, at 4:28 p.m., the TSA Blog Team received an email indicating that redacted SSI in TSA's Screening Management SOPs was on the internet and visible to the public. Figure 2 reflects TSA's senior leadership actions in response to the Blog Team notification.

Figure 2: Chronology of Security Breach Discovery



Source: OIG Analysis of TSA Information

TSA Actions in Response to the SSI Security Breach

In response to the notification of the improperly redacted Screening Management SOPs on the internet, TSA’s Acting Administrator implemented a number of immediate actions and formulated intermediate and long-term plans to mitigate vulnerabilities. Some of these actions include:

- Directing that all screening SOPs are to be marked and handled as SSI in entirety until further review.
- Conducting an inventory of all SSI documents and directing development of specific handling guidance.
- Directing ACQ review all other FedBizOpps.gov postings for SSI and take down any SSI documents.
- Directing OSO complete a full review of the SOP that was leaked and advise of any additional enhancements to security operations that should be made.
- Conducting aggressive outreach to industry stakeholders and partners.

Refer to Appendices H and I for more detailed information on these December 8, 2009, actions. Also to convey the level of importance of this incident the Acting Administrator conveyed, “It was a failure that we take

very seriously, but in the end, we will be a stronger organization and our security system will be even further enhanced because we have been through this crisis.”

Conclusion

Once TSA received notification that SSI in its Screening Management SOP was visible to the public, the Acting Administrator took a number of immediate, intermediate, and long-term actions to mitigate vulnerabilities. In reviewing the events and circumstances surrounding the SSI release, we determined that OSSI’s failure to follow its procedures resulted in an improper redaction of SSI. In addition, TSA actions to support the solicitation to privatize seven airports in the State of Montana faced a number of challenges, including several amendments to the solicitation and concerns that the Screening Management SOPs attachment was not marked properly. Although the solicitation closed on August 24, 2009, the original request for proposal with all attached documents remained visible on the internet until the TSA Blog Team received notification of the breach on December 6, 2009.

We are concerned that an improperly redacted version of the SSI Screening Management SOPs passed through a number of TSA offices from June 7, 2008, to posting the document on FedBizOps.gov on March 3, 2009, and again on March 16, 2009, without any internal procedures to determine whether the document was redacted properly. As a result, TSA and department internal controls for reviewing, redacting, and coordinating the protection of SSI are deficient. By implementing our five recommendations, TSA and the department will be positioned better to protect the handling, review, redaction, and dissemination of SSI.

Recommendations, Management Comments, and OIG Analysis

Recommendation #1: We recommend that the DHS Chief Privacy Officer convene a working group of information technology experts from across the department to determine a department-wide standard for redaction software, and to develop methods for the proper public release of any sensitive information. Ensure that any selected software meets the department-wide standards as determined by the working group.

Chief Privacy Officer Response: The Chief Privacy Officer concurs with Recommendation 1. In December 2009, DHS’ Deputy Secretary established a senior level team, the DHS Information Security Working Group, to examine the department’s information security program

protocols related to sensitive but unclassified information. The Chief Privacy Officer and the working group, which includes information technology, security, policy, privacy, and legal experts, have met several times and have instituted the planning necessary to take these steps.

TSA Response: TSA management responded that it will support all actions initiated in response to this recommendation.

OIG Analysis: The department's proposed actions are responsive to the intent of the recommendation, which is resolved and open. This recommendation will remain open pending our receipt of the working group's department-wide standard for redaction software, the methods developed for the proper public release of any sensitive information, and a determination that any software used for redaction meets the department-wide standards determined by the working group.

Recommendation #2: We recommend that the DHS Chief Privacy Officer, in coordination with the Acting Administrator for TSA revise policies, procedures, and training materials to ensure that upon transmission or receipt of any redacted document, department senders and recipients are required to determine whether redacted information in the document is visible or retrievable. When redacted information is visible or retrievable, the sender and recipient must acknowledge to one another the document is not redacted and cannot be disseminated publicly.

Chief Privacy Officer Response: The Chief Privacy Officer concurs with Recommendation 2, and will coordinate with TSA's Acting Administrator. The Chief Privacy Officer notes that the Acting Administrator responded separately to us, and TSA will revise its procedures and training materials to include the proper handling of redacted materials to ensure they no longer contain sensitive information prior to public release. The Chief Privacy Officer responded that the DHS Information Security Working Group is coordinating the review and revision of policies, procedures, and training materials department-wide.

TSA Response: TSA management responded that it concurs with Recommendation 2. TSA will revise its procedures and training materials to include the proper handling of redacted materials to ensure they no longer contain sensitive information prior to public release.

OIG Analysis: The department's proposed actions are responsive to the intent of the recommendation, which is resolved and open. This recommendation will remain open pending our receipt of TSA's revised procedures and training materials to include the proper handling of redacted materials.

Recommendation #3: We recommend that the Acting Administrator for TSA ensure that upon the redaction of any Sensitive Security Information document, there is an independent quality control procedure to validate that redacted information is not visible or retrievable. The quality control reviewer is someone other than the person who performs and applies the redactions. The quality control reviewer is to search the document for known redacted text, and is to determine that no visible or retrievable information exists before subsequent transmission of the document can occur.

TSA Response: TSA management responded that it concurs with Recommendation 3. TSA's Sensitive Security Information Program Office has been realigned from the Office of the Special Counselor to the Office of Intelligence as the Sensitive Security Information Branch. Immediately following this incident, the Sensitive Security Information Branch has made one employee responsible for Quality Assurance reviews. Based upon the results of this inspection, TSA will make additional changes to the Quality Assurance position.

OIG Analysis: TSA's proposed actions are responsive to the intent of the recommendation, which is resolved and open. This recommendation will remain open pending our receipt of TSA's changes to the Quality Assurance position, which demonstrates there is an independent quality control procedure to validate that redacted information is not visible or retrievable.

Recommendation #4: We recommend that the Acting Administrator for TSA provide Sensitive Security Information recipients with handling and transmission instructions, which include details for external releases and password protection measures. Further, these instructions should be retained with the Sensitive Security Information document.

TSA Response: TSA management responded that it concurs with Recommendation 4. In addition to required annual training for TSA employees, TSA makes guidance available on the proper handling of SSI. This guidance will be updated to include handling, transmission, and external release instructions.

OIG Analysis: TSA's proposed actions are responsive to the intent of the recommendation, which is resolved and open. The recommendation will remain open pending our receipt TSA's revised guidance, which includes updated handling, transmission, and external release instructions.

Recommendation #5: We recommend that the Acting Administrator for TSA conduct an audit of the Sensitive Security Information Tracking Audit and Review System to ensure that intake, review, and dissemination of requests are accurate.

TSA Response: TSA management responded that it concurs with Recommendation 5. The TSA's Acting Administrator has asked TSA's Office of Inspection to conduct a program review on this matter.

OIG Analysis: TSA's proposed actions are responsive to the intent of the recommendation, which is resolved and open. This recommendation will remain open pending our receipt of TSA's Office of Inspection program review of the Sensitive Security Information Tracking Audit and Review System.

Appendix A

Scope, Purpose, and Methodology

In response to a request from DHS' Secretary, we assessed the events and actions surrounding the review, public posting, and discovery of an unredacted SSI Screening Management SOPs document. Specifically, our objectives were to determine how and why the release occurred, and whether management controls are in place and operational to ensure that a similar event would not recur.

We interviewed representatives of multiple TSA offices, to include OSSI, the SPPO, ACQ, OIT, OSO, Office of Special Counselor, and the Office of Inspections. In addition, we interviewed employees and officials of relevant offices, components, and entities external to TSA and DHS. We did not perform an analysis of OSSI's assessment of what it considers SSI in the Screening Management SOP.

We also reviewed applicable legislation, regulations, directives, policies, operating procedures, databases, and official guidance, documents and manuals. In addition, we studied work previously performed by our office in this and associated areas, as well as the work conducted by Government Accountability Office.

Our fieldwork occurred in December 2009. We initiated this review under the authority of the *Inspector General Act of 1978*, as amended, and according to the "Quality Standards for Inspections," issued by the President's Council on Integrity and Efficiency.

Appendix B

TSA Comments to the Draft Report

DEC 23 2009

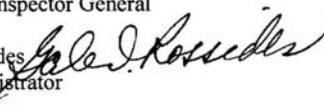


U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 20598

Transportation
Security
Administration

INFORMATION

MEMORANDUM FOR: Carlton I. Mann
Assistant Inspector General for Inspections
Office of the Inspector General

FROM: Gale D. Rossides 
Acting Administrator

SUBJECT: Transportation Security Administration Response to Office
of Inspector General Draft Report "TSA's Breach of
Sensitive Security Information"

Purpose

This memorandum presents the official agency response to the Office of the Inspector General's (OIG) draft report entitled "TSA's Breach of Sensitive Security Information." TSA appreciates OIG's work in investigating this incident and preparing this report.

Background

At the request of the Secretary, OIG reviewed the events surrounding the release of SSI contained in TSA's Screening Management Standard Operating Procedures. The objectives of OIG's review were to determine how and why the release occurred and whether management controls are in place to ensure that a similar event would not recur.

Discussion

TSA appreciates the work done by OIG in conducting this inspection and its timely response and review. We take this matter seriously and regret that it occurred.

Once TSA received notification that SSI in its Screening Management SOP was visible to the public, OIG found TSA took a number of immediate, intermediate, and long-term actions to mitigate vulnerabilities. In reviewing the events and circumstances, OIG determined that the SSI program office failed to follow its procedures which resulted in an improper redaction of SSI. In addition, OIG is concerned that an improperly redacted version of the SSI Screening Management SOP passed through a number of TSA offices from June 7, 2008, until the time it was posted on FedBizOps.gov on March 3, 2009, without any internal procedures to determine whether the document was redacted properly. As a result, OIG concluded that TSA and department internal controls for

Appendix B

TSA Comments to the Draft Report

designating, identifying, reviewing, redacting, and coordinating the release of SSI are deficient.

TSA agrees with OIG's conclusions and will continue to pursue an aggressive response to this breach with a comprehensive review of the manner in which TSA handles sensitive information of all types under the leadership of the internal Information Protection Oversight Board. In addition to the immediate measures referenced in the report, TSA is taking additional intermediate and long-term steps to ensure the proper control of sensitive information.

Conclusion

Despite this incident, TSA's aviation security procedures remain strong. The duties performed by TSA's dedicated workforce of Transportation Security Officers (TSOs), Federal Air Marshals, canine teams, and other have not been adversely impacted. TSA will continue to ensure the same high level of security we provide every day. Our workforce is responsive, accountable, and dedicated to safeguarding the traveling public. Neither our capability nor our resolve has been diminished by this incident.

TSA appreciates the work done in this engagement. Our response to the recommendations follows in the attachment.

Appendix B

TSA Comments to the Draft Report

Transportation Security Administration Response to Recommendations Office of the Inspector General Draft Report “TSA’s Breach of Sensitive Security Information”

Recommendation 1 is made to the Deputy Secretary. TSA will support all actions initiated by the Deputy Secretary in response to this recommendation.

Recommendation 2: Revise policies, procedures and training materials to ensure that upon transmission or receipt of any redacted document, department senders and recipients are required to determine whether redacted information in the document is visible or retrievable. If redacted information is visible or retrievable, the sender and recipient must acknowledge to one another the document is not redacted and cannot be disseminated publicly.

TSA concurs. TSA will revise its procedures and training materials to include the proper handling of redacted materials to ensure they no longer contain sensitive information prior to releasing them to the public.

Recommendation 3: Ensure that upon the redaction of any Sensitive Security Information document, there is an independent quality control procedure to validate that redacted information is not visible or retrievable. The quality control reviewer is someone other than the person who performs and applies to redactions. The quality control reviewer is to search the document for known redacted text, and is to determine that no visible or retrievable information exists before subsequent transmission of the document can occur.

TSA concurs. The Sensitive Security Information Program Office has been realigned from the Office of the Special Counselor to the Office of Intelligence as the Sensitive Security Information Branch. Immediately following this incident, the SSI Branch has made one employee responsible for Quality Assurance reviews. Based upon the results of this inspection, TSA will make additional changes to the QA position.

Recommendation 4: Provide Sensitive Security Information recipients with handling and transmission instructions, which include details for external releases and password protection measures. Further, these instructions should be retained with the Sensitive Security Information document.

TSA concurs. In addition to required annual training for TSA employees, TSA makes guidance available on the proper handling of SSI. This guidance will be updated to include handling, transmission, and external release instructions.

Recommendation 5: Conduct an audit of the Sensitive Security Information Tracking Audit and Review System to ensure that intake, review, and dissemination of requests are accurate.

Appendix B
TSA Comments to the Draft Report

TSA concurs. The Acting Assistant Secretary has asked TSA's Office of Inspection to conduct a Program Review on this matter.

Appendix C Chief Privacy Officer Comments to the Draft Report

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



**Homeland
Security**

January 6, 2010

MEMORANDUM FOR: Richard L. Skinner
Inspector General

FROM: Mary Ellen Callahan 
Chief Privacy Officer

SUBJECT: Response to *Office of Inspector General Draft Report "TSA's Breach of Sensitive Security Information"*

Thank you for the opportunity to review and provide comments on the subject report which pertains to the release of Sensitive Security Information contained in the Transportation Security Administration's (TSA) Screening Management Standard Operating Procedures. As Chief Privacy Officer, I concur with the recommendations as written. Listed below are my specific responses to the two recommendations assigned to me for action.

Recommendation 1: Immediately convene a working group of information technology experts from across the department to determine a department-wide standard for redaction software, and to develop methods for the proper public release of any sensitive information. Ensure that any selected software meets the department-wide standards as determined by the working group.

The Chief Privacy Officer concurs with this recommendation. In December 2009, the Deputy Secretary established a senior level team known as the DHS Information Security Working Group to examine the Department's information security program protocols related to Sensitive But Unclassified (SBU) information. The Chief Privacy Officer and the working group, which includes information technology -- as well as security, policy, privacy, and legal -- experts have met on several occasions and have already instituted the planning necessary to take these steps.

Recommendation 2: Revise policies, procedures, and training materials to ensure that upon transmission or receipt of any redacted document, department senders and recipients are required to determine whether redacted information in the document is visible or retrievable. If redacted information is visible or retrievable, the sender and recipient must acknowledge to one another the document is not redacted and cannot be disseminated publicly.

The Chief Privacy Officer concurs with this recommendation to coordinate with the Acting Administrator for TSA and notes that on December 23, 2009, the Acting Administrator for TSA separately provided a response to the Office of the Inspector General stating TSA will revise its procedures and training materials to include the proper handling of redacted materials to ensure they no longer contain sensitive information prior to releasing them to the public. The aforementioned

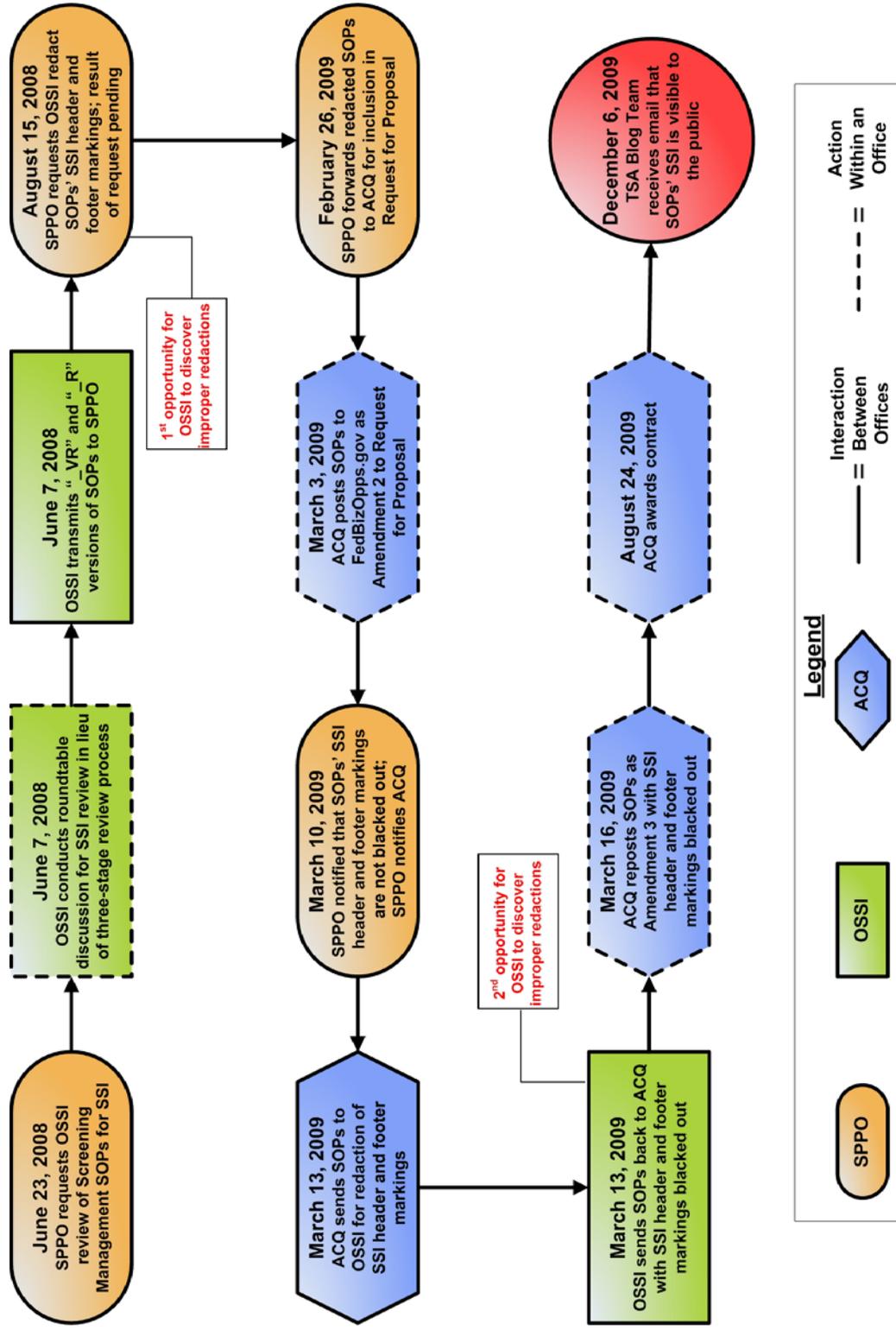
Appendix C

Chief Privacy Officer Comments to the Draft Report

Information Security Working Group is coordinating the review and revision of policies, procedures, and training materials department-wide.

If you have any questions or concerns, please contact me at (703) 235-0347 or by email at mary.ellen.callahan@dhs.gov.

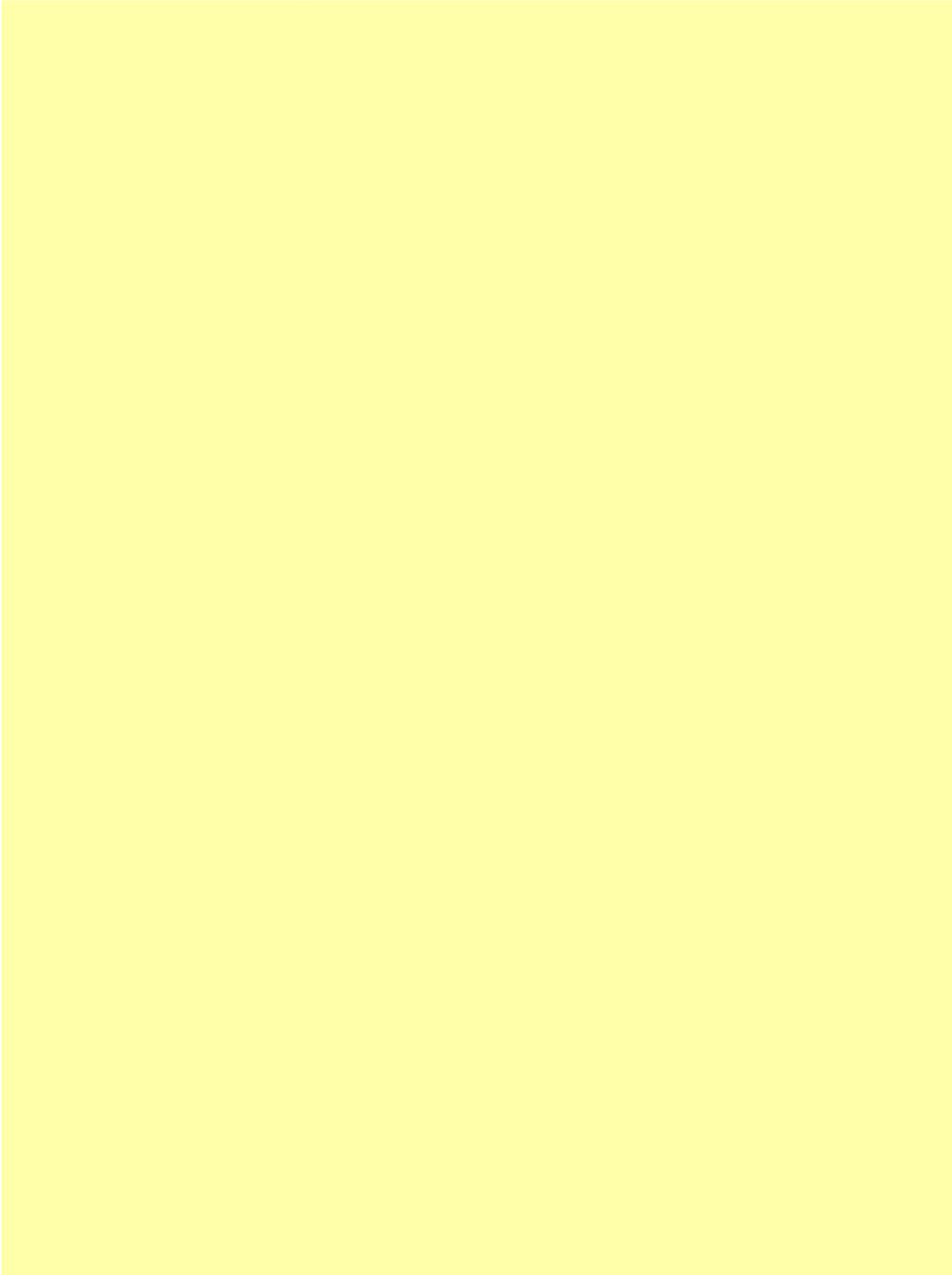
Appendix D Evolution and History of the Redacted Screening Management SOPs



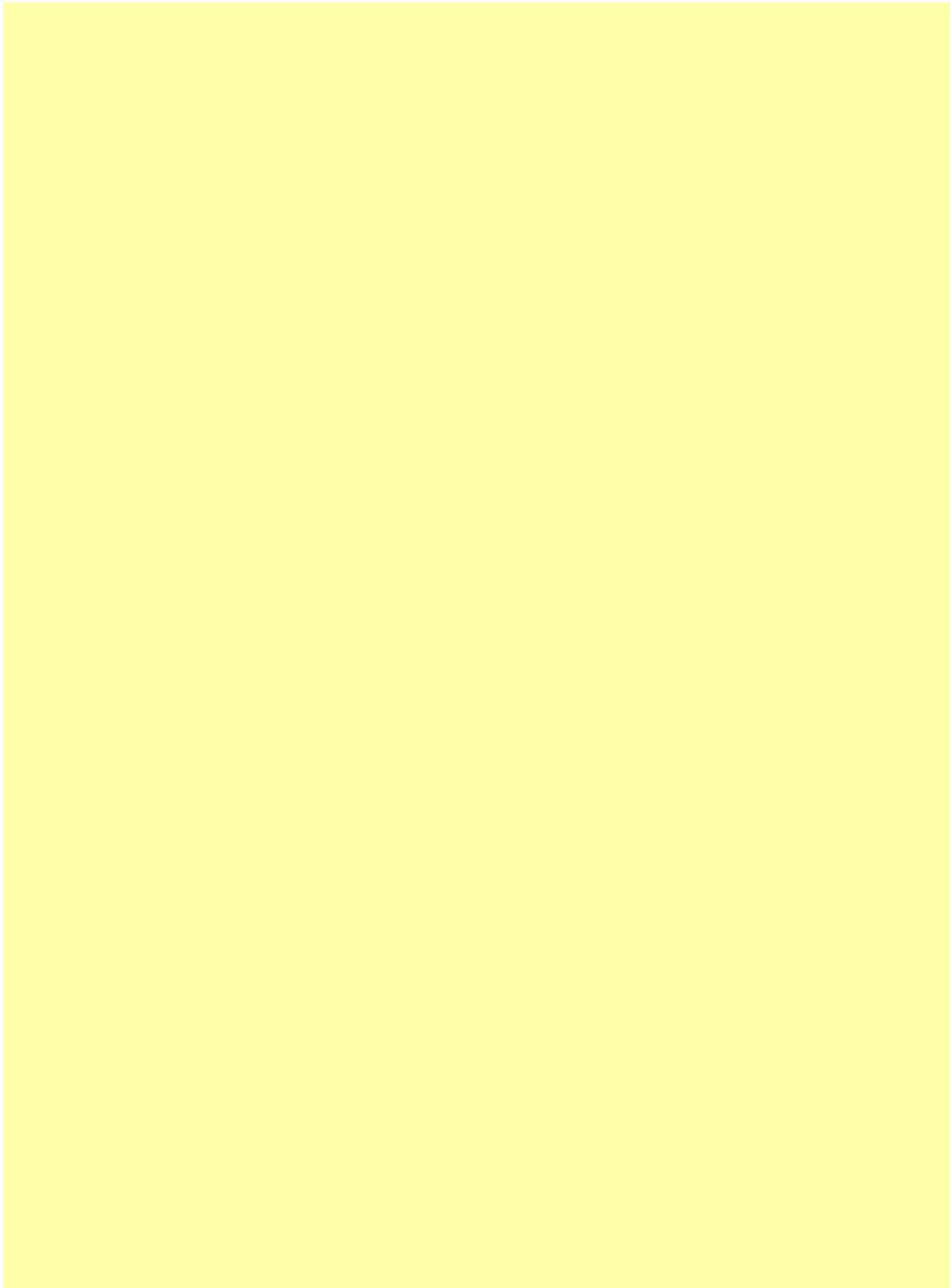
Source: OIG Analysis of TSA Information

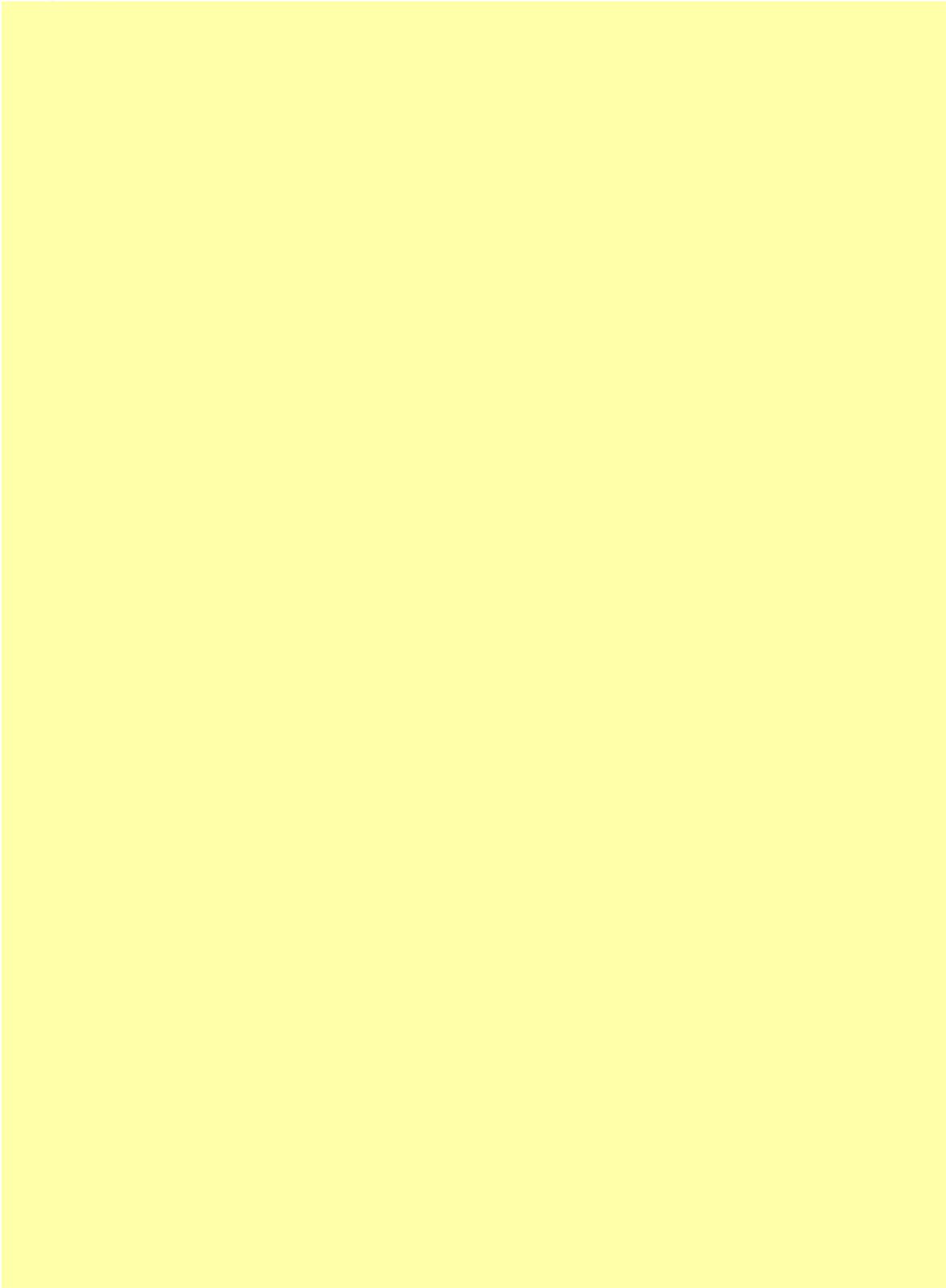
Note: On February 26, 2009, SPPO coordinated with the Office of Security Operations' Procedures Branch, to review updates to the content of the SOPs, not the redactions.

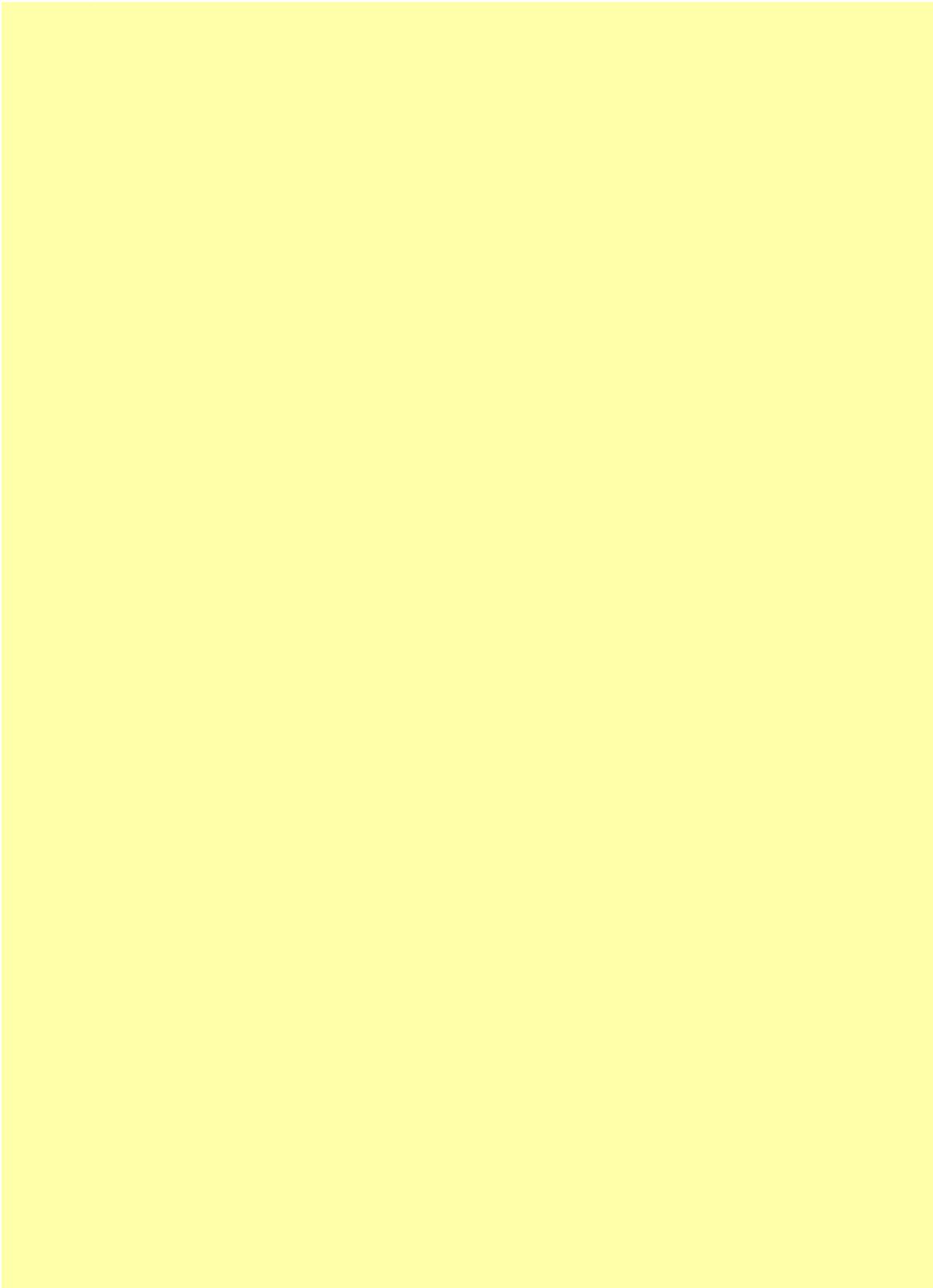
Appendix E
The SSI Review Analyst SOP Checklist and Style Guide

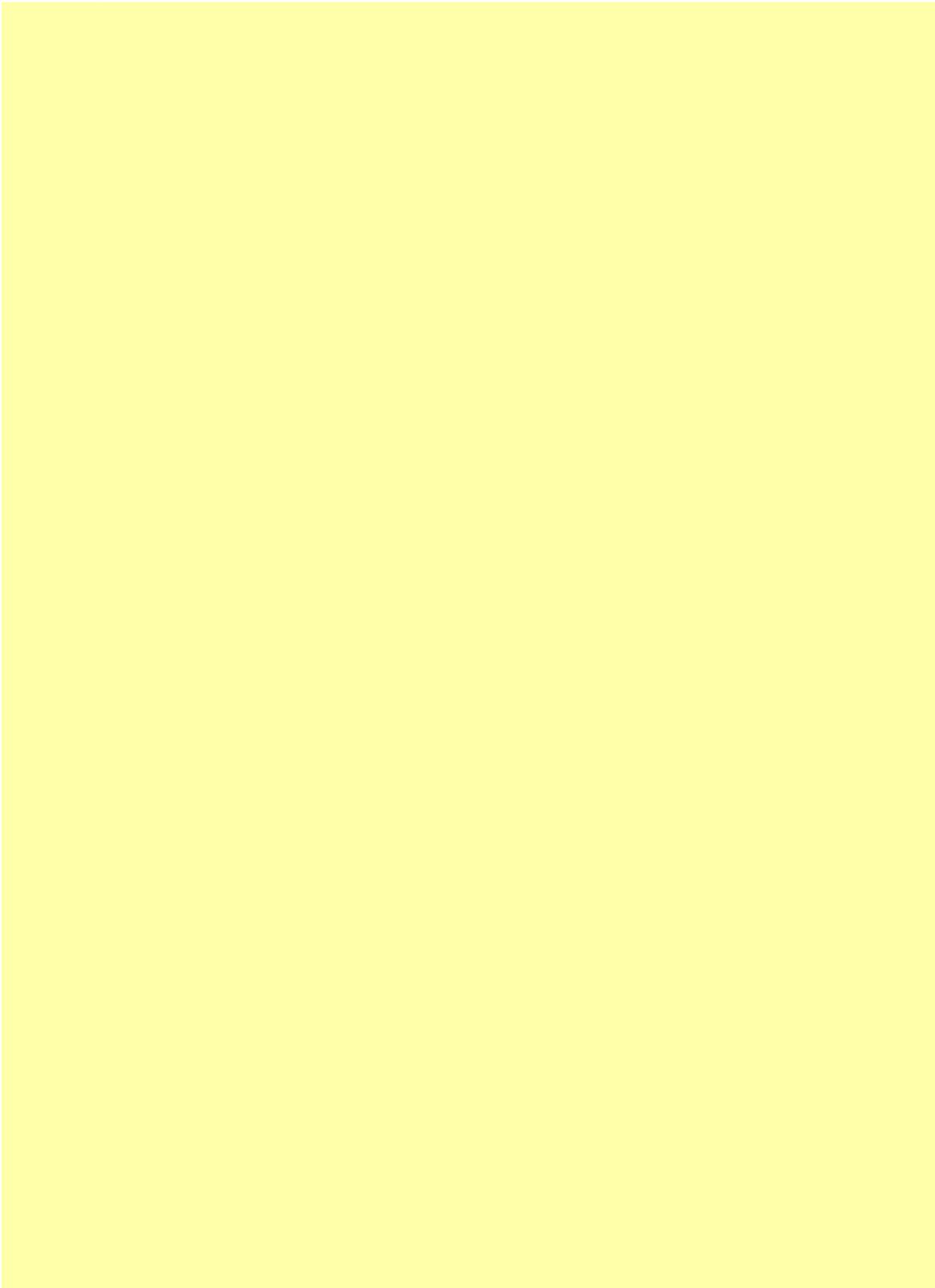


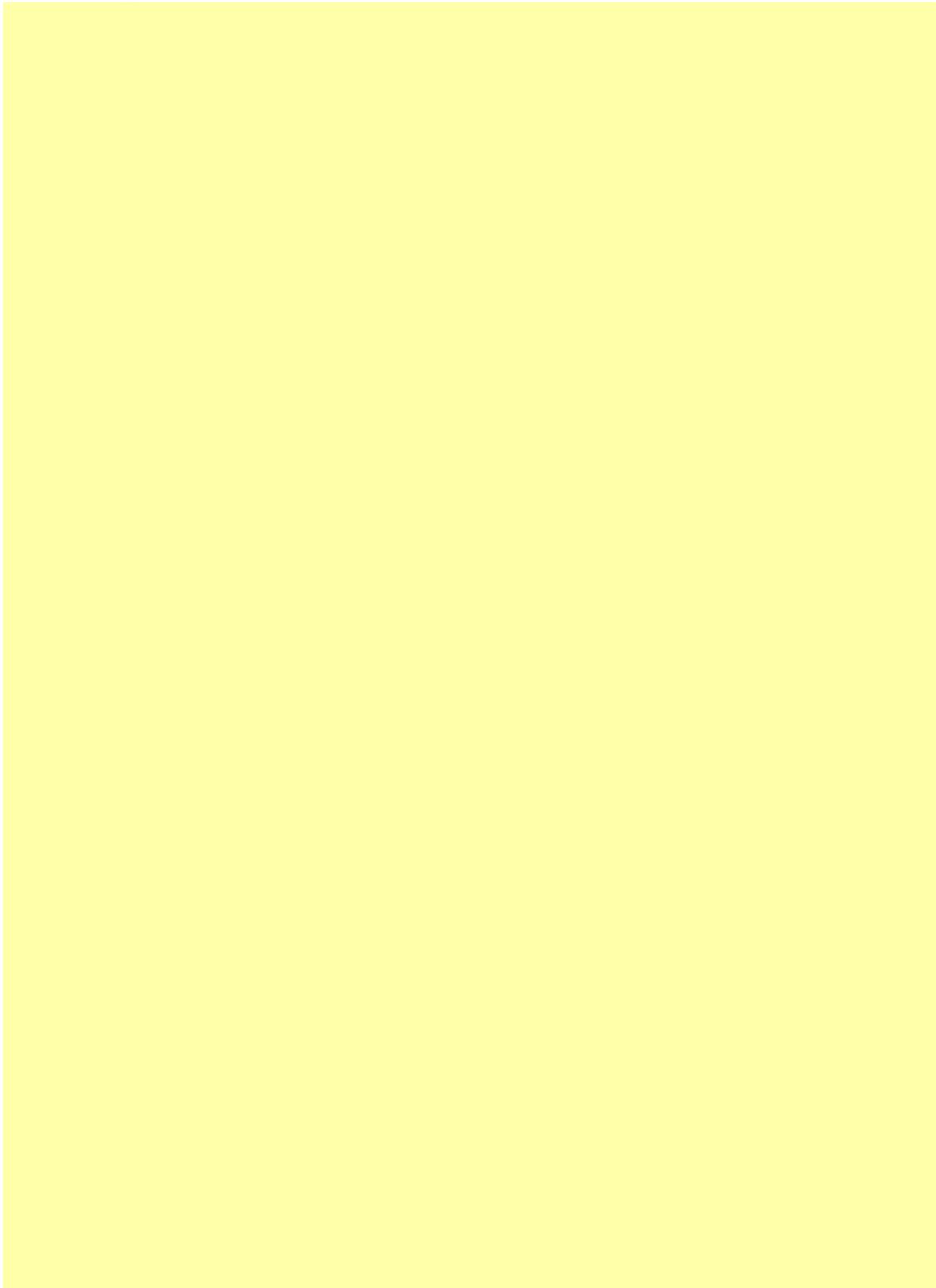
Appendix E
The SSI Review Analyst SOP Checklist and Style Guide

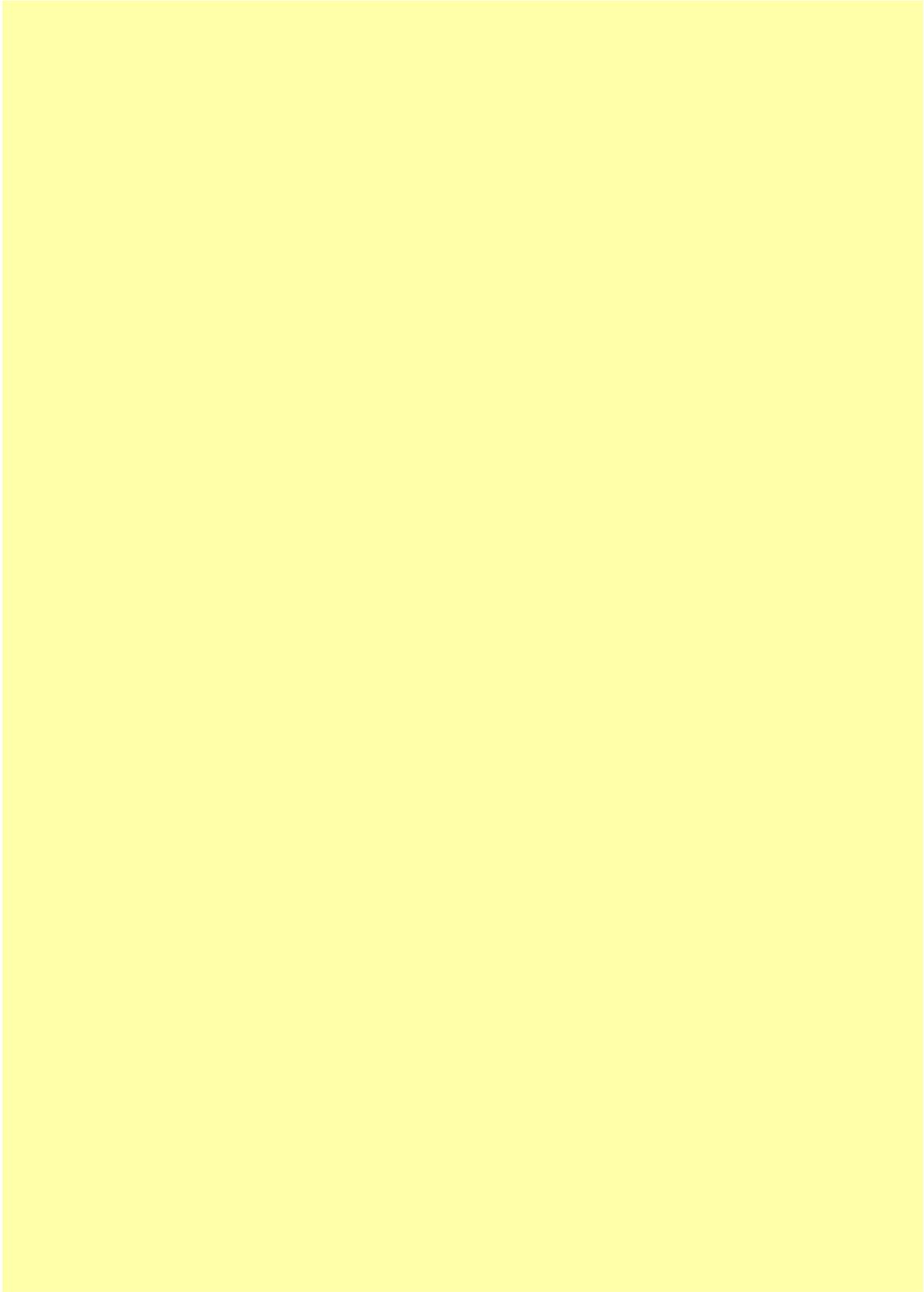


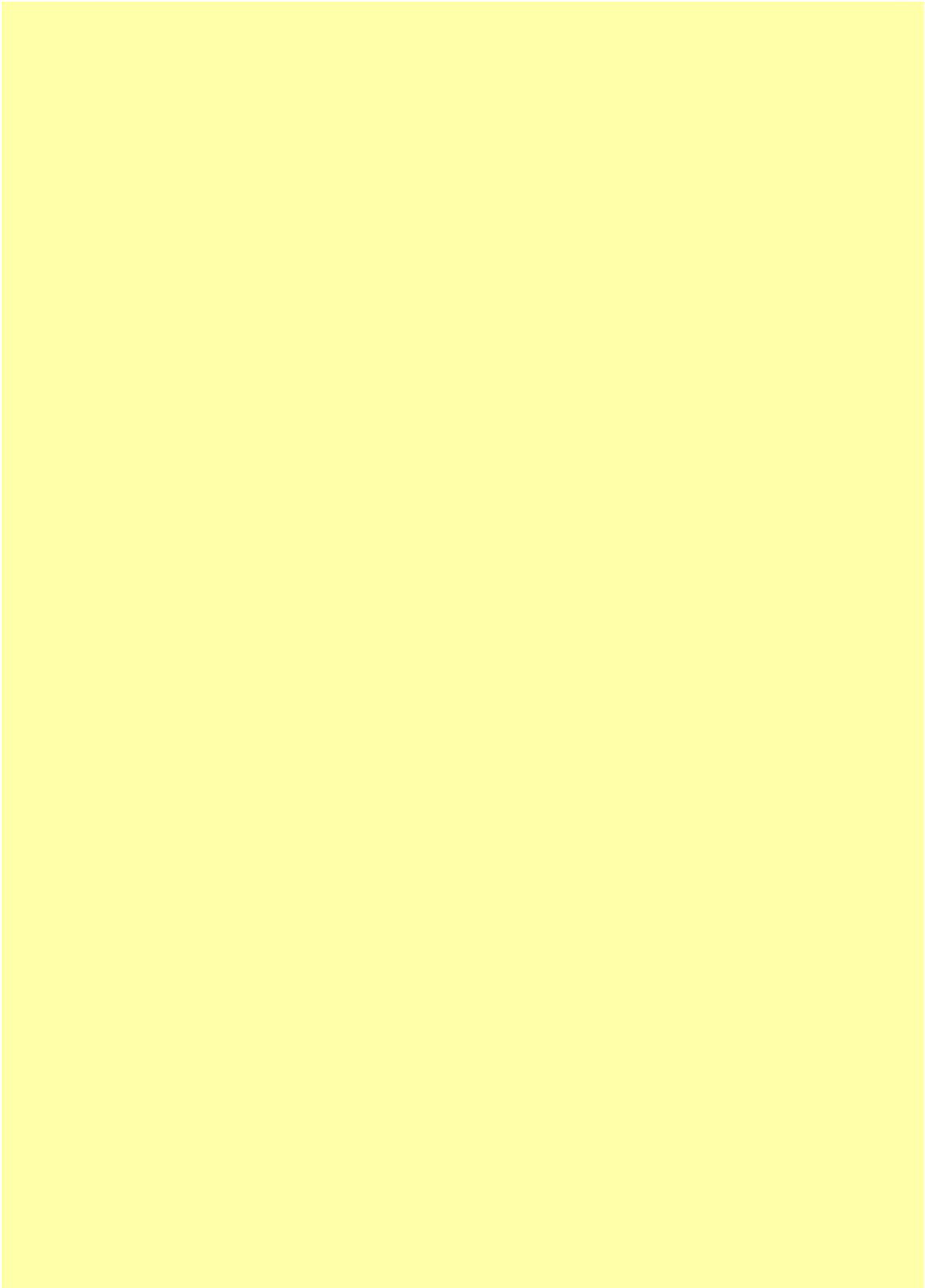


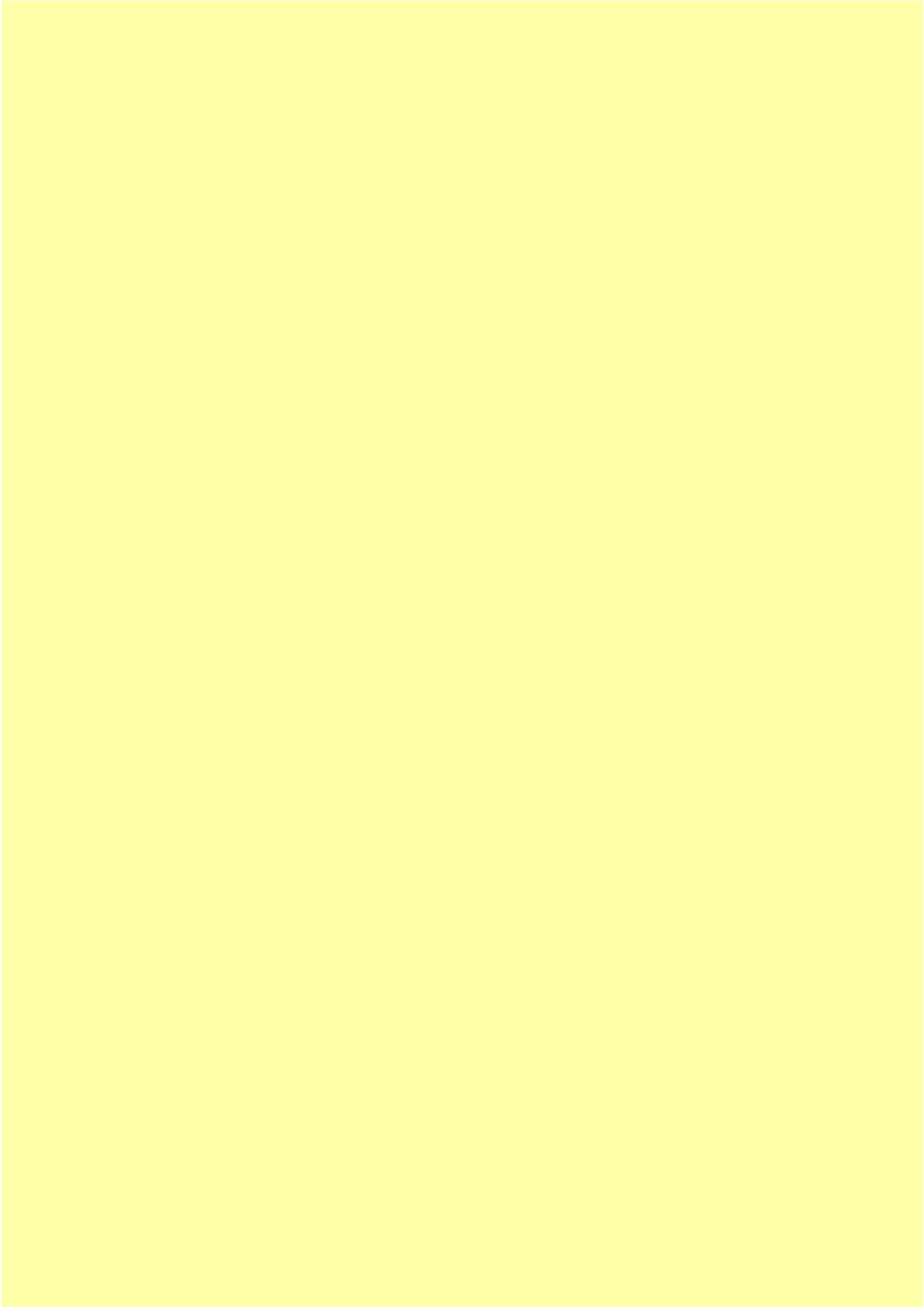




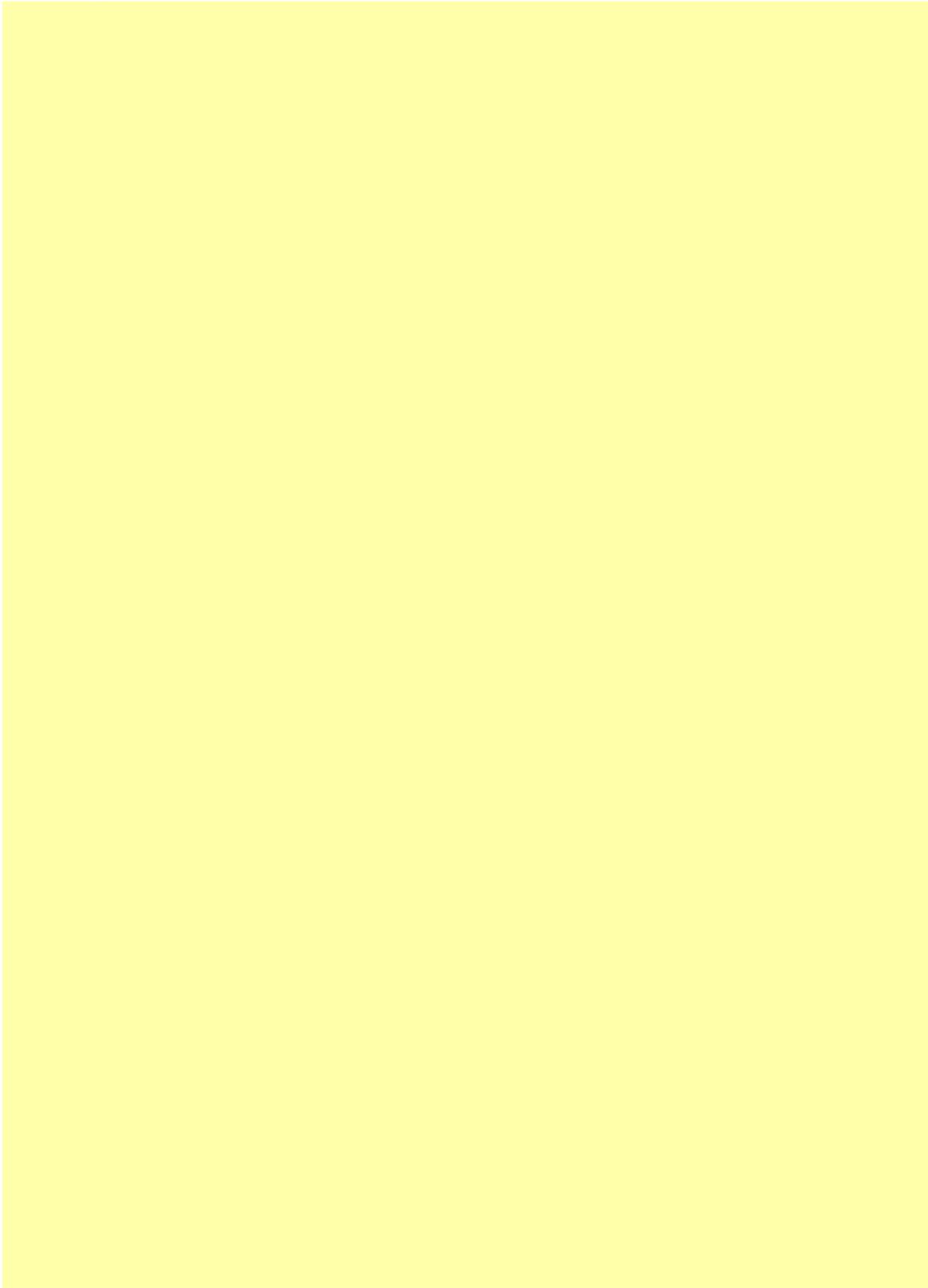


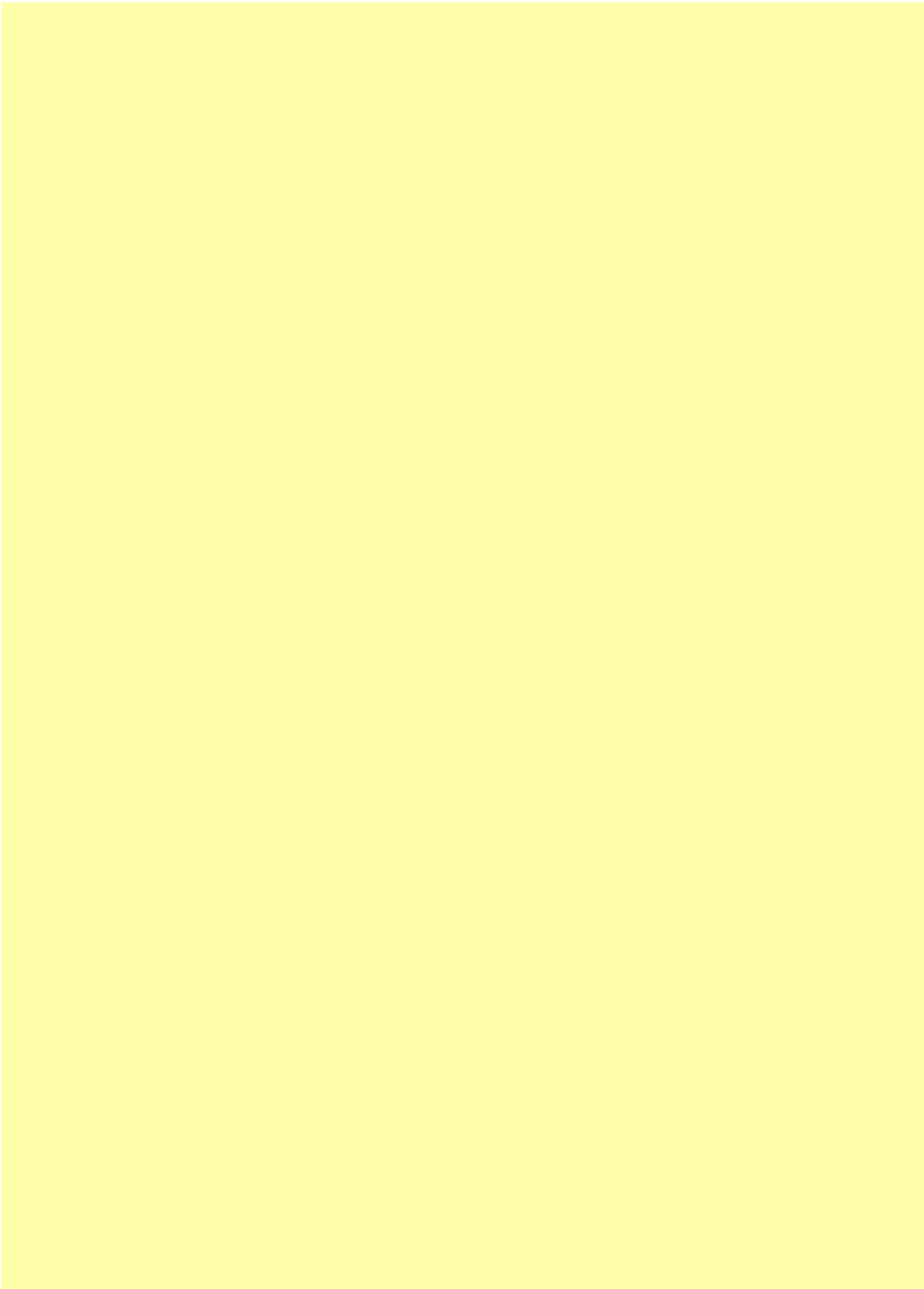


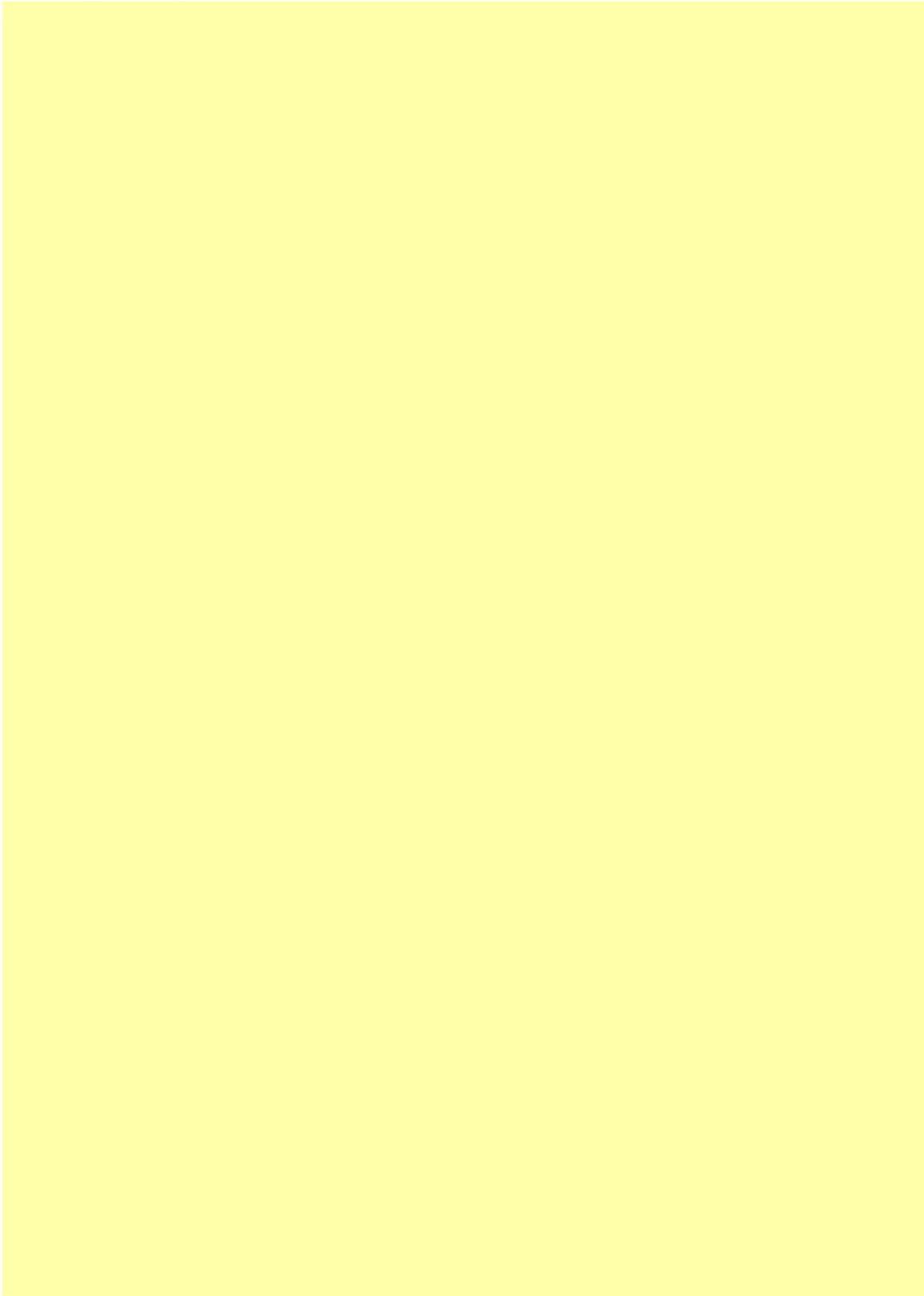




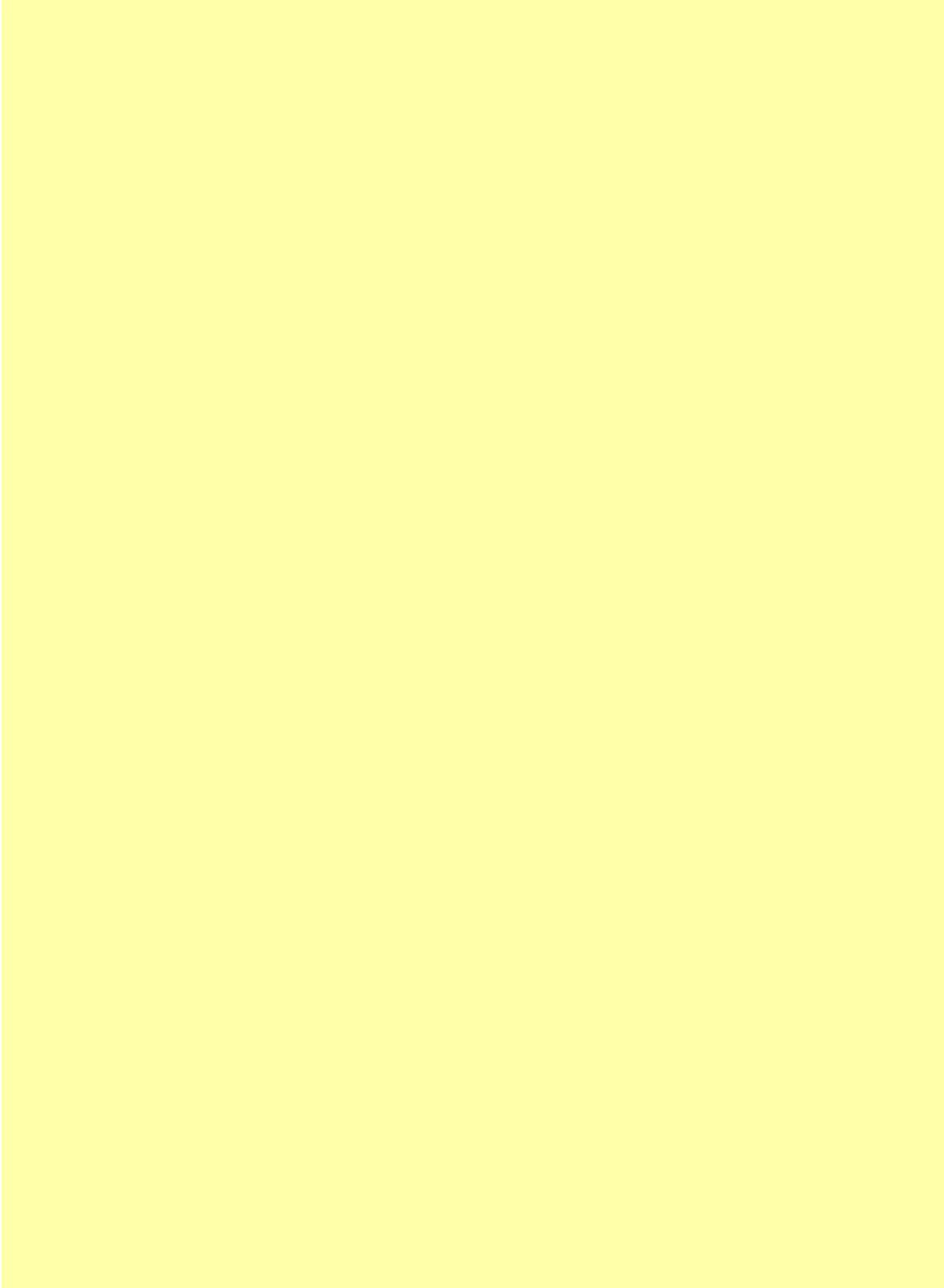
Appendix E
The SSI Review Analyst SOP Checklist and Style Guide

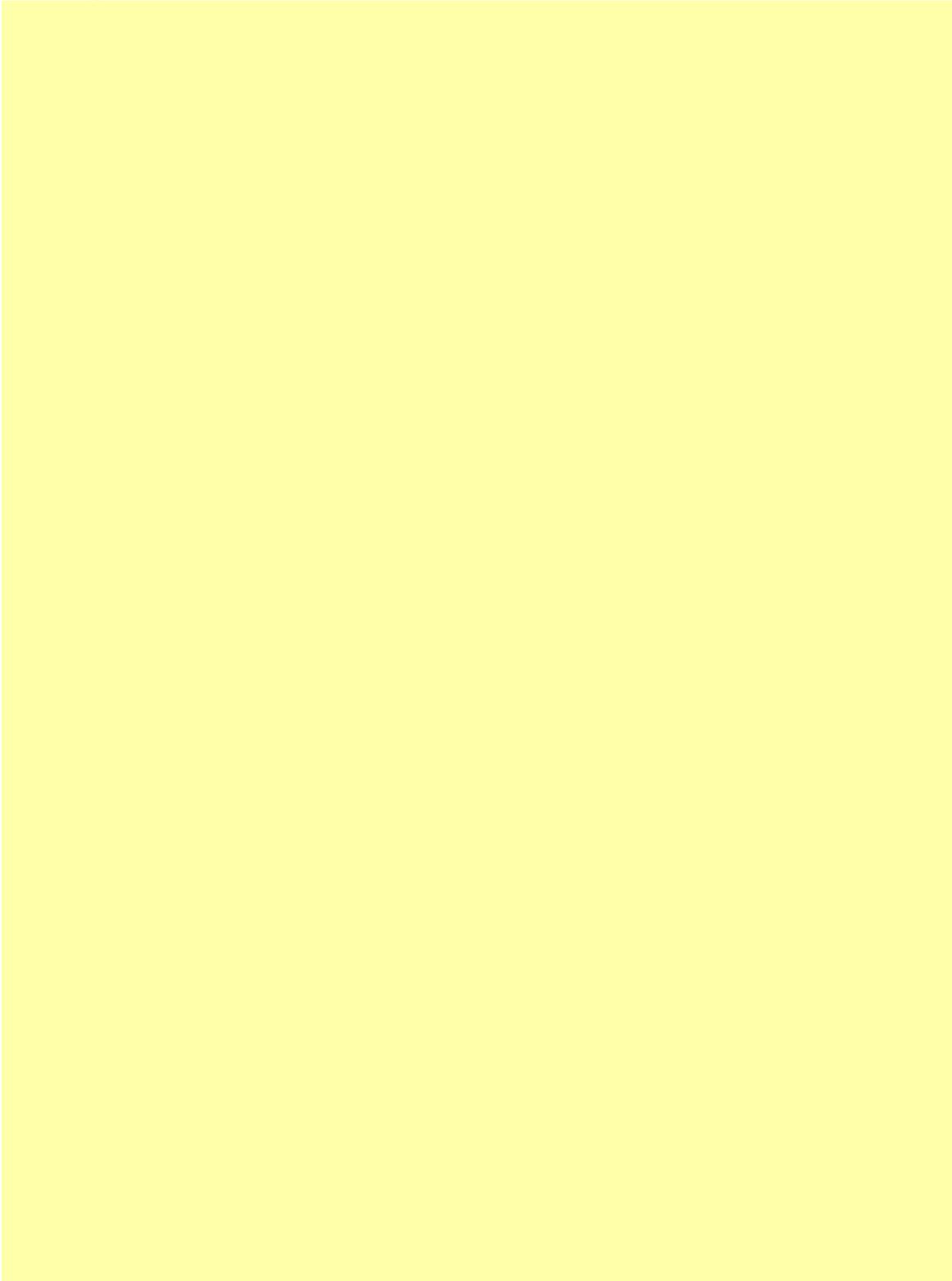






Appendix E
The SSI Review Analyst SOP Checklist and Style Guide

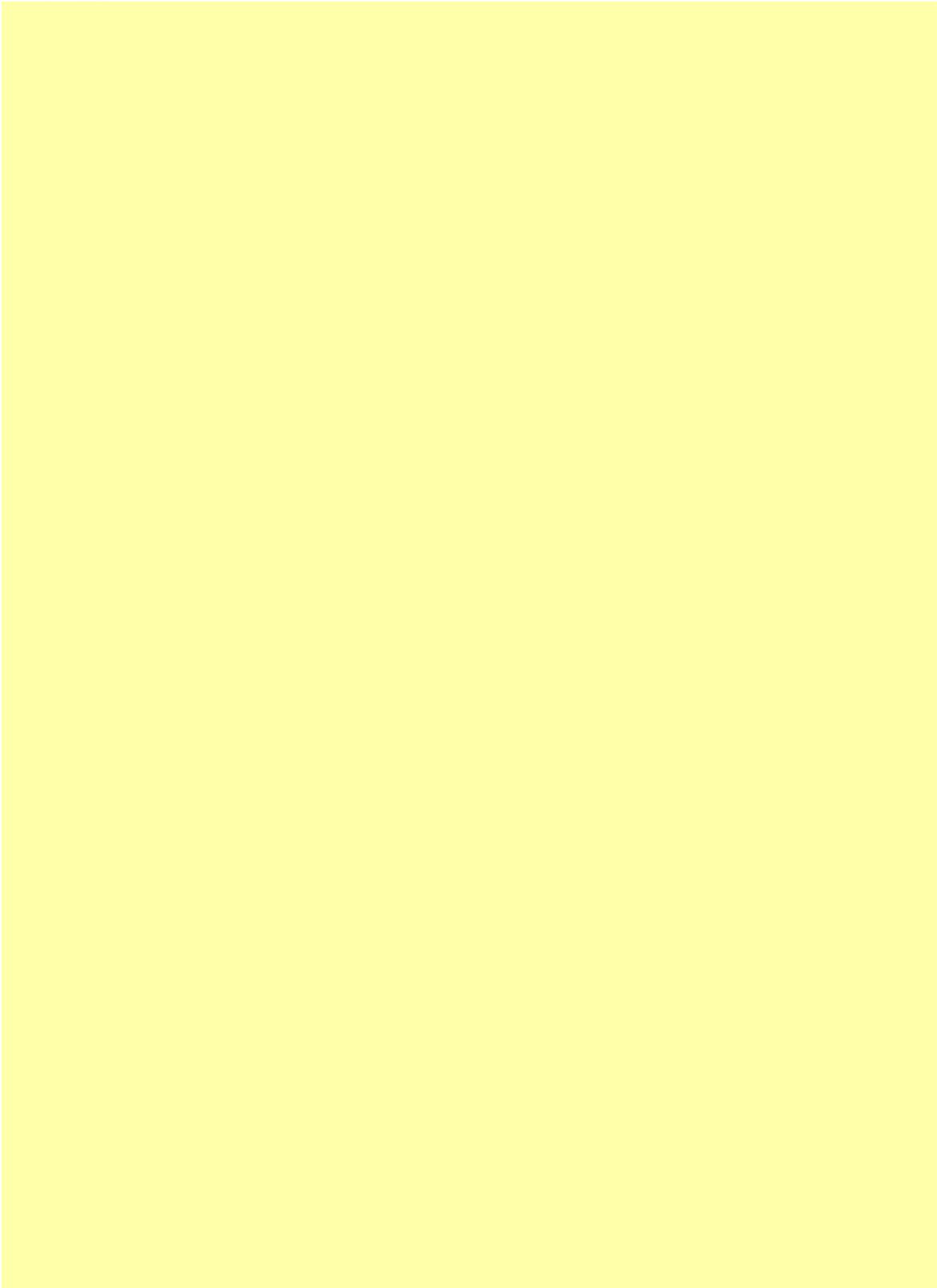




Appendix E
The SSI Review Analyst SOP Checklist and Style Guide



Appendix E
The SSI Review Analyst SOP Checklist and Style Guide



Appendix F
Office of SSI Transmission Email of Redacted Screening Management SOP to the Screening Partnership Program Office

From: [REDACTED]
Sent: Monday, July 07, 2008 3:03 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: INFORMATION: re: review determination - Screening Management SOP
Importance: High

[REDACTED]

INFORMATION: After review, it has been determined that the Screening Management SOP DOES CONTAIN SSI material. Attached please find a visibly redacted version that is password protected (current standard PW), a redacted version of the document, and the related findings memo identifying the citations that the SSI should be withheld per 1520.5(b). If you have any additional questions regarding this review, please feel free to contact me directly. Thanks.

[REDACTED]
[REDACTED]
Transportation Security Administration, DHS
Sensitive Security Information Office, Office of the Special Counselor
Telephone # [REDACTED]

Appendix G
Office of SSI Transmission Memorandum of Redacted Screening Management SOP
to the Screening Partnership Program Office

U.S. Department of Homeland Security
Arlington, VA 22202



Transportation
Security
Administration

Subject: R08-0370; SPP_Screening_management_SOP

Date: July 07, 2008

From: [REDACTED], SSI Office, Office of Special
Counselor

To: [REDACTED]

Per your request, the submitted Screening Management SOP has been reviewed for Sensitive Security Information. We did identify Sensitive Security Information within the document. The areas that have been identified, as SSI, should be withheld per the following under 1520.5(b) citations: (8)(i); (9)(i); (9)(iii). A visible redacted (VR) and a redacted (R) version are being provided. These files are protected using the current standard TSA internal password used for SSI documents. This password should not be shared outside of TSA because that would require distributing the password externally, which would result in the password becoming compromised and thus void for internal use. Instead, please distribute those files outside TSA only in hard-copy (paper) form or re-save this file with an idiosyncratic password of your choice that meets TSA's password requirements.

If at any time a question arises regarding the redactions made herein, please feel free to contact us at [REDACTED]

[REDACTED]

Attachments: 4018-0004-001: SPP_Screening_management_SOP

Appendix H Security Screening Standard Operating Procedures – Sensitive Security Information

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 20598-6031



Transportation
Security
Administration

Security Screening Standard Operating Procedures - Sensitive Security Information [49 C.F.R. §1520.5(b)(9)(i)]

Purpose

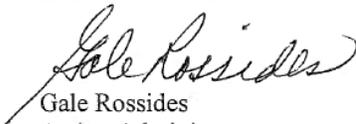
This memorandum addresses the provisions of 49 C.F.R. part 1520 that are applicable to the standard operating procedures (SOP) for the screening of persons, property and cargo.

Policy

In accordance with 49 C.F.R. §1520.5(b)(9)(i) Sensitive Security Information (SSI) includes: "Any procedures, including selection criteria and comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other unauthorized person."

Determination

Pending further review, all screening SOPs are SSI in their entirety in accordance with 49 C.F.R. §1520.5(b)(9)(i). All SOPs must be marked and handled as SSI in their entirety. Until such review is complete, the attached list of screening SOPs and any other screening SOP, to include any drafts or prior versions of these SOPs, are SSI in their entirety. These SOPs and any portion thereof will only be released to covered persons who have a need to know in accordance with 49 C.F.R. §§ 1520.7 and 1520.11.


Gale Rossides
Acting Administrator

December 8, 2009

Attachment

Appendix H
Security Screening Standard Operating Procedures – Sensitive Security
Information

ATTACHMENT



Appendix I
Inventory of SSI Documents and Proper Handling Guidance

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 20598



**Transportation
Security
Administration**

December 8, 2009

MEMORANDUM FOR: Assistant Administrators
Chief Counsel
Special Counselor

FROM: Gale D. Rossides 
Acting Administrator

SUBJECT: Inventory of SSI Documents and Proper Handling Guidance

This memo is to reiterate my earlier direction that each of you complete an inventory and assessment of all documents that have been publicly released by your offices to ensure that any SSI information is properly protected. It is critical that our employees know how to properly redact SSI and other protected material from documents available to the public. This is an individual and team responsibility, and very critical for the success of our mission.

As a result, all offices are required to report their inventories to the Chief Information Officer (CIO). I have asked the CIO to compile an accurate accounting of where SSI is posted, who has access to it, and assurances it is properly protected. Please provide your inventory to the CIO by Friday, December 11 and in collaboration with the CIO, complete the assessment of all documents.

In addition, the CIO is directed to develop specific guidance to ensure your offices have the most updated tools and information to protect sensitive information.

I take this matter very seriously and I hold all of you responsible for exercising the utmost care in securing and processing sensitive information of all types.

Appendix J
Major Contributors to this Report

Marcia Moxey Hodges, Chief Inspector, Department of Homeland Security, Office of Inspector General, Office of Inspections

Angela Garvin, Senior Inspector Department of Homeland Security, Office of Inspector General, Office of Inspections

McKay Smith, Inspector, Department of Homeland Security, Office of Inspector General, Office of Inspections

Anne Ford, Inspector, Department of Homeland Security, Office of Inspector General, Office of Inspections

Jordan Brafman, Inspector, Department of Homeland Security, Office of Inspector General, Office of Inspections

Office of Inspector General, Office of Investigations, Washington Field Office

Office of Inspector General, Office of Information Technology

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Deputy Chiefs of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Administrator for the Transportation Security Administration
Chief Privacy Officer
Under Secretary for Management
TSA Audit Liaison
Privacy Office Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate



ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

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

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

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