AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

HAS THE TSA BREACH JEOPARDIZED NATIONAL SECURITY? AN EXAMINATION OF WHAT HAPPENED AND WHY

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

DECEMBER 16, 2009

Serial No. 111–49

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

56–188 PDF WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
ANN KIRKPATRICK, Arizona
BEN RAY LUJÁN, New Mexico
WILLIAM L. OWENS, New York
BILL PASCRELL, JR., New Jersey
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
JAMES A. HIMES, Connecticut
MARY JO KILROY, Ohio
ERIC J.J. MASSA, New York
DINA TITUS, Nevada

PETER T. KING, New York
LAMAR SMITH, Texas
MARK E. SOUDER, Indiana
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
PETE OLSON, Texas
ANH "JOSEPH" CAO, Louisiana
STEVE AUSTRIA, Ohio

I. LANIER AVANT, *Staff Director*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

SHEILA JACKSON LEE, Texas, *Chairwoman*

PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
ANN KIRKPATRICK, Arizona
BEN RAY LUJÁN, New Mexico
EMANUEL CLEAVER, Missouri
JAMES A. HIMES, Connecticut
ERIC J.J. MASSA, New York
DINA TITUS, Nevada
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

CHARLES W. DENT, Pennsylvania
DANIEL E. LUNGREN, California
PETE OLSON, Texas
CANDICE S. MILLER, Michigan
STEVE AUSTRIA, Ohio
PETER T. KING, NEW YORK *(Ex Officio)*

MICHAEL BELAND, *Staff Director*
NATALIE NIXON, *Deputy Chief Clerk*
JOSEPH VEALENCIS, *Minority Subcommittee Lead*

CONTENTS

Page

STATEMENTS

The Honorable Sheila Jackson Lee, a Representative in Congress From the State of Texas, and Chairwoman, Subcommittee on Transportation Security and Infrastructure Protection 1
The Honorable Charles W. Dent, a Representative in Congress From the State of Pennsylvania, and Ranking Member, Subcommittee on Transportation Security and Infrastructure Protection 5
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Chairman, Committee on Homeland Security .. 8

WITNESSES

Ms. Gale Rossides, Acting Administrator, Transportation Security Administration, Department of Homeland Security:
Oral Statement 9
Prepared Statement 11

FOR THE RECORD

The Honorable Charles W. Dent, a Representative in Congress From the State of Pennsylvania, and Ranking Member, Subcommittee on Transportation Security and Infrastructure Protection:
Statement of the Federal Law Enforcement Officers Association 5
Letter From Honorable Charles W. Dent and Honorable Gus M. Bilirakis, December 11, 2009 7

HAS THE TSA BREACH JEOPARDIZED NATIONAL SECURITY? AN EXAMINATION OF WHAT HAPPENED AND WHY

Wednesday, December 16, 2009

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND
INFRASTRUCTURE PROTECTION,
Washington, DC.

The subcommittee met, pursuant to call, at 2:16 p.m., in Room 311, Cannon House Office Building, Hon. Sheila Jackson Lee [Chairwoman of the subcommittee] presiding.

Present: Representatives Jackson Lee, Thompson, Cleaver, Himes, Dent, Lungren, and Austria.

Also present: Representative Bilirakis.

Ms. JACKSON LEE [Presiding]. The subcommittee will come to order.

Let me acknowledge the presence of the Chairman of the full committee, Mr. Thompson of Mississippi, and Ranking Member, Mr. Dent of Pennsylvania.

Let me welcome those who are here and take a moment of personal privilege to acknowledge the family of Mr. Ed Kelly, who, in this business, is considered family.

Many of us gathered after 9/11 in our respective positions. Members of this committee gathered as Members of the Select Committee on Homeland Security. Many of us were there from the start. Mr. Kelly, comfortably retired, having served as part of the excellence of corporate America, decided to render that, if you will, for another day and accepted the call to become part of the fighting men and women who serve in the Department of Homeland Security. We owe him an enormous debt of gratitude for his service.

I was privileged to join my colleagues, Mr. Chairman, Mr. Dent, the full committee Ranking Member, Mr. King, to send a letter of sympathy and was additionally privileged to rise to the floor of the House to be able to give him the tribute that he deserves as an American hero.

I would like to have, if I am indulged with unanimous consent, to have his family stand at this time so that they might be acknowledged by all of us.

[Applause.]

I believe that is Mrs. Kelly, Ed Kelly's sister, and niece who are present with us today. Thank you all so very much for your presence here.

The subcommittee is meeting today to receive testimony on TSA's inadvertent disclosure of security information related to airports. Our witness will help us to assess what transpired and lay the groundwork for ensuring that this never happens again.

Remember, the title of this hearing is, "Has the TSA Breach Jeopardized National Security? An Examination of What Happened and Why."

That is our task, and that is our duty, to protect the homeland. The way to do that is to determine what and why and to say, "Never again."

I now recognize myself for an opening statement. Before I do that, we will have aired a film that has been presented previously on network television.

[Begin video clip.]

Mr. ORR. The breach reveals some of the Government's most sensitive aviation security secrets. The 93-page manual prepared for Federal airport screeners shows samples of law enforcement and official credentials—Federal air marshals, CIA officers, and Members of Congress—IDs which criminals or terrorists could copy.

The document also reveals travelers from a dozen countries—including Cuba, North Korea, Somalia, and Yemen—are always subjected to extra screening.

The Transportation Security Administration says the security playbook, prepared in May of 2008, is out of date and the sensitive methods have been updated six times, adding in a statement, "TSA is confident screening procedures currently in place remain strong."

Still, the TSA never meant for this information to be public. Each page of the report carries this notice, "Warning: This record contains Sensitive Security Information. No part may be disclosed without a need to know."

The TSA says the whole report was improperly posted by the agency on a Government jobs site, with redactions.

But Wired Magazine editor John Abell says savvy bloggers easily restored the blacked-out test.

Mr. ABELL. Clearly, this was a rookie mistake, so let's just call this a very early Christmas present to the kinds of people that traffic in this kind of secret information.

Some of the compromised information is just routine common sense: "An on-duty airport-assigned law enforcement officer may be cleared without undergoing screening."

But other guidance may be less intuitive. For example, searches for explosive residue are not required for wheelchairs, prosthetic devices, and orthopedic shoes.

The TSA is investigating and says it takes the failure seriously. But critics say, with aviation a known terrorist target, it is a little late to get serious.

Mr. ORR. Bob Orr, CBS News, Washington.

[End video clip.]

Ms. JACKSON LEE. The only early Christmas present that terrorists will get will be the resolve of the men and women of the Department of Homeland Security, the President of the United States, and the men and women of the United States Congress. That is why we are here today, to ensure that going forward in this holiday

season we have the opportunity to cure quickly the unfortunate and vast mistake that has been made.

So I hope, as we proceed in this hearing, we will hear that steps are being taken to ensure the safe travel of the families who will be visiting their families during what I hope will be a very happy holiday season.

We are here today, as well, to discuss last week's revelation that a TSA manual containing Sensitive Security Information was posted by TSA on the internet without proper technical safeguards. As a result, sensitive information about our airports and screening policies was made available for the world to see.

My colleagues and I were alarmed by this development, as it sent shockwaves across Capitol Hill. This subcommittee takes its oversight of TSA very seriously; after all, TSA was constructed to help protect the American people from the very type of events that transpired on September 11, 2001.

When events, such as last week's, are made public, it becomes all too clear that more must be done and that TSA must keep its eye on the ball. We must also be assured that contractors of varying types are, again, vetted, trained, questioned, queried, and if necessary, be part of the inquisition, because the security of America is paramount.

Today, we will be evaluating how this happened, the security ramifications of this misstep, and how we are going to avoid similar lapses in the future, and as well, to ensure that those missteps, if they can be characterized as such, do not, in fact, jeopardize the National security of the American people.

Before we go further, let me be clear that, although this was a serious breach in the management of sensitive information, I have been assured by TSA that additional personnel and procedures have been put in place at airports across the country to ensure the safety of the traveling public.

In essence, terrorists, watch out. Any terrorist group or individual wishing to exploit this situation should be aware and beware that the United States will continue to use all available resources to protect the flying public. During this busy holiday season, the American people should know that it is safe to fly, along with the courtesies that we expect to be offered by the Transportation Security Administration officers, we do expect for them to do their duty.

Last week, Chairman Thompson and I sent a letter to TSA urging a third-party review of this incident. I am happy to learn that Secretary Napolitano responded and requested that the inspector general investigate, take over completely, and provide recommendations regarding this incident. I look forward to a quick and immediate response.

In addition, I commend TSA for taking steps in response to this incident. For example, I have been informed by TSA that five people have been placed on administrative leave. This subcommittee, however, also needs assurance that TSA is reviewing its processes for handling and posting of Sensitive Security Information and making a full inventory search of all of its staff around these issues and ensuring that this is not permeated beyond the five that were engaged in this unfortunate set of circumstances.

Questions we have include: Who is in TSA's management—who in TSA's management is ultimately responsible for this process? Is there a manual for training employees on how to post such information? What is the role of contract employees in the handling and disseminating of sensitive security? What new steps are being put in place to vet those individuals on their training, their instincts, their knowledge, and as well, their ability to adhere to rules and safety precautions? Is there sufficient training for contract employees?

I would also like to know how broadly contract employees are solicited, and how far is the reach, and are we using small and minority-owned businesses? Are we using the same ones over and over again, therefore, committing the same mistakes over and over again?

One of the lessons made clear by this incident is that TSA needs permanent, effective leadership. Our witness today, Acting Administrator Rossides, has led TSA during a very active year, and we thank her for her service. But the person nominated by the President to lead TSA, Mr. Erroll Southers, has had his confirmation held up in the Senate.

Let me be very clear: We understand the duties and the constitutional privileges of the Senate, advise and consent. But what they are engaging in, in a partisan, one-sided approach is jeopardizing the security of the American people. We need action on his nomination immediately, and I hope all stakeholders will also call for his swift confirmation. Our homeland security efforts can no longer afford delay.

On a personal note, I have already mentioned the passing of a TSA family member. But, again, as I close, let me acknowledge that Ed Kelly managed TSA's cargo screening program and testified before this subcommittee just this past March. Ed was an incredibly dedicated individual and a consummate professional who left retirement, as I said, after September 11 attacks in order to work on behalf of our Nation's homeland security efforts.

Many in the industry said that he reformed the industry. He made leaps and bounds of change and outstanding contributions to the security of America.

Again, on behalf of the subcommittee Members and staff, my condolences are expressed to his family and to his colleagues at TSA.

Finally, I would like to point out that this subcommittee understands the enormity and importance of TSA's mission and the dedication of its employees, but after last week's announcement about the disclosure—and, unfortunately, other incidences—I think we can all agree that TSA can do better, and that is why we are here today. After a complete analysis of this incident, we will determine how to make the agency and its employees perform better and give the American people more confidence in the TSA.

I am considering legislation that will help provide a firewall over the issuance and distribution of data like this, along with additional oversight on contractors and the utilization of them.

Without objection, the Chairwoman is authorized to deem the subcommittee resolved into Executive Session to receive additional testimony, if necessary.

Hearing no objection, it is so ordered.

The Chairwoman now recognizes the Ranking Member, the gentleman from Pennsylvania, Mr. Dent, who, by the way, joined this in his sympathies for Mr. Kelly, but I also note that Mr. Kelly has come from his region, if not his particular district.

Mr. Dent, you are now recognized for your opening statement.

Mr. DENT. Thank you, Madam Chairwoman.

I, too, want to add my condolences and sympathies to the Kelly family. Ed was a wonderful public servant, served the Department of Homeland Security so well and this Nation so well, and our sympathies—I know I am speaking not only on my behalf, but on behalf of the entire community in expressing our condolences to his wife, Ann, his sister, Rosemary, and I believe his niece, Elizabeth, is here, as well, so, again, from all of us, our heartfelt condolences.

Again, thanks, Madam Chairwoman. For one thing, too, I note the family has a strong connection to northeastern Pennsylvania, Lake Ariel, and a very special place for the family and for many of us who know Pennsylvania well.

Again, Madam Chairwoman, I just want to thank you for holding this important hearing today. I agree that the TSA's disclosure of this Sensitive Security Information is, indeed, unfortunate, and I would add that, based on my review of the situation, TSA's mistake has undoubtedly weakened our aviation security.

While we have many layers in our aviation security processes, some of those layers have been exposed after having the aviation security screening management's standard operating procedures posted on a public website for the past 9 months. I agree with comments made last week from the Federal Law Enforcement Officers Association, which stated, "Air marshals and TSOs proudly shoulder considerable risk by virtue of their jobs. Their agency should not compound this risk with flawed internal controls and dismissive excuses."

I ask unanimous consent to include their statement in the record. Madam Chair, I would like to ask unanimous consent to include their statement in the record.

Ms. JACKSON LEE. Without objection, so ordered.

[The information follows:]

STATEMENT OF THE FEDERAL LAW ENFORCEMENT OFFICERS ASSOCIATION

DECEMBER 9, 2009

Today, J. Adler, National President for the Federal Law Enforcement Officers Association (FLEOA) announced that he is asking House Homeland Security Chairman Bennie Thompson to hold a private hearing on TSA HQ'S security breech. According to Adler, "Both TSA's posting of sensitive security information and their unwillingness to grasp the seriousness of this are unacceptable. A discreet hearing should be held so Congress can determine why TSA posted this information, and why TSA attempted to minimize the importance of the information as "outdated." The so-called "outdated" information should not be recklessly discounted like a college textbook that is last year's edition.

Unfortunately, in response to this serious unwarranted disclosure, TSA HQ has offered more "layers" of excuses than assurances of protection. Contrary to their efforts to deflect their responsibility for making a serious security breach, they do not have sound security procedures in play. What they have is a dedicated workforce that is tasked with overcompensating for a flawed system. Air Marshals and TSO'S proudly shoulder considerable risk by virtue of their jobs; their agency shouldn't compound this risk with flawed internal controls and dismissive excuses. Furthermore, the careless posting of information pertaining to law enforcement officers flying armed only serves to compromise their safety.

FLEOA takes great exception to the remarks attributed to former TSA Administrator Edmund "Kip" Hawley. His suggestion that no one should "hyperventilate" over the breach is offensive and epitomizes the hypocrisy of his tenure at TSA. To wit, he unfortunately did not hyperventilate when an external hard drive containing employee personnel data disappeared. Instead, he condoned management's pursuit and termination of dedicated Air Marshals who disclosed serious officer safety issues to the news media. One can only conclude that TSA HQ has their own set of rules that exempts them from accepting responsibility for serious security disclosures.

FLEOA expects Chairman Thompson and Ranking Member King will embrace the seriousness of the disclosure, as well TSA'S propensity for managing by double-standard. TSA HQ should be held accountable for this breach, and a discreet, closed-door hearing would be the appropriate forum to properly address this serious matter. FLEOA is confident that the committee will be able to persuade TSA HQ to conduct a comprehensive review of this situation, and provide them with a meaningful damage-control assessment.

Mr. DENT. As terrible as this—as the very public nature on which TSA's mistake was disclosed, I am pleased that we know the mistake was actually made in the document was accidentally released. Now TSA has an opportunity to learn from that mistake. The question is, will they?

Ms. Rossides, I am confident that TSA will.

While I understand that people make mistakes, my review of this incident over the course of the past week has led me to one simple conclusion: This was not the failure of an individual, but rather that of a failure of a system.

An individual in TSA's SSI review office failed to comply with the National Security Agency's processes for electronically redacting sensitive information. That individual's supervisors failed to notice it. The Office of Acquisition failed to review the document before posting it on the General Services Administration's FedBizOpps website. Finally, management failed to ask why it was necessary to post a security-related document on-line for a contract and failed to consider viable alternatives.

On his second day in office, President Obama said, "Transparency and the rule of law will be the touchstones of this presidency." Why then, after more than a week of phone calls, e-mails, letters, and in-person requests does this committee still not have the most recent version of the standard operating procedures? Section 114(r)(2) of Title 49, United States Code, specifically states that designating a document as Sensitive Security Information does not authorize information to be withheld from a committee of Congress authorized to have the information. That is what the code says.

While I appreciate that my staff was given a 1-hour meeting with an additional hour to review the most recent version of the standard operating procedures, that is not particularly transparent, in my view. After 4 days of asking nicely for the SOPs, Ranking Member Bilirakis and I authored a letter to Ms. Rossides insisting she provide the committee the document. Again, I ask unanimous consent to introduce that letter into the record.

Ms. JACKSON LEE. Without objection, so ordered.

[The information follows:]

LETTER FOR THE RECORD SUBMITTED BY HONORABLE CHARLES W. DENT

DECEMBER 11, 2009

Ms. Gale Rossides,
Acting Administrator, Transportation Security Administration, 601 South 12th Street, Arlington, VA 28598

DEAR ACTING ADMINISTRATOR ROSSIDES: We are writing to formally request an immediate copy of the most current version of the Transportation Security Administration's (TSA's) Aviation Security Screening Management Standard Operating Procedures. The TSA has repeatedly ignored our requests for this document since Tuesday, December 8th. TSA's unwillingness to provide the document is unproductive and a violation of law,

We would remind you that while section 114 of Title 49, United States Code, authorizes the Transportation Security Administration to issue regulations protecting sensitive security information from public disclosure, that same provision specifically states that it "does not authorize information to be withheld from a committee of Congress authorized to have the information."[1] We would further remind you that pursuant to House Rule X(i) of the Rules of the House of Representatives, the Committee on Homeland Security oversees "overall homeland security policy" and "transportation security." As such, the law explicitly prohibits TSA's dilatory tactics.

As you are aware, in addition to our review, the Subcommittee on Transportation Security and Infrastructure Protection will be holding a hearing on TSA's improper disclosure of sensitive airport screening procedures on Wednesday, December 16, 2009. The Subcommittee needs sufficient time to review the current version of the released document to gauge the real impact of TSA's security failure.

Thank you for your immediate and personal attention to this matter.

Sincerely,

CHARLES W. DENT,
Ranking Member, Subcommittee on Transportation Security and Infrastructure Protection.

GUS M. BILIRAKIS,
Ranking Member, Subcommittee on Management, Investigations, and Oversight.

Mr. DENT. Thank you, Madam Chairwoman.

In the end, you know, a lot of things went wrong, but a lot of things are now going right. I understand TSA is taking some risk mitigation measures and has taken some immediate common-sense actions to prevent any further disclosures. I would hope to the extent possible you could highlight some of these during your testimony this afternoon.

Finally, to those who re-posted this security information on the internet, you should share in the blame should security be breached as a result of this disclosure. In the future, I would ask that you please, please use the whistleblower process Congress has created for you. Call the Department. Call the inspector general. Call Congress and its committees. But, please, do not circulate sensitive security documents. Rest assured, we will hold the Department to account.

Ms. Rossides, I want you to know that I continue to believe that the men and women of TSA, including yourself and your staff, are giving your best efforts to improve the security of the traveling public. While the accidental disclosure was certainly disappointing and the lack of transparency provided by this administration is frustrating, I am committed to working with you to improve the Transportation Security Administration and the services it provides to our traveling public.

With that, I would yield back the balance of my time.

Ms. JACKSON LEE. I thank the gentleman for yielding back.

[1] 49 USC § 114(r)(2).

It is my privilege to acknowledge and recognize the Chairman of the full committee, the gentleman from Mississippi, Mr. Thompson, for an opening statement. Mr. Chairman.

Mr. THOMPSON. Thank you very much. Madam Chairwoman, I appreciate the holding of this hearing.

I would also like to take the opportunity to express my condolences to the Ed Kelly family, as well as his TSA colleagues who are here. Ed was a dedicated public servant, and his efforts in the cargo security will never be forgotten.

There is no doubt that the events that transpired last week raise several questions about TSA's operational procedures and practices in handling sensitive information. Perhaps more importantly, this incident also raises concerns about the security of our entire transportation system.

No actions, legislation, or press statement can undo the disclosure of this information. However, we can learn from this incident and move forward with security measures that ensure sensitive information will not be made available to the public.

The events from last week serve as a reminder of how critical it is to have accountability at the Department of Homeland Security.

I think it was the right decision for Secretary Napolitano to request that the DHS inspector general begin an investigation of this incident. The review and investigation by the inspector general is an important first step in learning the details that will be essential in helping TSA improve procedures for handling and posting sensitive material.

However, as I have said before, to get TSA to improve its operational performance in all program areas and at all levels of management, it is essential that TSA have permanent, effective leadership. The President has nominated Erroll Southers to be TSA administrator, and I think we have waited long enough for his confirmation.

His law enforcement background and operational experience will be essential in improving TSA and strengthening our homeland security efforts. With strong leadership is in place, incidents such as these are less likely to happen.

Nevertheless, today's hearing provides us in Congress with an opportunity to express our concerns and to hear from TSA about what it plans to do. I am sure that we will need follow-up briefings and perhaps another hearing to review the inspector general's report and to assess steps going forward.

Madam Chairwoman, there are some questions that I have after we have heard from our witness that would more or less enlighten us, I think, on this situation. But I am concerned about it. I will express those concerns during the question-and-answer period. I yield back.

Ms. JACKSON LEE. To the Chairman of the full committee, let me also express my appreciation for the astuteness and the detail of which the committee, with you as Chair, and the staff has taken to securing the homeland. I think this committee reflects that, and your cooperation and agreement with this subcommittee's intent to hold a hearing is much appreciated. Again, thank you very much for your leadership.

I wish to recognize—I think both of us are going to speak in tandem here on the gentleman from Florida, Mr. Dent.

Mr. DENT. Madam Chairwoman, I was going to ask unanimous consent that Ranking Member Bilirakis of the Management, Investigations and Oversight Subcommittee be authorized to join us on the dais and ask questions of the witnesses.

Ms. JACKSON LEE. As you ask, I am ordering that Mr. Bilirakis be allowed to sit on this committee and participate with questions through the unanimous consent.

Any objection? So ordered.

Let me acknowledge Mr. Bilirakis' presence, Mr. Austria's presence, and Mr. Cleaver's presence, and thank them for being here today.

Other Members of the subcommittee remind me that under committee rules opening statements may be submitted for the record.

Our witness today, Ms. Gale Rossides, is the acting administrator of TSA. As I indicated previously, we are grateful for her service, her long-standing service. As acting administrator, Ms. Rossides oversees a workforce of 50,000 people and the security operations of 450 federalized airports throughout the USA, as well as the Federal security regime for highways, railroads, ports, and mass transit systems.

Ms. Rossides was one of the six original Federal executives handpicked in 2002 to build TSA. Let me say that deserves commendation, and we thank you for that longevity of service.

Without objection, the witness's full statement will be inserted in the record. I now ask Ms. Rossides to summarize her statement for 5 minutes.

You are recognized for 5 minutes.

STATEMENT OF MS. GALE ROSSIDES, ACTING ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION, DEPARTMENT OF HOMELAND SECURITY

Ms. ROSSIDES. Good afternoon, Chairwoman Jackson Lee, Ranking Member Dent, and Chairman Thompson, and distinguished Members of the subcommittee.

First of all, I want to thank you for recognizing the services of Ed Kelly and his family. He was truly one of our heroes in TSA.

I appreciate your giving me the opportunity today to speak with you about the recent website posting of an improperly redacted version of a management standard operating procedure, or SOP, on a Federal website. I regret this occurred and take full responsibility for this mistake. Our response was swift, decisive, and comprehensive, because our priority first and foremost is the safety of the traveling public.

I want to reassure all Members of this committee and the traveling public that our aviation system is strong and the passengers will fly safely this holiday season and every day because of the layered security system we have in place.

From cutting-edge new technology to retraining our entire workforce to the implementation of new security programs, we have evolved and substantially strengthened security in the year-and-a-half since this document was drafted.

On Sunday, December 6, I became aware that the screening management SOP was posted to the Federal Business Opportunities website without having the Sensitive Security Information, or SSI, properly redacted. The document was an attachment to a screening partnership program contract solicitation.

We took immediate action. I convened a teleconference with TSA's senior executives, and we notified DHS headquarters on Sunday night. Also on Sunday night, we removed the document from the Government website within hours, thanks to prompt work by the General Services Administration.

I then directed TSA's Office of Inspection to immediately begin a review of what happened and how, and that review has since been passed on to the DHS inspector general. Our Security Operations Office conducted an operational assessment of any potential vulnerabilities that this disclosure may have caused. Out of an abundance of caution, we quickly put mitigation measures in place to close any potential gaps.

I directed an audit of sensitive information posted both internally and externally to be conducted by the chief information officer. We consulted with our Federal and law enforcement partners and stakeholders throughout the aviation domain, and all have been tremendously supportive.

There have been numerous and significant changes in our evolving security program that are not contained in the May 2008 version of this SOP.

As a point of reference, this document provides instructions on who and what needs to be screened. It does not include the specific procedures used by our transportation security officers to screen members of the traveling public.

Today, TSA's 12 other standard operating procedures, including the ones that cover an officer's screening procedures, remain secure. The strength of our dynamic security system is in our own people, our technology, our stakeholder partnerships, and our multilayered and complex protocols.

We take this matter very seriously and look forward to the inspector general's report. Our response to their recommendations will also be swift. We will hold individuals accountable as appropriate. At this time, five TSA employees have been placed on administrative leave, pending the outcome of the continued investigation.

This has been a critical incident for TSA, and we have managed it as such. From an exhaustive internal review, we will emerge with stronger internal document control measures for all employees. We will strengthen the electronic processes we use for sharing information. Most importantly, we will continue to evolve our security programs in light of intelligence and our own testing and training regime to ensure the on-going security of the system.

In closing, I want to again assure Members of this committee, the traveling public, and our partners that our Nation's aviation system is strong. We have closed any potential gaps, and we will continue to apply measures that enhance our complex security system.

I am happy to answer your questions and can discuss any sensitive material in the closed session to follow. Thank you.

[The statement of Ms. Rossides follows:]

PREPARED STATEMENT OF GALE D. ROSSIDES

DECEMBER 16, 2009

Good afternoon Chairwoman Jackson Lee, Ranking Member Dent, and distinguished Members of the subcommittee. Thank you for the opportunity to appear today to discuss the recent website posting of an improperly redacted version of a 2008 Transportation Security Administration (TSA) Screening Management Standard Operating Procedure (SOP). I appreciate the subcommittee's continued involvement in the security operations of TSA, and look forward to working closely with Congress in fulfilling our on-going mission to safeguard all sectors of transportation on behalf of the American people.

Let me begin by assuring the Members of the subcommittee and the traveling public that our aviation security procedures remain strong. The duties performed by TSA's dedicated workforce of Transportation Security Officers (TSOs), Federal Air Marshals, canine teams, and others have not been adversely impacted by this incident. TSA will continue to ensure the same high standard of security during the upcoming holiday season that was evident throughout the Thanksgiving Day travel period. Our workforce is responsive, accountable, and dedicated to safeguarding the traveling public, and neither our capability nor our resolve has been diminished by this incident.

Those who seek to infiltrate airport security will find no roadmap from the redacted text that was improperly released. This document, which was outdated, provides procedural information for managers. It is not the SOP used by our TSOs at airport checkpoints to screen members of the traveling public. Because we continually adjust our SOPs and our security protocols based on the receipt of intelligence information and the testing of our security regimen, there have been six newer versions since this SOP was drafted. Our TSO screening procedures have not been compromised, and our multi-layered transportation security system remains intact. Nonetheless, out of an abundance of caution, we have undertaken an operational assessment of any potential vulnerabilities that this disclosure may have caused, and have taken swift action to prevent the information from the SOP from being used to defeat a single point in our multi-layered security system.

That being said, TSA, and I personally, take this incident very seriously. This was a mistake and we are very sorry it occurred. I would like to provide a brief summary of the events surrounding this incident. On Sunday, December 6, TSA's Blog Team learned that a 2008 Screening Management SOP posted on the General Services Administration's (GSA) Federal Business Opportunities website contained redacted information that had not been properly protected. The SOP had been posted by TSA on the GSA contracting website for a contract solicitation under TSA's Screening Partnership Program. Such documents—when properly redacted—are used in contract solicitations to guarantee fairness in the procurement process. Unfortunately, the redaction on this particular document had been performed incorrectly, enabling readers to view the redacted portions as well as the headers and footers indicating that the document contained Sensitive Security Information (SSI).

TSA takes any breach of its security programs very seriously, and we reacted swiftly. I convened a Sunday evening senior staff conference call as soon as I learned of the improperly redacted document, notified the Department of Homeland Security's headquarters, and ordered that GSA be notified and immediate steps be taken to remove the document from the GSA website. Although this happened promptly and GSA cooperated fully with our request within 2 hours, outside individuals had already downloaded the document and made it available on their websites.

We initiated an extensive internal review through the TSA Office of Inspection and placed the employees who were involved with the redacting of the document on administrative leave pending completion of the review. Secretary Napolitano also asked the Department's Inspector General (IG) to conduct a thorough investigation of the matter, which we are currently engaged in now.

Since this incident, we have also instituted even more stringent new safeguards for all sensitive operational documents to ensure that no SSI is improperly released.

In closing, I deeply regret that this incident occurred. We have taken immediate actions and look forward to working with the IG on implementing any recommended actions in the future.

I am confident that through an exhaustive review of the facts and circumstances surrounding this incident, TSA will emerge a stronger agency.

Thank you for your continued assistance to TSA and for the opportunity to discuss this matter with you today. I would be pleased to respond to your questions.

Ms. JACKSON LEE. Allow me to thank you for your testimony and to now yield myself 5 minutes for questioning.

Before I do that, let me acknowledge the presence of Mr. Himes, a Member of the committee. Other Members will be recognized in the order in which they have arrived.

Ms. Rossides, thank you for the initial steps that have been taken. Let me just ask one pointed question, because when we started this unfortunate incident, and a lot of hysteria was created, both in terms of the media reporting it really looked devastating. Tell me what level of participation now is the IG? How comprehensive is the IG's investigation?

Ms. ROSSIDES. Madam Chairwoman, they are specifically looking at what happened, who was involved, how did it happen, and what measures and recommendations can they make to TSA so that it does not happen again. They are looking at both papers, and they are doing an extensive forensics on the technology, looking at the electronic transmission of the document.

Ms. JACKSON LEE. On the SOP, did you indicate that Members could have individual classified or confidential briefings on the new procedures?

Ms. ROSSIDES. Yes, Madam. We have offered and we will continue to offer, as we go through this process, briefings to any of the Members or their staff on the current SOP that is in place across the aviation system so that the Members can get a full understanding and appreciation of the fact that many systems improvements have been put in place since that version in 2008 was drafted.

Ms. JACKSON LEE. What is your best assessment of whether or not the lives of Americans are now presently at jeopardy or in jeopardy because of information that is already disseminated? What we are speaking of here is a pullback of what occurred and an investigation of why. But now that information has been disseminated, where are we with respect to security, as it relates to the traveling public?

Ms. ROSSIDES. Madam Chairwoman, the system is very strong, and I am very confident in saying that for several reasons. First of all, there were six versions or updates to the document that was released that had very significant changes to the way we conduct the screening procedures.

Secondly, this was a management's standard operating procedure; in other words, it had a lot of checklists of what to do to start the day at the checkpoint. It did not have a lot of Sensitive Security Information on how to actually do certain procedures at the checkpoint.

That being said, I appreciate the gravity and the significance with which people regarded this. But we knew and our immediate reaction was to begin to do a line-by-line review of that document, compare it to measures in place today, and, frankly, even with the confidence we had, out of an abundance of caution, we immediately took some additional measures which we do any time we get information that says, "Let's put an additional set of measures in place in order to be that much more confident in the system."

Ms. JACKSON LEE. Is it safe to say that you have changed the review procedures? Is it also—I am asking several questions at

once, so you might want to make note. The review—or the process that administers the SSI—meaning the document—prior to making the document available to the general public, to review those procedures, is it safe to say that, as the public is traveling, that there are new schemes and procedures that no one knows about?

Lastly, let me just hold this up. This is an example of the kinds of cards that were displayed. Some others dealt with law enforcement officers who need to have confidentiality and privacy. The question is, should we begin to change all of these IDs in order to ensure the safety of those who are in the service of their Government?

Ms. ROSSIDES. Madam Chairwoman, let me answer your questions and make sure that I am fully responding to your several questions.

First of all, with respect to the review of the procedures, there were several things we did. We began our information protection oversight board, which is a board we established several years ago, to look at incidents like this. We also—I asked that, even though SOPs be treated in their entirety as SSI, I asked that we just hold and not release any other SOPs until we could get a complete review of what had been released and what the circumstances were.

I also directed the Office of Acquisition to look at all of their current and recent postings for procurement solicitations and take down any that had any other relevant SSI or sensitive information in them and to make sure that they looked completely at those, which, to the best of my knowledge, we had no other.

We put in a number of measures, mitigation measures that are part of the flexibilities that we have across the system. Federal security directors on Monday morning were directed to implement some of those other flexible provisions so that we would ensure the safety of the traveling public.

I would like to specifically, you know, describe the ID that you show. Although, you know, we take full responsibility and we are not at all pleased that this document was released, those IDs in the document are photocopies. I just want to assure you and the traveling public and our law enforcement partners, there are other aspects to those identifications and credentials that have security features to them, and we have extensive procedures in place to validate the authenticity of persons traveling through that represent themselves as law enforcement officers. In fact, some of those improvements we have made have been at the direct urging of this committee.

Ms. JACKSON LEE. I thank you, Administrator, and now yield 5 minutes to the Ranking Member, Mr. Dent.

Mr. DENT. Thank you, Madam Chairwoman.

Thanks, Ms. Rossides, for being here today. The President, as you know, has stated repeatedly that the administration would embrace the spirit of transparency. The day after his inauguration, the President stated, "Transparency and rule of law will be the touchstones of this presidency."

Are you familiar with Section 114(r), which authorizes TSA to prescribe regulations prohibiting the disclosure of Sensitive Security Information?

Ms. ROSSIDES. Yes, sir, I am.

Mr. DENT. Can you please explain your interpretation of the Congressional exemption included in Section 114(r)(2)?

Ms. ROSSIDES. My understanding is that, when TSA receives a request like this, we are required to provide it to the Congress when it is received from the leadership of a committee, and we do that when we are properly requested.

Mr. DENT. Do you have a certain date when you will be transmitting to the Committee on Homeland Security a copy of the current document, such as today, you know, next week, you know, any date certain after the new year?

Ms. ROSSIDES. Mr. Congressman, what I will pledge to you is that, in the aftermath, the immediate aftermath of this, we wanted to exercise the absolute operational security over all of these SOPs. My commitment to you is, once we are through the traveling holiday season, I will come back and I will talk with you and the leadership of this committee about how to make all of that information available to you. In the meantime, we will sit and give briefings to any Members or their staff that requested on this document specifically.

Mr. DENT. You know, I certainly appreciate that TSA provided my staff about an hour briefing on the differences between these two documents. Then I think there was about an hour to review the latest version of the document, but I want to make sure that I am clear that I still would like to have a hard copy of the document for a thorough review.

I guess the question still is why does TSA not want to provide the committee with a hard copy of this document, given that we have asked for thousands of pages of Sensitive Security Information in the past and TSA has provided them? Why is this different?

Ms. ROSSIDES. The only reason this is different right now is in the immediate aftermath of this incident. I was very concerned to maintain the tightest controls over the current version, because it does have very significant changes to what was released. I just wanted to take the absolute measures to protect that information, and that is why a hard copy wouldn't be presented, but we were very, very willing to provide the information and actually explain the difference in the versions from one document to the other.

Mr. DENT. I thank you for that answer. I keep hearing that the administration is reviewing our request for an unclassified document, and I guess the question is, where are you in that review? Who, if anybody, would be holding up the documents from being provided to our committee? Is it the TSA? Is it DHS, the White House?

Ms. ROSSIDES. Right now, sir, it is—basically, the request is pending and that ultimate decision would be mine or the Secretary's to make. Those are the—under the regulation, we are the two officials with the authority to make the decision to release it.

Mr. DENT. Well, speaking for the Republican side of this committee, I just really would, again, request that we get a date certain for that document. As I have said, we have received, thousands of pages of—Sensitive Security Information and it has never been an issue, but this one seems to be. I understand the issue that you and I have talked about with the travel season being upon us

here, but certainly it would be, I thought, reasonable to have a date certain, some time early in the new year.

Ms. ROSSIDES. I will get back to you, sir.

Mr. DENT. Finally, after the TSA asked the General Services Administration to review the document from its website, it removed it in about 2 hours, but not before being captured and then reposted by various other websites. Do the current regulations provide you a mechanism to keep individuals from reposting this information on other websites?

Ms. ROSSIDES. No, sir, they do not. We do not have any authority to ask non-Government or non-DHS sites to take it down.

Mr. DENT. What action did TSA intend to take against those who are reposting this sensitive document that should not be in the public domain?

Ms. ROSSIDES. Well, right now, there really isn't any authoritative action we can take. Honestly, persons that have posted it, I would, you know, hope that out of their patriotic sense of duty to, you know, their fellow countrymen, they would take it down. But, honestly, I have no authority to direct them and order them to take it down.

Mr. DENT. So there is nothing in current regulations that provide you a mechanism to compel they remove this information?

Ms. ROSSIDES. No.

Mr. DENT. I yield back.

Ms. JACKSON LEE. Thank you very much.

Just as I yield to Chairman Thompson, let me be very clear, Administrator Rossides, that there is a view by the majority—and I appreciate the comments of the Ranking Member—that we want to see the inspector general's work completed before any public distribution of these items, the SOP in particular, because there is concern about the impact on National security.

I would encourage Members to take full advantage of the personal review of documents, but we ask you to urgently move forward, as our Ranking Member has indicated, and we are going to be following this through the holiday season and into the beginning of the year.

I now am pleased to yield 5 minutes to the Chairman of the full committee, Mr. Thompson.

Mr. THOMPSON. Thank you very much, Madam Chairwoman.

Just for timeline purposes, Ms. Rossides, can you tell the committee when this particular posting went up on the web and when TSA found out about it?

Ms. ROSSIDES. Yes, sir. It went up in March 2009. It was part of a solicitation for the SPP program. It came to my attention and senior leadership's attention on Sunday, December 6, in the early evening.

Mr. THOMPSON. So this particular item was in the public domain from March until December?

Ms. ROSSIDES. Yes, sir.

Mr. THOMPSON. Well, I guess one of my concerns is you said you took swift, decisive, and comprehensive action. That is after you found out.

Ms. ROSSIDES. Correct.

Mr. THOMPSON. So before that, it was in wherever. I guess, what are the—can you explain to the committee the protocols for putting items on the web?

Ms. ROSSIDES. Yes, sir. At least through the acquisition process, there are two approaches when we post procurement actions. One is to—when we have any kind of sensitive information, one is to post it to the secure side of the GSA FedBizOpps site, which means that it is password-protected or otherwise secured. The other is solicitations get posted to FedBizOpps' unsecured side.

This particular solicitation got posted on their unsecured side and then was not properly redacted. The—there are other ways that we also will give potential vendors the opportunity to look at SSI information and procurement actions. We might have a physical reading room where we invite the vendors in, and then they can look at that—any SSI material in a physical reading room.

Mr. THOMPSON. Thank you. Now, was this a private contract, who did this, who did this posting?

Ms. ROSSIDES. That is within the scope of the IG's review right now. I can't really comment, because of the IG's due diligence on determining exactly who did what postings. There was a contractor under the SSI office at the time, a contract company under contract with the SSI office.

Mr. THOMPSON. Why would we have a contractor in the SSI office?

Ms. ROSSIDES. Small contracts like that often just provide clerical support. Sometimes they provide research support. Sometimes they provide some technical support. They are not people that are making the decisions on the technical aspects of a job, in terms of like the redactions.

Mr. THOMPSON. Are they required to have clearances?

Ms. ROSSIDES. Yes, sir, they are.

Mr. THOMPSON. Did all these employees in question here have clearances?

Ms. ROSSIDES. That I cannot answer specifically, but during the scope of the IG review, we will know exactly what clearances everybody did have and the particular people involved.

Mr. THOMPSON. Well, you have already suspended five people.

Ms. ROSSIDES. Yes, sir.

Mr. THOMPSON. I would hope that part of your review would have looked at whether or not these clearances were in effect.

Ms. ROSSIDES. The five people who were put on administrative leave do have clearances, yes, sir.

Mr. THOMPSON. Well, but the—to your knowledge, these are not all the people who had access to what we are talking about. Am I correct?

Ms. ROSSIDES. Exactly, sir. As part of the IG's review, they will determine if it was confined to just these five or if, in fact, there are more people who are responsible for this error.

Mr. THOMPSON. For the committee's point of information, how did we find out about this—how did TSA find out about this posting?

Ms. ROSSIDES. I found out from a blogger notifying our blog team. We have a TSA blog team. A blogger who frequently blogs on TSA's blog called and sent an e-mail to one of our bloggers and

pointed it out. That followed a chain of events of my being notified of it.

Mr. THOMPSON. So the particular software that was used to do the redacting, is that a TSA-approved software?

Ms. ROSSIDES. Any of the software on TSA computers are approved by our chief information officer.

Mr. THOMPSON. Did that chief information officer understand that it could be unredacted on the web?

Ms. ROSSIDES. That will be part of what we learn in the IG review, exactly which software, what version of the software, and what version was on the various computers that actually touched this document.

Mr. THOMPSON. So we don't know?

Ms. ROSSIDES. I do not know yet.

Mr. THOMPSON. I would take that you have talked to the chief information officer?

Ms. ROSSIDES. Yes. They are going through and looking at all of the versions of the software on TSA computers now, and they are going through that inventory right now, with the goal being that we will ultimately have the same software on all computers, and everybody will be properly trained to that software.

Mr. THOMPSON. Is there a software presently being used by TSA that can't be unredacted?

Ms. ROSSIDES. Yes, sir, there is.

Mr. THOMPSON. Have we made that software available to everyone who is doing posting on the web for TSA?

Ms. ROSSIDES. Yes, sir, we have. We are going back and making sure that everybody who is using that software is properly trained and knows, again, how to properly use that software. If I could add, had this software been properly used, it would have worked on this document, so we are making sure that everybody who deals with SSI information——

Mr. THOMPSON. Wait a minute. You just told me you don't know which software—you mean, this——

Ms. ROSSIDES. The software in use, the software that our CIO uses today and authorizes, if that software was used——

Mr. THOMPSON. Okay. I got you now.

Ms. ROSSIDES [continuing]. It would have worked.

Mr. THOMPSON. But you don't know which software was used?

Ms. ROSSIDES. Exactly.

Mr. THOMPSON. Okay. Thank you very much.

I yield back, Madam Chairwoman.

Ms. JACKSON LEE. I thank the Chairman.

Now I recognize Mr. Austria.

Mr. AUSTRIA. Thank you, Madam Chairwoman and Ranking Member Dent. I would just like to lend my voice to those who are deeply troubled by this incident. It is extremely concerning to me that here we sit, 8 years after 9/11, and our Government, whether it be accidental or carelessness, can make such a mistake as posting sensitive information on a website.

I am very concerned about that. I am very concerned with the fact that TSA posted the standard operating procedures, that the Federal Government with this incident may have inadvertently helped those that we don't want to see this information, terrorists,

others, do their homework for them, so to speak. I am very concerned about that.

So let me—if I may, I have a number of questions here. I am going to get right to my questions. But, Ms. Rossides, thank you for your testimony today.

Let me, first of all, ask you—kind of following up on the Chairman's questions on redaction—how often does the TSA post redacted standard operating procedures on the internet? What is the purpose of that?

Ms. ROSSIDES. Sir, this was the first time that we had ever posted a standard operating procedure for a procurement solicitation, and it was done specifically for the procurement, for companies to compete for privatizing airports in the State of Montana.

Mr. AUSTRIA. Let me follow up on that answer, because my next question would be, why would TSA post any of its standard operating procedures, sensitive or not? I understand that the entire document may not have been security sensitive, but there were parts that the general public should not have seen. Why would you post anything? Why would you give anyone the opportunity to learn anything about TSA's aviation security procedures?

Ms. ROSSIDES. In the course of that particular solicitation, any vendors will have to be able to prove that they can provide the security procedures at those airports. So they needed to know what kind of requirements we would have at checkpoints for them to be able to demonstrate their qualification to be a qualified vendor to be considered for this contract.

Beyond that, one of the questions that the IG is asking is, why did we take the steps that we did? They are reviewing that decision in terms of, why was it posted?

Mr. AUSTRIA. Let me follow up on this question again, but what is the purpose of posting this? Why does TSA post this on the internet? What is the purpose of that?

Ms. ROSSIDES. The purpose was for a procurement action. It is not something that we post routinely. It was for a specific procurement action that this particular SOP was posted.

Mr. AUSTRIA. So going forward, will TSA continue to use the internet to post redacted Sensitive Security Information for potential contractors or vendors? Or have you changed the way you are doing business?

Ms. ROSSIDES. We have immediately—I have immediately directed the Office of Acquisition to not post any SOPs like this. What we will review with the General Services Administration is ensuring that if we ever do have to post solicitations again—say, for the technology purchases that we are doing—that would contain any SSI information, we will verify that that is in a secure environment on their secure website.

We are also looking at other measures, physically inviting potential vendors in to look at material, as opposed to doing any postings at all.

Mr. AUSTRIA. Okay. I appreciate that answer.

Let me kind of follow up a little bit on what the Chairman was talking about as far as redacting the sensitive documents, because I think that is very important. Can you tell us, as a committee,

what TSA's normal process and procedures are for redacting sensitive documents?

Ms. ROSSIDES. Yes, sir. The normal process is that within program offices that have SSI information, there is a designated individual who is trained to properly redact the materials. The chief information office puts out the instructions on how to properly redact information, based upon the technology that is on each individual's computer.

That process now we are going back and reviewing, both as part of the IG review, in terms of how did this actually happen, and then now, what our CIO is also doing is making sure that the same software for redacting is on all computers, so that the training is consistent from office to office to office.

Mr. AUSTRIA. Okay. One last question I have—I know my time is up, Madam Chairwoman.

Ms. Rossides, based on what has happened here, do you believe that our aviation security has been compromised or weakened because of this incident?

Ms. ROSSIDES. No, sir, I do not.

Mr. AUSTRIA. Thank you, Madam Chairwoman.

Ms. JACKSON LEE. Thank you.

The gentleman from Missouri is recognized, Mr. Cleaver, for 5 minutes.

Mr. CLEAVER. Ms. Rossides, thank you for being here.

To follow with Mr. Austria's, the answer to that question would have been what you just said no matter what, right?

Ms. ROSSIDES. Yes, sir. I believe that our system is very strong.

Mr. CLEAVER. No, no, no. I mean, but even if it weren't, that that would be the answer, right?

Ms. ROSSIDES. I don't understand.

Mr. CLEAVER. I mean, you wouldn't have sat here in front of, you know, TV cameras that our system has been compromised.

Ms. ROSSIDES. I believe that the system is very strong and it was not compromised as a result of this, sir.

Mr. CLEAVER. Okay. I understand why you won't answer the question, which is why I asked the question. But that was somewhat of an answer. Has there been a—see, I don't—I am not sure you can answer my questions here, because I don't—because——

Ms. ROSSIDES. I can—perhaps when we get into the closed session, I can answer and give you more examples as to why I am confident in our systems.

Mr. CLEAVER. Well, generally, whether it is science or theology or anthropology or epidemiology, we all build on what was. So it seems to me that any new versions were built on older versions. Am I right about that?

Ms. ROSSIDES. Yes, sir.

Mr. CLEAVER. Okay. So if I am correct, then there obviously is information that is out there that is in the latest iteration.

Ms. ROSSIDES. That is true. But that—the bulk of that information is not SSI information. It is checklists. It is routine standard procedures.

Mr. CLEAVER. The SSI material was posted on the fob.com on March 3, but it was not discovered by TSA until December 6. What was the—what happened differently in between time?

Ms. ROSSIDES. The procurement solicitation was up on the FedBizOpps website. In fact, the procurement went through its whole process. A contractor was selected for that procurement. Then the normal routine is, once the contract is awarded, the GSA keeps the procurement award posted on the FedBizOpps and advises the public, who actually won the contract.

Mr. CLEAVER. Okay. Unfortunately, it sounds like we have been called to vote. The questions that I have, based on what you are saying, I am not sure I want answered. I mean, I don't think you will answer it in front of everybody in the first place.

So I don't want to ask it, because then I get frustrated, because you can't answer it. On top of that, I appreciate you not answering it—sounds clear.

Ms. ROSSIDES. Well, if we have the opportunity to go into the Executive Session, perhaps I can give you some answers that won't frustrate you and will be able to give you more information.

Mr. CLEAVER. But you understand the——

Ms. ROSSIDES. Yes, sir, I do. I understand.

Mr. CLEAVER. Madam Chairwoman, thank you.

Ms. JACKSON LEE. I thank the gentleman.

The gentlelady is correct. If we are prepared to go into Executive Session—we are called for a vote. We are going to continue for a period of time.

I do want to ask the administrator on her time circumstances here. I see the number of Members, but we do want to pose that question to you. What is your time circumstance, please?

Ms. ROSSIDES. You know, probably, Madam Chairwoman, I have got to be out of here by about 4:15.

Ms. JACKSON LEE. 4:15.

Ms. ROSSIDES. Yes, ma'am.

Ms. JACKSON LEE. Let me now recognize—and we will contemplate what our next step is. Let me recognize Mr. Lungren for 5 minutes. He is not a Member of the committee—yield to—but we are graciously accepting him, but we are going to Members first.

Mr. Himes is recognized.

Mr. HIMES. Thank you, Madam Chairwoman. A couple of quick questions.

First, I share my colleagues' concern, obviously, with this disclosure of sensitive information. Of course, no organization doesn't make mistakes. The measure of an organization is how well you learn from your mistakes. It sounds like you have taken a fairly aggressive approach to that.

Here's a slightly off-the-wall question, but one that I think is important. We know that, through a couple of different mechanisms, this information is now in the public domain. Are you or is anybody looking to see who has subsequently downloaded it?

Ms. ROSSIDES. I believe that is part of what the IG is looking at. We do know—we have in our—our CIO shop has done an initial review of who did download it and has it on their websites, the non-Government, non-DHS websites. We do know that.

Mr. HIMES. Thank you. Yes, no, I am just intrigued by the possibility that you might cross-check a list of those end-users, not just cross-posters, but end-users who downloaded it perhaps with other

lists that could—from which we could maybe make some inferences.

When we get classified information on this committee, each page is usually marked with some degree of classification. Sometimes each paragraph has actually indicated some level of classification. Do you follow a similar protocol on a hard copy? Would SSI be always indicated as such?

Ms. ROSSIDES. Yes, sir. If appropriately marked, the SSI document would be marked and the pages would have a header and a footer on them that said it is SSI information.

Mr. HIMES. Not having seen the SSI that was disclosed, was that, in fact, appropriately marked as such?

Ms. ROSSIDES. No, sir, it was not, no. That was part of the problem.

Mr. HIMES. So the failure was one of marking.

Ms. ROSSIDES. And redacting.

Mr. HIMES. And redacting, okay. Do you have a sense for what your overall rate of compliance is with respect to marking appropriately your documents?

Ms. ROSSIDES. Well, sir, we do a number of self-assessments as part of our SSI program, and we do those routinely. We also had a very extensive review by GAO at the end of 2007 who actually gave very good grade to TSA for how we do—our program office addresses SSI.

Mr. HIMES. Thank you. I yield back the balance of my time.

Ms. JACKSON LEE. I thank the gentleman from Connecticut.

I would like to now recognize Mr. Bilirakis for 5 minutes.

Mr. BILIRAKIS. Yes, I will go ahead and ask my questions during the Executive Session, Madam Chairwoman. Thank you.

Ms. JACKSON LEE. Let me——

Mr. DENT. May I ask your indulgence, Madam Chairwoman? I know we have a few minutes before the vote, but before we go into Executive Session, I am struggling a little bit with the underlying premise of Ms. Rossides' response.

By refusing to give a document to this committee because you are concerned about public disclosure, that is implying that the subcommittee will disclose the document. That is what troubles me the most: The implication that this subcommittee is not taking security of these documents that seriously, and I think we all agree that we know that is not the case.

For the record, I am glad the inspector general is doing his investigation, but that is not particularly relevant to our request for this document. We are a separate and equal branch of Government responsible for overseeing TSA's activities. I am frustrated by, again, a willingness to provide us a date certain for delivering this critical document to the subcommittee.

So I feel like I have been left with no choice. I feel like we have given the administration every opportunity to provide this document. I appreciate the fact that our staff has been able to look at this for a few hours.

I think, somewhat reluctantly, along with Ranking Member Bilirakis, Mr. Lungren and Mr. King, and others, you know, I will be introducing a resolution of inquiry demanding that the Secretary provide the House of Representatives with this document. I think

it is only appropriate, and I would rather not do it. If I had a date certain, I would not ask for this resolution.

Ms. JACKSON LEE. The gentleman—if the gentleman's finished his remarks—let me ask you, Administrator Rossides, if you have a definitive date or whether you could submit a definitive date of the completion of the IG report?

Ms. ROSSIDES. No, Madam. I am sorry. I do not. I do not know when the IG will definitively be finished. I know that they have this on an expedited track, but I don't have a specific date. I couldn't speak——

Ms. JACKSON LEE. Do you have a close, proximate date?

Ms. ROSSIDES. All I know is when they first began the engagement and took it over from our office of inspection, they said they wanted to have it done in a matter of a couple weeks, so that they started that, you know, earlier, right after—they started it on December 9.

Ms. JACKSON LEE. Okay, well, let me just say that I am very moved by the sincerity of Mr. Dent's request and intent to offer a resolution of inquiry, but I am aware that the Chairman of the full committee has authority to move forward, and it would seem, Mr. Dent, that you would raise that question with the Chairman of the full committee. I think that would be the appropriate next step and not a resolution of inquiry.

I might also say that part of our concern has been that, in disclosing the SOP, it is possible for leaks. Of course, it sounds maybe that it is ironic that I would use the term leaks, because, obviously, we have had a breach. But there have been many, many Members of the House and the Senate that have asked for this document, and there is no doubt this is a high-profile document, but our job is to ensure that there are no further leaks equally egregious.

So I would ask that you ask the Chairman of the full committee as a first step, but more importantly, I would say that I would like Ms. Rossides to come back in the next 24 hours, if she can be in touch with the Secretary and the IG, to get a more definitive time. I know answering today may be difficult, but I would think the inspector general would be open to the fact that this is urgent. Mr. Dent has indicated it is urgent. There is a suggestion of a resolution of inquiry, which I think is premature.

But even so, that shows the urgency of the matter. We need to, in essence, respond to that. So I would suggest that the first response for Mr. Dent and his colleagues is a request to the Chairman of the full committee, Mr. Thompson. Then I would want to have the additional information for our subcommittee as to the time that you believe this might occur.

Ms. ROSSIDES. Yes, ma'am, I will do that.

Ms. JACKSON LEE. The IG's report.

Mr. DENT. Madam Chairwoman, the only thing I would ask——

Ms. JACKSON LEE. I yield to the gentleman for a response.

Mr. DENT. The only thing I would ask, respectfully, is that we be given a date certain as to when we would receive this document, then I would quite happily withdraw the motion for the resolution of inquiry. I do feel that the inspector general investigation is irrelevant to our request for that particular document. As I said previously, we have received, many thousands of pages of sensitive

and security information, and I think our committee has handled them well and we certainly will make a request to the Chairman.

I would just like to keep this resolution out there for consideration. Hopefully in the intervening time, we can get a date certain. If we were to get a date certain for the release of document, then we could at that time withdraw the resolution.

Ms. JACKSON LEE. I think we found some measure of reconciliation or a moment that we can reconsider.

Let me quickly—I think there are one or two Members that are going to be here. I am continuing the hearing because of the time constraints of Ms. Rossides. So anyone that is interested in the—going forward on the Executive Session, they need to hurry back, because the first vote—let me just proceed—I assume all Members have gone forward. I will yield myself for a second round until we convene into the Executive Session.

Do you believe that any actions taken by the individuals that you have put on administrative leave or have disposed of in another manner—and I do need to get a correct interpretation—were some of these individuals contract employees?

Ms. ROSSIDES. Madam Chairwoman, at the time in March 2009, one of the individuals was a contractor, but he is now a TSA employee, and he is one of the five TSA employees that is on administrative leave.

Ms. JACKSON LEE. Do you believe that any actions by these employees was intentional?

Ms. ROSSIDES. I would have to wait for the IG report, but my honest assessment is no.

Ms. JACKSON LEE. But you——

Ms. ROSSIDES. I think this was an accident.

Ms. JACKSON LEE. Your honest assessment is no, but you do not know?

Ms. ROSSIDES. I don't know for sure until the IG gives us the report.

Ms. JACKSON LEE. One of the employees was a contractor, and you are representing to this committee that that individual is now employed. But are you also representing that that individual went through the normal security checks?

Ms. ROSSIDES. Yes. If he was hired as a TSA employee, he would have had a background check.

Ms. JACKSON LEE. What do we learn from the idea—not the idea, but the actual happening of this incident occurring in March 2009 and this was exposed in the last 3 weeks? What do we learn from that?

Ms. ROSSIDES. I think that—

Ms. JACKSON LEE. As you answer that question, can you comprehend the disappointment that we have in that issue?

Ms. ROSSIDES. Yes, Madam Chairwoman. I think there are a number of things that we learned from this. Our learnings from this are that we definitely need better processes in place and tighter controls on how we handle sensitive information. In the size of TSA, as large of an organization it is, where this information is shared across the organization, we are going to have to make sure that we have designated personnel who are properly managing—and managing this information and treating it in the manner in

which it should be. We need to make sure that our personnel are trained and really truly understand.

If there is a lesson that the entire TSA organization has learned in this, it shows that, you know, the accident or the mistake of one or a few can tremendously impact the whole agency and our credibility with the American public. So we are taking it very, very seriously. I think that our front-line officers, our FAMs, our inspectors, our TSOs are very much aware of their responsibility now because a document like this has been put out there.

So I think there will be a number of lessons that we will learn. I also think that there are technology solutions that hopefully will come from the IG's report about the right technology to use, the right versions to use when redacting information.

Ms. JACKSON LEE. Let me say this. I will recess this committee, and keeping in mind your schedule, we will return quickly, but my intent is to write legislation, first of all, with a great deal of respect for the reliance of this Government overall, not just Department of Homeland Security, on contract employees, from Blackwater employees to a number of others.

It is clear that there needs to be standards utilized for the hiring, retaining, and utilizing of contract employees. It will be my thought, it will be my legislative initiative to insist that contract employees not be used to handle Sensitive Security Information, period.

Then we are looking to craft legislation that puts a firewall around certain technology, because as I was listening to the Chairman, if this is unique technology that ultimately will prevent redacting from showing up again on a website, then I don't want random individuals having access to that, because then you can be exploited.

So I will introduce legislation in the early part of the year to establish that criteria, and we will also have to find a better pathway of informing the Members of this House and Senate, and I would imagine the White House, on issues of breach of security.

With that, this hearing remains in recess. We may start back in—with a brief open session, but we will then go into the Executive Session. Thank you. This hearing is now in recess.

[Recess.]

Ms. JACKSON LEE. Committee is called to order.

Ms. Rossides, I would like to pursue a line of questioning. This is not the Executive Session, which we will go into very shortly.

Would you please share, again, with the explanation as to whether or not we had a different software in March 2009, but we now have a different software in December 2009, dealing with this particular issue?

Ms. ROSSIDES. Madam Chairwoman, I can't answer that question with any specificity, because I do not know, and that is what the IG's forensic team is looking at, as they are looking at all of the computers that were used by people in this action, so I cannot answer that. That will be part of the IG's review.

Ms. JACKSON LEE. Do you have information—and if you have said it before, if you could say it again—that the policies of dealing with SSI have now changed, is there a review process of several individuals that are now as we speak looking at Sensitive Security

Information and making a paper trail decision, meaning that you will know who made the decision, on what goes onto the web?

Ms. ROSSIDES. Yes. That is really—I would give you a couple of answers to that. First of all, our procedures for how SSI information is handled internally is part of our review and our lessons learned. We will look again at those procedures.

The SSI office maintains very detailed records of how they look at the documents and then how the documents are passed forward to other offices. The acquisition office is also looking at their procedures. Then most importantly, the CIO, our chief information officer, is looking at both the technology that should be used across the whole agency in handling redacted material. We have actually asked the NSA to come in and help us ensure, give us a certification that any tool we use for redacting material electronically will meet their certification standards. So we are taking that added measure.

Ms. JACKSON LEE. As you do that, you are going to have written criteria, some roadmap to go forward on the handling of these materials so that we can assure the American people that this will not happen again?

Ms. ROSSIDES. We will do a exhaustive review—and I commit to you that we will make sure we have procedures in writing that we train the appropriate personnel and that we raise every employee awareness about the importance of handling SSI material appropriately.

Ms. JACKSON LEE. All right. As I indicated with respect to contractors, is there any determination that contractors would be outside the realm of sensitive security materials?

Ms. ROSSIDES. No. Madam Chairwoman, right now, I believe that we do have some contractors that handle SSI material, but if they do, they are subject to the exact same procedures that any employee in handling SSI is subject to.

Ms. JACKSON LEE. Well, I, frankly, believe that we should leave our SSI materials to employees of Homeland Security. I know that this Government has become very dependent in many areas—and in some areas, it is very effective. I have no problem with who builds our highways and bridges. It may be very difficult for the Government to engage in construction.

But I certainly have concern about the use of non-Government employees in the handling of Sensitive Security Information. I am going to raise that with the Department. I am raising it with you. I would like you to raise it with your team. We will have to come to some resolution on that, because there is little reprimand, I believe, under the circumstances for a contract employee who is getting paid by tax dollars, but then is, unfortunately, in a breach such as this, which we have not determined whether or not it was intentional. Certainly, I appreciate your representation at the level that it was at.

Then final question before we enter into this session, the individuals that you were dealing with that have been, I guess, suspended——

Ms. ROSSIDES. Placed on administrative——

Ms. JACKSON LEE [continuing]. Administrative leave, what level civil service rank would they have been at? What was their level?

Ms. ROSSIDES. I would have to get back to you and confirm. They are at the mid-level and one, I believe, is at a senior management level. But I could have—I would have to confirm all—all five of them. I know that—that one, the high—the highest level one was at a senior management level. It is the K band in TSA's pay system.

Ms. JACKSON LEE. Okay. With that in mind, thank you. The subcommittee will now resolve into Executive Session. I ask the clerk to prepare the room.

[Whereupon, at 3:52 p.m., the subcommittee proceeded in Executive Session, and subsequently adjourned the hearing at 4:14 p.m.]

○