NO ACT

DIVISION OF
CORPORATION FINANCE

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549-3010

PE
2-20-08

Received SEC

FEB 20 2008

Washington, DC 20549

February 20, 2008

William V. Fogg
Cravath, Swaine & Moore LLP
Worldwide Plaza
825 Eighth Avenue
New York, NY 10019-7475

Act: 1934
Section:
Rule: 14A-8
Public
Availability: 2/20/2008

Re: Burlington Northern Santa Fe Corporation

Dear Mr. Fogg:

This is in regard to your letter dated February 19, 2008 concerning the shareholder proposal submitted by the International Brotherhood of Teamsters General Fund for inclusion in BNSF's proxy materials for its upcoming annual meeting of security holders. Your letter indicates that the proponent has withdrawn the proposal, and that BNSF therefore withdraws its January 25, 2008 reconsideration request. Because the matter is now moot, we will have no further comment.

Sincerely,

PROCESSED
FEB 28 2008
THOMSON
FINANCIAL

Jonathan A. Ingram
Deputy Chief Counsel

cc: Louis Malizia
Assistant Director
Capital Strategies Department
International Brotherhood of Teamsters
25 Louisiana Avenue, NW
Washington, DC 20001

CRAVATH, SWAINE & MOORE LLP

WORLDWIDE PLAZA
825 EIGHTH AVENUE
NEW YORK, NY 10019-7475

TELEPHONE: (212) 474-1000
FACSIMILE: (212) 474-3700

CITYPOINT
ONE ROPEMAKER STREET
LONDON EC2Y 9HR
TELEPHONE: 44-20-7453-1000
FACSIMILE: 44-20-7860-1150

WRITER'S DIRECT DIAL NUMBER

212-474-1131

ROBERT D. JOFFE
ALLEN FINKELSON
RONALD S. ROLFE
PAUL C. SAUNDERS
DOUGLAS D. BROADWATER
ALAN C. STEPHENSON
MAX R. SHULMAN
STUART W. GOLD
JOHN E. BEERBOWER
EVAN R. CHESLER
MICHAEL L. SCHLER
RICHARD LEVIN
KRIS F. HEINZELMAN
B. ROBBINS KIESSLING
ROGER D. TURNER
PHILIP A. GELSTON
RORY O. MILLSON
FRANCIS P. BARRON
RICHARD W. CLARY
WILLIAM P. ROGERS, JR.
JAMES D. COOPER
STEPHEN L. GORDON
DANIEL L. MOSLEY
GREGORY M. SHAW
PETER S. WILSON

JAMES C. VARDELL, II
ROBERT H. BARON
KEVIN J. GREHAN
STEPHEN S. MADSEN
C. ALLEN PARKER
MARC S. ROSENBERG
SUSAN WEBSTER
TIMOTHY G. MASSAD
DAVID MERCADO
ROWAN D. WILSON
PETER T. BARBUR
SANDRA C. GOLDSTEIN
PAUL MICHALSKI
THOMAS G. RAFFERTY
MICHAEL S. GOLDMAN
RICHARD HALL
ELIZABETH L. GRAYER
JULIE A. NORTH
ANDREW W. NEEDHAM
STEPHEN L. BURNS
KATHERINE B. FORREST
KEITH R. HUMMEL
DANIEL SLIFKIN
JEFFREY A. SMITH
ROBERT I. TOWNSEND, III

WILLIAM J. WHELAN, III
SCOTT A. BARSHAY
PHILIP J. BOECKMAN
ROGER G. BROOKS
WILLIAM V. FOGG
FAIZA J. SAEED
RICHARD J. STARK
THOMAS E. DUNN
JULIE SPELLMAN SWEET
RONALD CAMI
MARK I. GREENE
SARKIS JEBEJIAN
JAMES C. WOOLERY
DAVID R. MARRIOTT
MICHAEL A. PASKIN
ANDREW J. PITTS
MICHAEL T. REYNOLDS
ANTONY L. RYAN
GEORGE E. ZOBITZ
GEORGE A. STEPHANAKIS
DARIN P. MCATEE
GARY A. BORNSTEIN
TIMOTHY G. CAMERON
KARIN A. DEMASI
LIZABETHANN R. EISEN

DAVID S. FINKELSTEIN
DAVID GREENWALD
RACHEL G. SKAISTIS
PAUL H. ZUMBRO
JOEL F. HEROLD
ERIC W. HILFERS
GEORGE F. SCHOEN
ERIK R. TAVZEL
CRAIG F. ARCELLA
TEENA-ANN V. SANKOORIKAL
ANDREW R. THOMPSON
DAMIEN R. ZOUBEK
LAUREN ANGELILLI
TATIANA LAPUSHCHIK
ERIC L. SCHIELE

SPECIAL COUNSEL
SAMUEL C. BUTLER
GEORGE J. GILLESPIE, III
THOMAS D. BARR

OF COUNSEL
CHRISTINE BESHAR

RECEIVED
2008 JAN 28 PM 4:07
OFFICE OF CHIEF COUNSEL
CORPORATION FINANCE

January 25, 2008

Burlington Northern Santa Fe Corporation - Shareholder Proposal Submitted by the International Brotherhood of Teamsters' General Fund

Ladies and Gentlemen:

This letter is submitted on behalf of Burlington Northern Santa Fe Corporation ("BNSF" or the "Company") in response to a letter dated December 27, 2007, that BNSF received from the Division of Corporation Finance, in which the Staff denied BNSF's request for no action with respect to a shareholder proposal submitted to BNSF by the International Brotherhood of Teamsters' General Fund (the "Proponent") for inclusion in BNSF's 2008 proxy statement and other proxy materials (the "2008 Proxy Materials"). In a letter dated November 19, 2007 (the "No-Action Request"), BNSF submitted a request to the Staff for a no-action letter on the ground that the Proponent's proposal (the "Proposal") was excludable under Rule 14a-8(i)(7) and Rule 14a-8(i)(3) under the Securities Exchange Act of 1934 (the "Exchange Act"). The Proponent subsequently submitted a letter to the Staff dated December 7, 2007 (the "Proponent's Response"), addressing the No-Action Request. In response to such letter, BNSF submitted a letter to the Staff dated December 19, 2007 ("BNSF's Response"). The Proponent's Proposal is attached as Exhibit A, the No-Action Request is attached as Exhibit B, the Proponent's Response is attached as Exhibit C, and BNSF's Response is attached as Exhibit D.

BNSF hereby respectfully requests that the Staff reconsider the position taken in its letter dated December 27, 2007. In support of such request, we have identified additional arguments and lines of analysis that were not addressed by the No-Action Request or BNSF's Response. Based on such analysis, we urge the Staff to confirm that it will not recommend any enforcement action to the Commission if, in reliance on certain provisions of Commission Rule 14a-8 under the Exchange Act, BNSF excludes the Proposal from its 2008 Proxy Materials.

In accordance with Rule 14a-8(j), we are filing six copies of this letter and the Exhibits. We are simultaneously forwarding a copy of this letter via overnight courier, with copies of all enclosures, to the Proponent as additional notice of the Company's intention to exclude the Proposal from the Company's 2008 Proxy Materials.

The Proposal states:

Resolved: That the shareholders of Burlington Northern Santa Fe Corporation ("BNSF" or "Company") hereby request that the Board of Directors make available, omitting proprietary information and at reasonable cost, in BNSF's annual proxy statement, by the 2009 annual meeting, information relevant to the Company's efforts to safeguard the security of their operations arising from a terrorist attack and/or other homeland security incidents.

We believe that the Proposal may be properly omitted from BNSF's 2008 proxy materials pursuant to Rule 14a-8 for the reasons set forth below.

BASES FOR EXCLUSION

I. BNSF may exclude the Proposal in reliance on Rule 14a-8(i)(2) because the Proposal, if implemented, would cause BNSF to violate federal law.

A shareholder proposal may be properly excluded under Rule 14a-8(i)(2) "if the proposal would, if implemented, cause the company to violate any state, federal or foreign law to which it is subject." In this case, the Proposal makes a very broad request for information, specifically "information relevant to the Company's efforts to safeguard the security of [its] operations arising from a terrorist attack and/or other homeland security incidents." The information in BNSF's possession that meets this request, however, has been deemed "Sensitive Security Information," the disclosure of which would violate a variety of federal regulations and statutes to which BNSF is subject. Therefore, implementation of the proposal would force BNSF to violate federal law.

A. Compliance with the Proposal would require BNSF to violate federal regulations pertaining to Sensitive Security Information.

In the wake of the September 11, 2001 terrorist attacks on New York and Washington, the United States Congress took a variety of actions to prevent a similar tragedy. Pursuant to the Aviation and Transportation Security Act, Congress established the Transportation Security Administration (the "TSA") as an "administration of the Department of Transportation" ("DOT"). 49 U.S.C. 114(a). The TSA was subsequently given the authority to "prescribe regulations prohibiting the disclosure of information obtained or developed in carrying out security . . . [if it] decides that disclosing the information would . . . be detrimental to the security of transportation." 49 U.S.C. 114(s).

1. The TSA has authority to classify information as Sensitive Security Information, and it has confirmed that BNSF's security plan is Sensitive Security Information

Using the authority granted to it by Congress, the TSA enacted a set of federal regulations that pertain to the protection and non-disclosure of certain information that the TSA has "determined to be Sensitive Security Information" ("SSI"). 49 C.F.R. 1520.1. Under these regulations, SSI is defined as "information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would . . . [b]e detrimental to the security of transportation." 49 C.F.R. 1520.5(a). The regulation goes on to specify that SSI includes "[a]ny security program or security contingency plan issued, established, required, received, or approved by DOT or [the Department of Homeland Security ("DHS")]." 49 C.F.R. 1520.5(b)(1). After listing a number of other categories of SSI, the regulations further provide that "[a]ny information not otherwise described in [49 C.F.R. 1520.5] that TSA determines is SSI" will qualify as SSI for the purposes of these regulations. *See* 49 C.F.R. 1520.5(b)(16). This subsection, therefore, gives the TSA broad discretion to classify information as SSI. The TSA in turn has developed detailed procedures for determining whether specific information and types of information are SSI, and it has communicated these protocols and internal policies to its staff members and other parties (including private parties) through a variety of sources. For example, these procedures are outlined in the Department of Homeland Security's Management Directive Number 11056 (12/16/2005) and also in a report from the United States Government Accountability Office titled "Transportation Security Administration's Processes for Designating and Releasing Sensitive Security Information." These documents are attached to this letter as Exhibits E and F respectively. These internal policies demonstrate that only specially-trained TSA employees are entrusted with the responsibility of designating information as SSI, and that a great deal of time and energy goes into each such designation. The TSA does not make such classifications haphazardly or hastily, and when information does receive the SSI classification there is a bona fide justification for that determination: specifically, if such information were to be broadly disseminated, it would significantly compromise transportation security.

In the years since the TSA implemented this system for classifying certain information as SSI, BNSF has had many discussions and other communications with the TSA regarding the secrecy of its overall Security Management Plan. For example, a letter confirming the TSA's review of this plan is attached as Exhibit G. As confirmed by the last paragraph on page 1 of the TSA's letter, the TSA has designated information relating to BNSF's Security Management Plan, which by its very nature includes "information relevant to the Company's efforts to safeguard the security of [its] operations arising from a terrorist attack and/or other homeland security incidents," as SSI. Put differently, the TSA has confirmed that disclosure of this information would compromise the security of the railroad industry. Also, pursuant to the guidelines set forth in the letter from the TSA, other materials that BNSF has submitted to the TSA have been stamped with a label that includes "**SENSITIVE SECURITY INFORMATION/FOR OFFICIAL USE ONLY**." Accordingly, BNSF is required by law to protect this SSI pursuant to the strictures of the TSA regulations. Even without a specific SSI determination by TSA, certain categories of information are identified by regulation as SSI, and BNSF would be prohibited from disclosing SSI, including but not limited to security plans and procedures, contingency plans, and vulnerability assessments.

2. Disclosure of SSI is specifically prohibited by federal law

In furtherance of the Congressional goals of protecting the country from terrorist attacks and homeland security incidents, the relevant TSA regulations safeguard SSI by prohibiting persons or entities with access to SSI (such as BNSF) from making any unauthorized disclosure of such information. Specifically, the regulations provide that SSI may only be disclosed to persons "*who have a need to know*" the contents of the SSI. 49 C.F.R. 1520.9(a)(2) (emphasis added). The regulations go on to detail exactly when somebody has a "need to know" certain SSI. According to the regulations, a person who is not a federal employee only has a "need to know" the information under the following circumstances:

> (1) When the person requires access to specific SSI to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.
>
> (2) When the person is in training to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.
>
> (3) When the information is necessary for the person to supervise or otherwise manage individuals carrying out transportation security activities approved, accepted, funded, recommended, or directed by the DHS or DOT.
>
> (4) When the person needs the information to provide technical or legal advice to a covered person regarding transportation security requirements of Federal law.
>
> (5) When the person needs the information to represent a covered person in connection with any judicial or administrative proceeding regarding those requirements. 49 C.F.R. 1520.11(a).

Any disclosure of SSI to a person who does not fit into these categories violates the regulations.

Based on these restrictions, if the Proposal were implemented, BNSF would be in violation of 49 C.F.R 1520.9(a)(2), as it would be disclosing SSI to many people who do not have a "need to know" such information, specifically the Proponent, other BNSF shareholders, and the general public. The Proposal broadly requests "information relevant to the Company's efforts to safeguard the security of [its] operations arising from a terrorist attack and/or other homeland security incidents." The information that meets this request, however, necessarily includes SSI in the Company's possession, including the Security Management Plan developed by the Company as a countermeasure to possible terrorist attacks and other homeland security incidents (thereby making it clearly "relevant to the Company's efforts to safeguard the security of [its] operations" against such events). Compliance with the Proposal would therefore force BNSF to violate 49 C.F.R. 1520.9(a)(2), by publishing information that TSA has

deemed SSI in its annual proxy materials and thereby disseminating that information to the general public.[1]

In giving the TSA broad authority to designate and protect SSI, Congress's purpose was clear: to safeguard the country from future terrorist attacks by preventing sensitive information from falling into the wrong hands. Implementation of the Proposal would run counter to this important policy, as it would place secret information in the public domain, thereby providing terrorists with a blueprint to BNSF's most sensitive security procedures. The regulations cited above were implemented to prevent such an outcome, and the Proposal should therefore be excluded to prevent BNSF from having to choose between making the requested disclosures or violating these regulations.

The steps that BNSF has already taken to comply with these regulations and safeguard its SSI further illustrate the extreme sensitivity of the information that the Proponent has requested. Because the Company can only legally disseminate the information to those who have a "need to know," only a few BNSF employees (no more than 10) have been given access to all of the information that the Proponent would have BNSF place in its 2008 Proxy Materials. BNSF is careful to ensure that only those employees whose job responsibilities require that they have access to information protected as SSI receive that access; furthermore, BNSF limits the access to the portion of the SSI relevant to their job responsibilities. Not even BNSF's Board of Directors has access to all this information because it does not have a "need to know" all the SSI pursuant to federal regulations. Consistent with the detailed and careful steps BNSF has taken to safeguard SSI internally, and in compliance with the applicable federal laws and regulations, the Company should not be asked to provide public disclosure of this type of information in its annual proxy materials (or otherwise) and the Proposal should therefore be excluded.

B. Compliance with the Proposal would require BNSF to violate federal regulations pertaining to hazardous materials.

Additionally, implementation of the Proposal would cause BNSF to violate various other federal regulations that pertain to the transportation of hazardous materials. Because BNSF regularly ships hazardous materials, including toxic-by-inhalation, radioactive, and explosive materials, it is required to "develop and adhere to a security plan" for the shipment of those materials which complies with various strictures set forth by the DOT. *See* 49 C.F.R. 172.800, 172.802. BNSF has developed a security plan that complies with these regulations. Information about BNSF's procedures and

---

[1] As an ancillary matter, we note that even if BNSF were to omit "proprietary information" from the requested disclosure (as allowed by the Proposal), much of the information that it would still have to include would qualify as SSI. Though the Proponent makes no attempt to define "proprietary information," it is generally used in BNSF's industry to refer to confidential business information that is developed and exploited for commercial gain, like trade secrets. Much of BNSF's confidential SSI would not qualify as proprietary information, as it pertains to matters like threat response protocols or vulnerabilities in BNSF's security systems. Thus, the Proposal, as written, would still require BNSF to disclose SSI, which would mean that BNSF could be found in violation of federal regulations.

security plan to safeguard the hazardous materials it transports would be covered by the Proposal as that information is "relevant" and pertains to the Company's "efforts to safeguard the security of [its] operations arising from a terrorist attack and/or other homeland security incidents." One of the specific risks that BNSF considered in developing this plan was the risk of a terrorist attack on trains that carry hazardous materials. Therefore, if the Proposal were implemented, the Company's security plan for hazardous materials would qualify as "information relevant to the Company's efforts to safeguard the security" of its operations.

However, disclosure of the security plan for hazardous materials would violate 49 C.F.R. 17.802(b), which states that "copies of the security plan, or portions thereof, must be available to employees who are responsible for implementing it, *consistent with personnel security clearance or background investigation restrictions and a demonstrated need to know.*" 49 C.F.R. 17.802(b) (emphasis added). As these regulations indicate, dissemination of this sensitive information is limited to employees with appropriate clearances and a demonstrated need to know the information. The regulations safeguard the security of hazardous materials by limiting the distribution of information relating thereto, and they would be violated by any public disclosure the Company might make of its hazardous materials security plan. For this reason also, the Proposal is properly excludable from the Company's proxy.

II. BNSF may exclude the Proposal in reliance on Rule 14a-8(i)(7) because it relates to ordinary business operations.

Rule 14a-8(i)(7) permits a company to exclude a stockholder proposal if it pertains to "a matter relating to the company's ordinary business operations." According to the Commission release accompanying the 1998 amendments to Rule 14a-8, the term "ordinary business" refers to matters that are not necessarily "ordinary" in the common meaning of the word, but instead the term "is rooted in the corporate law concept of providing management with flexibility in directing certain core matters involving the company's business and operations." Exchange Act Release No. 40018 (May 21, 1998) (the "1998 Release"). In the 1998 Release, the Commission described the two "central considerations" for the ordinary business exclusion:

> The first relates to the subject matter of the proposal. Certain tasks are so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight. Examples include the management of the workforce, such as the hiring, promotion, and termination of employees, decisions on production quality and quantity, and the retention of suppliers. However, proposals relating to such matters but focusing on sufficiently significant social policy issues (e.g., significant discrimination matters) generally would not be considered to be excludable, because the proposals would transcend the day-to-day business matters and raise policy issues so significant that it would be appropriate for a shareholder vote. The second consideration relates to the degree to

> which the proposal seeks to "micro-manage" the company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment.

Thus, when examining whether a proposal may be excluded under Rule 14a-8(i)(7), the first step is to determine whether the proposal raises any significant social policy issue. If a proposal does not, then it may be excluded under Rule 14a-8(i)(7). If a proposal does raise a significant social policy issue, it is not the end of the analysis. As discussed below, the Staff has concurred with the exclusion of shareholder proposals that raise a significant social policy issue when other aspects of the report or action sought in the proposals implicate a company's ordinary business. We believe that most Rule 14a-8(i)(7) determinations considered by the Staff do not revolve around whether the subject matter of a proposal has raised a significant social policy issue, but instead depend on whether the specific actions sought by the proposal or some other aspect of the proposal involve day-to-day business matters.

The Staff also has stated that a proposal requesting the dissemination of a report may be excludable under Rule 14a-8(i)(7) if the substance of the report is within the ordinary business of the issuer. *See* Exchange Act Release No. 20091 (Aug. 16, 1983). In addition, the Staff has indicated, "[where] the subject matter of the additional disclosure sought in a particular proposal involves a matter of ordinary business . . . it may be excluded under rule 14a-8(i)(7)." *Johnson Controls, Inc.* (Oct. 26, 1999).

A. BNSF's efforts to safeguard the security of its operations from terrorist attacks and/or other homeland security incidents is a day-to-day activity.

The entirety of BNSF's business operations revolves around the transport of its railcars and their cargo. A central feature of this service is ensuring the safety of its customers' cargo. Because BNSF's ability to manage and ensure the safety of its trains is so fundamental to the Company, it must evaluate and review its safety procedures and policies every single day. This process focuses on *all* risks and threats that the Company faces, including the risk of terrorist attacks, incidents involving hazardous materials, and other matters that might implicate homeland security. Terrorist attacks and other homeland security incidents may well have a major effect on the general public and the environment broadly, and for some companies these risks may involve nothing more than broad social and political issues. However, because homeland security concerns are so much a part of the regular and ordinary work of railroad companies, in BNSF's case these risks require the Company's daily attention.

Moreover, the Proposal's reference to "homeland security incidents" encompasses a wide range of security considerations separate from and in addition to a potential "terrorist attack" that BNSF must address every day. In fact, the security incidents over which the DHS has jurisdiction are broad. In creating the DHS, Congress specified that two of the Department's "primary responsibilities" are "border and transportation security" and "emergency preparedness and response." Homeland Security Act of 2002, section 101(b)(2)(C) and (D). Thus, among the

responsibilities transferred to the DHS were the Federal Emergency Management Agency ("FEMA"), the United States Customs Service and the Animal and Plant Health Inspection Service. Homeland Security Act of 2002, sections 402 and 502. Recognizing that it is responsible for responding to incidents that include but are not limited to potential terrorist attacks, FEMA has established the National Incident Management System under which "first responders from different jurisdictions and disciplines can work together to respond to natural disasters and emergencies, including acts of terrorism." *See* Summary, Draft Revised NIMS Document (August 2007), *available at* http://www.fema.gov/emergency/nims/nims_doc.shtm. The DHS's FEMA operations assist in preparing for and responding to incidents such as earthquakes, floods, hurricanes, landslides, thunderstorms, tornados, wild fires and winter storms.[2]

In order to implement the Proposal by reporting on all of the Company's efforts to safeguard its operations from homeland security incidents, the Company would need to address:

- its preparations for maintaining operations, avoiding injuries and assisting in response to natural disasters such as earthquakes, floods, hurricanes, landslides, thunderstorms, tornados, wild fires and winter storms;

- its efforts to secure against incidents involving avoidance of tariffs and customs duties or smuggling of contraband and counterfeit merchandise in violation of U.S. customs rules; and

- its actions to protect and inspect agricultural products and livestock that it transports to ensure that there is not an incident where tainted or diseased cargo crosses the borders into or is transported across our country.

Safeguarding the safety and security of the railroad against these types of incidents is an important, but ordinary and day-to-day aspect, of the Company's operations. As stated above, the Company dedicates considerable resources towards efforts to avoid, prepare for, respond to and minimize any impact these types of incidents could have on the Company, its employees, the communities it serves, and our country. Thus, the implementation of security measures to safeguard operations from the wide variety of incidents overseen by the Department of Homeland Security is a central and routine element of the Company's ordinary business. Regardless of whether the Company's efforts to safeguard its assets from a potential terrorist attack transcends the Company's ordinary business, the Proposal clearly also requests that the Company report on actions it has taken to safeguard the security of its operations from incidents and threats that are routine and that have been faced by railroads for more than 150 years. Therefore, given the unique features of the railroad industry, a

[2] Terrorism is only one of seventeen types of incidents that FEMA addresses, as reported on its homepage. *See* http://www.fema.gov/index.shtm

review of BNSF's safety procedures as they relate to terrorism and homeland security is an ordinary business matter under Rule 14a-8(i)(7).

In addition to the precedents cited in the No-Action Request, we have identified a number of SEC staff no-action precedents in which the respective proposals could be read to implicate broad social policy issues, but because of the nature of the companies' businesses, were held to pertain to ordinary business matters that the companies dealt with on a daily basis. For example, in *Verizon Communications Inc.* (Feb. 22, 2007), the proposal at issue asked Verizon to publish "a report to shareholders in six months, at reasonable cost and excluding confidential and proprietary information, which describes the overarching technological, legal and ethical policy issues surrounding the disclosure of customer records and communications content to (1) the Federal Bureau of Investigation, NSA and other government agencies without a warrant and (2) non-governmental entities (e.g. private investigators) and their effect on the privacy rights of Verizon's MCI long-distance customers." This proposal was made shortly after the enactment of various executive orders that gave government agencies broad leeway to request companies like Verizon to disclose a variety of private customer information. This proposal was held to be excludable as pertaining to an ordinary business matter, because it related to the protection of customer information, which is an activity that Verizon undertakes on a daily basis. This decision is analogous to BNSF's case in two respects. First, as a telecommunications company, Verizon is in the business of facilitating conversations between its customers, and the efforts that it takes to safeguard those communications is a matter that Verizon deals with on a daily basis. Likewise, BNSF is in the business of transporting other people's cargo, and the efforts that it takes to ensure the safety of that service is a matter that it must analyze every day. Second, the *Verizon* decision demonstrates that while a proposal may raise broad social issues, the manner in which a company attempts to militate against the risks created by those issues on a daily basis can qualify as an ordinary business matter. Specifically, the proposal in *Verizon* related to information disclosures that the government asked of Verizon as part of a focused effort to prevent future terrorist attacks. Ordinarily, issues like dissemination of personal information and the right to informational privacy are topics of broad social and ethical discussion. However, because the safety of Verizon's customers' personal information is integral to Verizon's day-to-day business, the steps that Verizon took to deal with the risk of government requests for disclosure was held to be an ordinary business matter. In this case, the threat of terrorism compromises the safety of BNSF's railroads and the steps the Company takes to manage that risk is also an ordinary business matter.

The proposal in *Newmont Mining Corp.* (Feb. 5, 2005) which was held excludable as an ordinary business matter (specifically, as an evaluation of risk) is also very similar to the Proposal in this case. In *Newmont Mining*, the proposal asked management to "review its policies concerning waste disposal at its mining operations in Indonesia, with a particular reference to potential environmental and public health risks incurred by the company by these policies, and to report to shareholders on the findings of this review." By focusing on "environmental and public health risks," the proponent in *Newmont Mining* attempted to cast the proposal as a significant social policy issue that could escape the ordinary business matter exception. However, the Staff recognized that

because waste disposal was such a fundamental aspect of Newmont's day-to-day operations, the proposal warranted exclusion. In this instance, the Proponent has likewise attempted to focus on public and environmental risks and harm by giving considerable attention to those matters in both the Proposal's supporting statement and in the Proponent's Response. Regardless of other interests in these matters, however, they are for the Company matters that require ordinary and daily attention. As with the proposal in *Newmont Mining*, the Proposal implicates an assessment of the risks faced by BNSF's operations in the course of managing its regular business operations (as such an assessment is a necessary component of its "efforts to safeguard the security of [its] operations arising from a terrorist attack and/or other homeland security incidents") and should therefore be excluded.

Additionally, the proposal in *Wal-Mart Stores, Inc.* (Mar. 24, 2006) also provides a strong basis for comparison. That proposal asked the company to "publish a report evaluating Company policies and procedures for systematically minimizing customers' exposure to toxic substances in products" that Wal-Mart sells to consumers. The SEC allowed Wal-Mart to exclude the proposal because it pertained to an ordinary business matter. As Wal-Mart discussed in its no-action request, even though the proposal touched on "a socially significant issue," it could not possibly be viewed as a matter that was proper for shareholder oversight because it dealt with an issue that was entirely wrapped up in the company's complex daily operations. Wal-Mart sells a myriad of products, some of which carry an inherent risk of exposing the user to toxins; the decisions that Wal-Mart makes with respect to ensuring that its customers are not harmed by those products are "complex business considerations that are outside the knowledge and expertise of shareholders." Just as Wal-Mart was asked to prepare a report on the steps it had taken to minimize its customers' exposure to the dangers that are innate to its products, BNSF has been asked to report on the steps it has taken to minimize its customers' exposure to one of the dangers that is innate to the service that it provides. The efforts that BNSF has made in this regard are likewise complex, and not a proper subject for shareholder review.

Finally, the Staff has consistently concurred that a proposal may be excluded in its entirety when it addresses both ordinary and non-ordinary business matters. Recently, the Staff affirmed this position in *Peregrine Pharmaceuticals Inc.* (July 31, 2007), concurring with the exclusion of a proposal under Rule 14a-8(i)(7) recommending that the board appoint a committee of independent directors to evaluate the strategic direction of the company and the performance of the management team. The Staff noted "that the proposal appears to relate to both extraordinary transactions and non-extraordinary transactions. Accordingly, we will not recommend enforcement action to the Commission if Peregrine omits the proposal from its proxy materials." In *General Electric Co.* (Feb 10, 2000), because a portion of the proposal related to ordinary business matters, the Staff concurred with the exclusion of a proposal requesting that the company (i) discontinue an accounting technique, (ii) not use funds from the GE Pension Trust to determine executive compensation, and (iii) use funds from the trust only as intended. *See also Medallion Financial Corp.* (May 11, 2004) (concurring with the exclusion of a proposal requesting that the company consult an investment bank to evaluate ways to

increase shareholder value, and noting that it "appears to relate to both extraordinary transactions and non-extraordinary transactions"); *Wal-Mart Stores, Inc.* (Mar. 15, 1999) (concurring with the exclusion of a proposal requesting a report to ensure that the company did not purchase goods from suppliers using unfair labor practices because the proposal also requested that the report address ordinary business matters). In this case, the Proposal might touch on various non-ordinary matters, like public and environmental harm, but the thrust of the resolution asks BNSF to report on "the security *of [its] operations*" which, as demonstrated above, is clearly an ordinary business matter. Because the Proposal's focus remains as such, it may be excluded under Rule 14a-8(i)(7).

B. The Proposal is excludable because it seeks an evaluation and report on actions BNSF has taken to minimize the risks and liabilities of its operations.

As illustrated by the precedents cited above, even if a given shareholder proposal touches on broader social policy issues, it may be excluded if it also implicates a company's ordinary business. Moreover, the fact that even one prong of a proposal may invoke a significant policy issue does not automatically mean that prong does not involve ordinary business matters. For example, in *General Motors Corp.* (Apr. 4, 2007) the Staff excluded a proposal that addressed the social policy issue of executive compensation, noting that "while the proposal mentions executive compensation, the thrust and focus of the proposal is on ordinary business matters." Indeed, the Staff established its standard for determining whether shareholder proposals implicate social policy issues or ordinary business matters in Staff Legal Bulletin 14C:

> To the extent that a proposal and supporting statement focus on the company engaging in an internal assessment of the risks or liabilities that the company faces as a result of its operations that may adversely affect the environment or the public's health, we concur with the company's view that there is a basis for it to exclude the proposal under rule 14a-8(i)(7) as relating to an evaluation of risk. To the extent that a proposal and supporting statement focus on the company minimizing or eliminating operations that may adversely affect the environment or the public's health, we do not concur with the company's view that there is a basis for it to exclude the proposal under rule 14a-8(i)(7).

In light of this standard, the Staff has recently issued a number of no-action letters with regards to proposals that are similar to the Proposal, in that they focus on an "evaluation of risks" resulting from steps the companies were taking to address issues that could be viewed as implicating significant social policy matters. For example, in *Centex Corp.* (May 14, 2007), the Staff allowed the company to exclude a shareholder proposal requesting a report on how Centex was "responding to rising regulatory, competitive and consumer pressure to address global warming," as that disclosure was simply an evaluation of risk. In *The Ryland Group, Inc.* (Feb. 13, 2006), the Staff concurred that the company could exclude a proposal requesting the company to assess its response to rising regulatory, competitive and public pressure to increase

energy efficiency. *See also Ace Ltd.* (Mar. 19, 2007), (concurring in the exclusion of a proposal requesting a report on "the company's strategy and actions related to climate change, including . . . steps taken by the company in response to climate change").

Moreover, shareholder proposals need not explicitly request an "evaluation of risk" to be excludable on that basis under Rule 14a-8(i)(7). For example, in *Pulte Homes Inc.* (Mar. 1, 2007), the Staff concurred that the company could exclude as relating to "evaluation of risk" a proposal requesting that the company "assess its response" to rising regulatory, competitive, and public pressure to increase energy efficiency. *See also Wells Fargo & Co.* (Feb. 16, 2006) (allowing exclusion of a proposal requesting a report on the effect on Wells Fargo's business strategy of the challenges created by global climate change called for an evaluation of risk); *The Dow Chemical Co.* (Feb. 23, 2005) (concurring with the exclusion of a shareholder proposal requesting a report describing the reputation and financial impact of the company's response to pending litigation because it related to an evaluation of risks and liabilities); *American International Group, Inc.* (Feb. 19, 2004) (concurring that the company could exclude a proposal that requested the board of directors to report on "the economic effects of HIV/AIDS, tuberculosis and malaria pandemics on the company's business strategy," because it called for an evaluation of risks and benefits).

As mentioned in the No-Action Request and in BNSF's Response, the Proponent has tried to cast its Proposal as a social policy issue by avoiding all references to financial risk. However, the thrust and focus of the Proposal remains on a risk that the Company may face as a result of its daily operations. It does not request a report on "minimizing or eliminating operations that may adversely affect the environment or the public's health." Therefore, under the standard set forth in Staff Legal Bulletin 14C, the Proposal qualifies as an evaluation of risk and may be excluded under Rule 14a-8(i)(7).

III. BNSF may exclude the Proposal in reliance on Rule 14a-8(i)(10) because it has been substantially implemented.

Rule 14a-8(i)(10) permits a company to exclude a stockholder proposal from its proxy materials "[i]f the company has already substantially implemented the proposal." The Commission stated in 1976 that the predecessor to Rule 14a-8(i)(10) was "designed to avoid the possibility of shareholders having to consider matters which already have been favorably acted upon by the management." Exchange Act Release No. 12598 (July 7, 1976). When a company can demonstrate that it already has taken actions to address each element of a stockholder proposal, the Staff has concurred that the proposal has been "substantially implemented" and may be excluded as moot. *See Hewlett-Packard Company* (Dec. 11, 2007); *see, e.g., Exxon Mobil Corp.* (Jan. 24, 2001); *The Gap, Inc.* (Mar. 8, 1996); and *Nordstrom, Inc.* (Feb. 8, 1995). Moreover, a proposal need not be "fully effected" by the company in order to be excluded as substantially implemented. *See* Exchange Act Release No. 34-20091, at § II.E.6. (Aug. 16, 1983); *see also* Exchange Act Release No. 40018 at n.30 and accompanying text (May 21, 1998);

As stated in Section I of this letter, BNSF believes that the Proposal would require it to disclose information in violation of federal regulations and should be excluded on those grounds. If, on the other hand, the Proposal had been written to exclude disclosures that would violate the law, BNSF believes that it would have substantially complied with the Proposal, as such information has already been disclosed to the public.

Specifically, the Company already provides information that is responsive to the Proposal on its website and through other media. It should not be required to repackage or restate that same information in a proxy statement. Due to the Proposal's lack of specificity as to the nature of the information requested, the Company believes that the information it currently provides to the public addresses each element of the Proposal and thus "substantially implements" the Proposal.

The Company's website (www.bnsf.com) (under the "Customer Tools" tab) devotes an entire section to "Resource Protection." The links and information found therein detail a number of measures that BNSF has taken to ensure the safety of its trains and the cargo that it transports, including its "On Guard Program" and its "Trespasser Abatement Program," its participation in the e-RAILSAFE program in which third-party contractors are screened, and its participation in the Customs-Trade Partnership Against Terrorism (C-TPAT), a cooperative endeavor with the U.S. Customs Service to develop, enhance, and maintain effective security processes throughout the global supply chain. BNSF was also an industry leader in developing the first community-based rail fan reporting program called Citizens for Rail Security (CRS). This program includes security measures that are pertinent to terrorist and/or other homeland security threats and enlists the public in safely helping to address terrorist and other threats and to protect the railroad by reporting security violations, trespassers or unusual occurrences. Since its inception, more than 7,700 rail fans have joined CRS in helping protect the railroad by reporting security violations, trespassers or unusual occurrences. These programs, in addition to others listed on this website, all relate to security measures that BNSF has taken to protect its railroad from all kinds of safety risk, including terrorist threats. Also, BNSF's website provides information regarding BNSF's Police Solutions Team and its Load and Ride Solutions Team, both of which are in place to help mitigate against unforeseen safety risks. BNSF's website also has a search function, and when one runs a search for "Homeland Security," the function yields over 40 results, most of which are pertinent to the Proponent's information request. Finally, information on BNSF security precautions as they relate to employees, is available through BNSF employee publications which can be found on BNSF's public website. All told, BNSF's website already reports on its commitment to safeguard the security of its operations in the following areas:

- Public safety,
- Hazardous Materials Safety,
- Track Maintenance and Crossing Safety;

- Employee safety, and
- Rail security.

As demonstrated on the website and other disclosures, the Company's efforts to safeguard the security of its operations include a highly-specialized secure network, which provides enhanced monitoring for state homeland security and law enforcement officials with respect to the status of the Company's trains and rail cars. The Company also provides for joint training among the Company's experts and law enforcement officials trained to respond to security incidents.

Thus, the Company's employees, investors, and the public at-large have access at any time to information that the Company believes would be responsive to the Proposal. To require the Company to include this or more detailed Sensitive Security Information again in its Proxy Statement is simply duplicative, unnecessary and could potentially damage the Company's ability to effectively protect its employees and critical infrastructure.

IV. Conclusion

For the foregoing reasons, we request your confirmation that the Staff will not recommend any enforcement action to the Commission if the Proposal is omitted from BNSF's 2008 proxy materials.

If the Staff has any questions with respect to the foregoing, or if for any reason the Staff does not agree that BNSF may omit the Proposal from its 2008 proxy materials, please contact me at (212) 474-1131. I may also be reached by facsimile at (212) 474-3700 and would appreciate it if you would send your response to us by facsimile to that number as well as to BNSF at (817) 352-2397. The Proponents' legal representative, C. Thomas Keegel, may be reached by telephone at (202) 624-6800 and at the International Brotherhood of Teamsters, 25 Louisiana Avenue, NW, Washington, DC 20001. We request that the Staff notify the undersigned if it receives any correspondence on the Proposal from the Proponent or other persons, unless that correspondence has specifically confirmed to the Staff that BNSF or its undersigned counsel have timely been provided with a copy of the correspondence. In addition, we agree to promptly forward to the Proponent any response from the Staff to this motion for reconsideration that the Staff transmits by facsimile to us or BNSF only.

Please acknowledge receipt of this letter and the enclosures by date-stamping the enclosed copy of this letter and returning it in the enclosed self addressed stamped envelope.

Very truly yours,

William V. Fogg

Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F Street, N.E.
Washington, D.C. 20549

Encls.

UPS OVERNIGHT AND EMAIL

Copies w/encls. to:

Thomas J. Kim
Associate Director and Chief Counsel
Office of the Chief Counsel
Division of Corporation Finance
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549

Jonathan Ingram
Deputy Chief Counsel
Office of the Chief Counsel
Division of Corporation Finance
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549

C. Thomas Keegel
General Secretary-Treasurer
International Brotherhood of Teamsters
25 Louisiana Avenue, NW
Washington, D.C. 20001

Roger Nober
Executive Vice President Law and Secretary
Burlington Northern Santa Fe Corporation
2650 Lou Menk Drive, F12
Forth Worth, TX 76131

James Dunn
Deputy General Manager, Freight Rail
TSA-28
Transportation Security Administration
601 South 12th Street
Arlington, VA 22202-4220

EXHIBIT A

INTERNATIONAL BROTHERHOOD OF TEAMSTERS

JAMES P. HOFFA
General President

25 Louisiana Avenue, NW
Washington, DC 20001

C. THOMAS KEEGEL
General Secretary-Treasurer

202.624.6800
www.teamster.org

Roger Nober
JUL 02 2007

June 28, 2007

BY FACSIMILE: (817) 352-7171
BY UPS NEXT DAY

Mr. Roger Nober, Corporate Secretary
Burlington Northern Santa Fe Corporation
2650 Lou Menk Drive, Fl 2
Fort Worth, TX 76131

Dear Mr. Nober:

I hereby submit the following resolution on behalf of the Teamsters General Fund, in accordance with SEC Rule 14a-8, to be presented at the Company's 2008 Annual Meeting.

The General Fund has owned 60 shares of Burlington Northern Santa Fe Corporation continuously for at least one year and intends to continue to own at least this amount through the date of the annual meeting. Enclosed is relevant proof of ownership.

Any written communication should be sent to the above address via U.S. Postal Service, UPS, or DHL, as the Teamsters have a policy of accepting only Union delivery. If you have any questions about this proposal, please direct them to Louis Malizia of the Capital Strategies Department, at (202) 624-6930.

Sincerely,

C. Thomas Keegel

C. Thomas Keegel
General Secretary-Treasurer

CTK/lm
Enclosures

RESOLVED: That the shareholders of Burlington Northern Santa Fe Corporation ("BNSF" or "Company") hereby request that the Board of Directors make available, omitting proprietary information and at reasonable cost, in BNSF's annual proxy statement, by the 2009 annual meeting, information relevant to the Company's efforts to safeguard the security of their operations arising from a terrorist attack and/or other homeland security incidents.

SUPPORTING STATEMENT: Since BNSF is involved with the transportation, storage and handling of hazardous materials including chemicals, explosives, radioactive materials, gases, poisons and corrosives, it is critical that shareholders be allowed to evaluate the steps the Company has taken to minimize risks to the public arising from a terrorist attack or other homeland security incident.

The United States Naval Research Lab reported that one 90-ton tank car carrying chlorine, if targeted by an explosive device, could create a toxic cloud 40 miles long and 10 miles wide, which could kill 100,000 people in 30 minutes. Safeguarding U.S. security should be a priority for BNSF, especially since the 9/11 attacks have crystallized the vulnerability of our nation's transportation infrastructure. Further, the train bombings in London and Madrid, where hundreds of people died and thousands were injured, highlight the vulnerability of railways as prime targets for terrorist attacks.

Citizens for Rail Safety, Inc. (CRS), a national non-profit public interest organization comprised of transportation consultants and concerned citizens advocating for national railroad safety and efficiency, unveiled a Penn State University report on June 12, 2007, exposing glaring holes in rail security and therefore, opportunities for terrorism in the U.S. system. The report, "Securing and Protecting America's Rail System: U.S. Railroads and Opportunities for Terrorist Threats" uncovered the need for an increase in terrorism preparedness training for rail workers in order to improve rail security and protect the public.

Rail workers throughout our Company report that BNSF has failed to implement significant security improvements to deter or respond to a terrorist attack on the U.S. rail network, which could potentially devastate communities in our country and destroy our Company.

While other rail companies, such as Canadian Pacific Railway, have disclosed extensive detail of both security actions taken to protect their infrastructure and personnel and their cost, BNSF makes only passing mention in their 10-K of efforts to improve security operations in order to tackle the threat to the railroad in high risk areas like Chicago, Houston and San Francisco. These disclosures are particularly important in light of BNSF's history of accidents involving hazardous materials, which totaled 243, the highest number of accidents at a U.S. rail company in 2006 [Gibbons, Timothy. *CSX Hit with 3 Accidents Already this Year.* 2/26/2007].

The lack of such information prevents shareholders from assessing crucial information relating to the protection of our country, our Company and our workers.

We urge you to support disclosure of homeland security measures at BNSF by voting **FOR** this proposal.

AMALGAMATED BANK.

June 26th, 2007

Mr. Roger Nober
Corporate Secretary
Burlington Northern Santa Fe Corporation
2650 Lou Menk Dr Fl 2
Fort Worth TX 76131

Re: Burlington Northern Santa Fe Corp. – Cusip # 12189t104

Dear: Mr. Nober:

Amalgamated Bank is the record owner of 60 shares of common stock (the "Share") of Burlington Northern Santa Fe Corporation, beneficially owned by the International Brotherhood of Teamsters General Fund. The shares are held by Amalgamated Bank at the Depository Trust Company in our participant account # 2352. The International Brotherhood of Teamsters General Fund has held the Shares continuously since 05/31/2005 and intends to hold the shares through the shareholders meeting.

If you have any questions or need anything further, please do not hesitate to call me at (212) 895-4971.

Very truly yours,

Hugh A. Scott
First Vice President
Amalgamated Bank

EXHIBIT B

Jeffrey T. Williams
Senior General Attorney

Burlington Northern
Santa Fe Corporation
P. O. Box 961039
Fort Worth, Texas 76161-0039
2500 Lou Menk Drive
Fort Worth, Texas 76131-2828
tel 817 352-3468
fax 817 352-2397
Jeffrey.williams@bnsf.com

RECEIVED
2007 NOV 21 AM 10:44
OFFICE OF CHIEF COUNSEL
CORPORATION FINANCE

November 19, 2007

VIA OVERNIGHT MAIL

Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F Street, N.E.
Washington, D.C. 20549

Re: Burlington Northern Santa Fe Corporation - Shareholder Proposal Submitted by the International Brotherhood of Teamsters' General Fund

Ladies and Gentlemen:

On behalf of Burlington Northern Santa Fe Corporation ("BNSF") and pursuant to Rule 14a-8(j) under the Securities Exchange Act of 1934, I hereby request confirmation that the Staff of the Securities and Exchange Commission will not recommend enforcement action if, in reliance on Rule 14a-8, the Company excludes a proposal submitted by the International Brotherhood of Teamsters' General Fund (the "Proponent") from the proxy materials for BNSF's 2008 annual shareholders' meeting, which we expect to file in definitive form with the Commission on or about March 14, 2008.

We received a notice on behalf of the Proponent dated June 28, 2007, submitting the following proposal for consideration at our 2008 annual shareholders meeting (a copy of which, together with the supporting statement, is attached as Exhibit A) (the "Proposal") :

> Resolved: That the shareholders of Burlington Northern Santa Fe Corporation ("BNSF" or "Company") hereby request that the Board of Directors make available, omitting proprietary information and at reasonable cost, in BNSF's annual proxy statement, by the 2009 annual meeting, information relevant to the Company's efforts to safeguard the security of their operations arising from a terrorist attack and/or other homeland security incidents.

Pursuant to Rule 14a-8(j), I have enclosed six copies of the proposal and this letter, which sets forth the grounds upon which we deem omission of the proposal to be proper. Pursuant to Rule 14a-8(j), a copy of this letter is being sent to the Proponent to notify it of our intention to omit the proposal from our 2008 annual meeting proxy materials.

We believe that the Proposal may be properly omitted from BNSF's 2008 proxy materials pursuant to Rule 14a-8 for the reasons set forth below.

BASES FOR EXCLUSION

I. BNSF may exclude the Proposal in reliance on Rule 14a-8(i)(7) because it relates to ordinary business operations.

Rule 14a-8(i)(7) permits a company to exclude a stockholder proposal if it pertains to "a matter relating to the company's ordinary business operations." The Commission has stated that the purpose of Rule 14a-8(i)(7) is "to confine the resolution of ordinary business problems to management and the board of directors, since it is impracticable for shareholders to decide how to solve such problems at an annual shareholders meeting." *SEC Release No. 34-40018* (May 28, 1998). This exception extends to proposals that simply request additional disclosure from a company (as opposed to the taking of a particular action), so long as the "subject matter" of that disclosure relates to a matter of ordinary business. *See Johnson Controls, Inc* (Oct. 26, 1999); *see also Otter Tail Corp.* (Jan. 13, 2004)

A. The Proposal Meets the SEC's Criteria for Qualifying as an Ordinary Business Operation

According to SEC Release No. 34-40018 the two "central considerations" in determining whether the ordinary business exception of Rule 14a-8(i)(7) applies are (i) whether the proposal relates to tasks that are "so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight," and (ii) "the degree to which the proposal seeks to 'micro-manage' the company." *SEC Release No. 34-40018.* Exclusion would be appropriate where the proposal "prob[es] too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment." *Id.* (citing *Exchange Act Release No. 12999* (Nov. 22, 1976)). Additionally, even if a given proposal simply requests a special informational report, as opposed to some sort of specific action, the proposal is still excludable under Rule 14a-8(i)(7) if "the *subject matter* of the special report . . . involves a matter of ordinary business" *SEC Release No. 34-20091* (Aug. 16, 1983) (emphasis added). These factors demonstrate that the ordinary business exception applies to the Proponent's proposal.

BNSF owns one of the largest railroads in North America, with approximately 32,000 route miles of track in 28 states and two Canadian provinces. The security and safety measures employed to protect our employees and our operations are designed to prevent, prepare for, and mitigate any event that could affect our rail operations and the safety of our employees, contractors and customers, and the communities through which we operate. While terrorist attacks are extraordinary events, the *threat* of terrorism is an ongoing and ever-present reality that requires *daily* attention. Accordingly, various management efforts to safeguard BNSF from terrorism and other risks to homeland security are incorporated in management's daily functions. These efforts are integrally related to management's ordinary day-to-day programs and protocols to protect our operations from a variety of risks, including homeland security incidents.

and implementation of the company's new safety technologies, because it pertained to ordinary business. *See also, AMR Corporation* (Apr. 2, 1987) (concluding that a proposal relating to the nature and extent of review of the safety of that company's airline operations was a matter relating to its ordinary business operations); *Union Pacific Corporation* (Dec. 16, 1996) (finding that the railroad company could omit proposals requesting information on railroad safety systems). Likewise, the Commission has generally found that the ordinary business exception also applies to proposals requesting companies to provide reports which assess the risk of external events on those companies. For example, in *Pfizer Inc.* (Jan. 24, 2006), the SEC allowed the company to exclude a proposal requesting a report on the economic effects of certain pandemics and the company's efforts to combat these effects, because such a report would require the company to engage in an internal evaluation of external risks, which qualified as an ordinary business matter. *See also, The Chubb Corp.* (Jan. 25, 2004) (finding that the company could exclude a proposal for a report regarding the impact of climate changes on the business); *The Ryland Group, Inc.* (Feb. 13, 2006) (finding that the company could exclude a proposal for a report regarding the impact on the business of "rising regulatory, competitive, and public pressure to increase energy efficiency"). A report on the efforts to safeguard operations against terrorist attacks falls into both of these categories, as it pertains to the overall safety of our operations, and relates to the effect that an uncontrollable outside event (terrorism) has on BNSF.

C. The Proposal Requests Information that is not a Broad Question of Policy, But Instead, a Matter of Ordinary Business Operations

Further, to the extent that the Proponent may argue that these matters could affect the public's health and thus include significant policy issues, see *Staff Legal Bulletin No. 14C* (June 28, 2005). There, the Commission distinguishes proposals that deal generally with the risk or liability of operations to the company from those that focus on minimizing or eliminating particular operations that may adversely affect the environment or the health of the general public:

> To the extent that a proposal and supporting statement focus on the company engaging in an internal assessment of the risks or liabilities that the company faces as a result of its operations that may adversely affect the environment or the public's health, we concur with the company's view that there is a basis for it to exclude the proposal under rule 14a-8(i)(7) as relating to an evaluation of risk. To the extent that a proposal and supporting statement focus on the company minimizing or eliminating operations that may adversely affect the environment or the public's health, we do not concur with the company's view that there is a basis for it to exclude the proposal under rule 14a-8(i)(7).

The Staff Bulletin is consistent with many no-action letters in which the Staff agreed with the company's position that analysis of policy risks and benefits is a fundamental and ongoing part of a company's ordinary business operations. *See, e.g., Dow Chemical* (Feb. 23, 2005); *Xcel Energy Inc.* (Apr. 1, 2003). Like similar proposals which the Commission has determined to be excludable under Rule 14a-8(i)(7), the Proposal and Supporting Statement in this instance focus on potential risks and liabilities to BNSF, not on minimizing operations that affect the environment or public health, and thus provide a basis for exclusion "as relating to an evaluation of risk." Specifically, the Supporting Statement references the harm that an outside terrorist

event could cause to the railroad, its workers, and the public at large, and the Proposal itself requests a report on BNSF's efforts to "safeguard the security of their operations arising from a terrorist attack and/or other homeland security incidents." Such a report would not focus on any of BNSF's operations that may adversely affect the public, but rather on the risks and liabilities the company faces as a result of terrorist threats. Analogously, in *Pfizer Inc.*, a proposal requesting a report on the economic effect that various pandemics could have on the company was viewed as an evaluation of risk, and therefore an ordinary business matter. In *General Electric Co.*, (Jan. 13, 2006), the SEC excluded a proposal requesting a report on the risk to the company's reputation as a result of increased outsourcing and offshoring to other countries. Accordingly, a report on BNSF's responses to and safeguards from terrorism would require precisely the sort of risk assessment that qualifies as an ordinary business matter.

Moreover, proposals that merely touch on or implicate social policy issues are not exempt from the ordinary business exception. To the contrary, they are still excludable if they revolve around a company's ordinary business operations. For example, in *General Electric Co* (Feb. 3, 2005), a proposal that touched on the social policy of relocating jobs to foreign countries was still excluded because it related to management of the workforce, which is an ordinary business matter. *See also Newmont Mining Corp* (Feb. 4, 2004) (finding that it was unnecessary to consider social policy implications, because the proposal requested a report on financial risks and environmental liabilities, which were ordinary business matters). Indeed, so long as *any* portion of a proposal implicates a company's ordinary business operations, it is excludable under Rule 14a-8(i)(7). *See Medallion Financial Corp.* (May 11, 2004) (finding that even though a proposal pertained to both extraordinary transactions and non-extraordinary transactions, the entire proposal could be excluded because the non-extraordinary transactions were matters of ordinary business). Therefore, even if the Proponent's Proposal could be described as touching on a social policy or other ancillary issue, the entire Proposal is still excludable because, as outlined above, it relates to BNSF's ordinary business operations.

Finally, as an ancillary matter, many of BNSF's counter terrorism measures taken to safeguard the company, its railroads, and employees must remain confidential and are required to be kept so through arrangements with appropriate government agencies (e.g., U. S. Department of Homeland Security) and connecting carriers. In many discussions with the Transportation Security Administration of the U.S. Department of Homeland Security, BNSF's overall Security Management Plan has been deemed Security Sensitive Information (SSI). Countermeasures contained within the plan are highly confidential and must be safeguarded. Public knowledge of these measures would negate the purpose of the measures and make BNSF more vulnerable to terrorist attacks. By making the information available to shareholders, BNSF would also be making the information available to persons the programs were designed to target, thus undermining the efficacy of its efforts.

II. BNSF may exclude the Proposal in reliance on Rule 14a-8(i)(3) because it is materially misleading in violation of Rule 14a-9.

Rule 14a-8(i)(3) permits a company to exclude a proposal "[i]f the proposal or supporting statement is contrary to any of the Commission's proxy rules, including Rule 14a-9, which prohibits materially false or misleading statements in proxy soliciting materials." Moreover, the

Commission has stated that "when a proposal and supporting statement will require detailed and extensive editing in order to bring them into compliance with the proxy rules, [the Commission] may find it appropriate for companies to exclude the entire proposal, supporting statement, or both, as materially false or misleading." *SEC Staff Legal Bulletin No. 14* (July 13, 2001). In this case, the Supporting Statement would need to be greatly altered to comply with the proxy rules, so the Proposal is excludable on the grounds that the Supporting Statement is materially misleading under Rule 14a-8(i)(3). The Proponent's proposal is misleading in three respects.

A. Reference to Penn State University Report

The Supporting Statement refers to "a Penn State University report on June 12, 2007, exposing glaring holes in rail security and therefore, opportunities for terrorism in the U.S. system."

The Proponent's statement gives the impression that BNSF is partly responsible as one of the "glaring holes in rail security." However, this impression is entirely false since the Penn State report never identifies BNSF or our operations as vulnerable to terrorist attacks. Rather, the Penn State report (available at http://www.citizensforrailsafety.org/docs/PennStateStudy.pdf) cites BNSF's programs as examples of the types of safety programs recommended for the rail industry. Specifically:

- The report recommends "[e]fforts to involve the general public and the rail enthusiast, such as the BNSF's Citizens for Rail Security program, should be supported and expanded". (p. 9)
- As an example of an industry response to terrorism, the report notes "[o]ne individual railroad initiative is the Strategic Transportation Asset Tracking System (STAT for short) undertaken by the BNSF to provide real time tracking of high value and other sensitive cargo—interpreted to mean that it could apply to hazmats and to military moves." (p. 35)
- The report recommends that the industry "[c]onsider utilizing railfans as additional eyes and ears for the railroads. While in the past there have been contentious issues, their interest is obvious and their knowledge of railroad operations often goes far beyond that of the casual observer. BNSF has a program to register railfans and the AAR has an embryonic concept on its website. A useful metaphor is that this becomes the railroads' equivalent of the neighborhood watch." (p. 59)

The Proponent attempts to cite generally to a report assessing the risks of terrorist activity towards the U.S. rail industry in the hope that investors will demand more information from BNSF. However, even a brief review of the Penn State report shows that the report supports many of BNSF's counter-terrorism efforts and in no way targets BNSF as deficient in its counter-terrorism efforts.

B. References to BNSF's Rail Workers

The Proponent claims that "[r]ail workers throughout our Company report that BNSF has failed to implement significant security improvements to deter or respond to a terrorist attack on

the U.S. rail network, which could potentially devastate communities in our country and destroy our Company." The statement contains vague and unquantifiable terminology, such as "significant security improvements" and "potentially devastate." Without proper authority for its contention or more specific measures of the proposed risk, the statement is not verifiable and thus merely a thinly veiled attempt to paint BNSF employees as a whole as disgruntled and concerned for their safety.

Also, this statement is highly suspect because it implies that rail workers are privy to sufficient information to enable them to evaluate BNSF's counter-terrorism efforts. However, many of BNSF's efforts and successes are the result of high level programs and strategies known only by BNSF management. Moreover, many of BNSF's counter-terrorism measures and the intelligence received on a restricted access basis from government agencies cannot be disclosed outside of management due to government mandate or agreements with other carriers regarding certain jointly-developed and implemented strategies. Other than equipping BNSF workers with information necessary to implement the counter-terrorism programs, certain aspects of the programs have not been disclosed in order to maintain their efficacy. Accordingly, it is imperative that many aspects of BNSF's anti-terrorism strategies remain confidential.

C. References to Other Rail Companies

The Supporting Statement contrasts BNSF with "other rail companies, such as Canadian Pacific Railway," which "have disclosed extensive detail of both security actions taken to protect their infrastructure and personnel and their cost," while "BNSF makes only passing mention in its 10-K of efforts to improve security operations in order to tackle the threat to the railroad in high risk areas like Chicago, Houston and San Francisco."

The Proponent's statement gives the misleading impression that BNSF lags behind its peers in disclosing its counter terrorism measures. However, upon review of the 2006 10-K reports of our main competitors (Union Pacific Corporation, Kansas City Southern, Norfolk Southern Corporation, and CSX Corporation), there are no disclosures related to terrorism or counter-terrorism efforts other than brief risk statements that the heightened risk of terror may affect the company's operations; otherwise, our competitors are silent. Therefore, BNSF's disclosures are actually consistent with the U.S. industry standard.

III. Conclusion

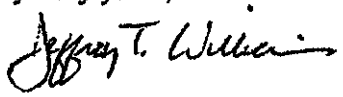
For the foregoing reasons, I request your confirmation that the Staff will not recommend any enforcement action to the Commission if the Proposal is omitted from BNSF's 2008 proxy materials. To the extent that the reasons set forth in this letter are based on matters of law, pursuant to Rule 14a-8(j)(2)(iii) this letter also constitutes an opinion of counsel of the undersigned as an attorney licensed and admitted to practice in the States of Illinois and Texas.

If the Staff has any questions with respect to the foregoing, or if for any reason the Staff does not agree that we may omit the Proposal from our 2008 proxy materials, please contact me at (817) 352-6050. I may also be reached by facsimile at (817) 352-2397 and would appreciate it if you would send your response to us by facsimile to that number. The Proponents' legal

representative, C. Thomas Keegel, may be reached by telephone at (202) 624-6800 and at the International Brotherhood of Teamsters, 25 Louisiana Avenue, NW, Washington, DC 20001. We request that the Staff notify the undersigned if it receives any correspondence on the Proposal from the Proponent or other persons, unless that correspondence has specifically confirmed to the Staff that BNSF or its undersigned counsel have timely been provided with a copy of the correspondence. In addition, BNSF agrees to promptly forward to the Proponent any response from the Staff to this no-action request that the Staff transmits by facsimile to BNSF only.

Please acknowledge receipt of this letter and the enclosures by date-stamping the enclosed copy of this letter and returning it in the enclosed self-addressed envelope.

Very truly yours,



Jeffrey T. Williams
Senior General Attorney

cc: C. Thomas Keegel
Roger Nober

Enclosures

EXHIBIT C

INTERNATIONAL BROTHERHOOD OF TEAMSTERS

JAMES P. HOFFA
General President

C. THOMAS KEEGEL
General Secretary-Treasurer

25 Louisiana Avenue, NW
Washington, DC 20001

202.624.6800
www.teamster.org

RECEIVED
DEC 10 2007
LAW DEPARTMENT

December 7, 2007

U.S. Securities and Exchange Commission
Office of the Chief Counsel
Division of Corporation Finance
100 F Street, NE
Washington, D.C. 20549-1090

Re: Burlington Northern Santa Fe Corporation's no-action request regarding shareholder proposal submitted by the Teamster General Fund

Dear Sir or Madam:

By letter dated November 19, 2007 (the "No-Action Request"), Burlington Northern Santa Fe Corporation ("BNSF" or the "Company") asked that the Office of Chief Counsel of the Division of Corporation Finance (the "Staff") confirm that it will not recommend enforcement action if the Company omits a shareholder proposal (the "Proposal") submitted pursuant to the Commission's Rule 14a-8 by the Teamster General Fund (the "Fund") from the Company's proxy materials to be sent to shareholders in connection with the 2008 annual meeting of shareholders (the "2008 Annual Meeting").

The Proposal requests that the Company make available, omitting proprietary information and at reasonable cost, in BNSF's annual proxy statement, by the 2009 annual meeting, information relevant to the Company's efforts to safeguard the security of their operations arising from a terrorist attack and/or other homeland security incidents.

The Company contends that it is entitled to exclude the Proposal in reliance on (i) Rule 14a-8(i)(7), arguing that the Proposal deals with matters relating to the

Company's ordinary business operations, and (ii) Rule 14a-8(i)(3), arguing that the Proposal is materially misleading in violation of Rule 14a-9.

We believe that BNSF should not be permitted to exclude the Proposal from its 2008 proxy materials pursuant to Rule 14a-8 for the reasons set forth below.

BASES FOR INCLUSION

I. Rail Security is a Significant Social Policy Issue, Precluding Application of the Ordinary Business Exclusion

We believe that Section I. of BNSF's No-Action Request is predicated on the false understanding that "so long as *any* portion of a proposal implicates a company's ordinary business operations, it is excludable under Rule 14a-8(i)(7)."(See Section I.C., No-Action Request) On the contrary, Staff Legal Bulletin 14C explicitly states: "The fact that a proposal relates to ordinary business matters does not conclusively establish that a company may exclude the proposal from its proxy materials."[1]

BNSF's No-Action Request fails to recognize a critical element of the Staff's interpretation of Rule 14a-8(i)(7)—that the ordinary business exclusion is not applicable to proposals that focus on matters of significant social policy issues, even if such proposals and their supporting statements relate to day-to-day business matters.

A. Significant Social Policy Issues Are Beyond The Realm of Ordinary Business

In 1998, the Commission clarified its approach to applying the ordinary business exclusion (Rule 14a-8(i)(7)), limiting the scope of what is considered ordinary business. In the adopting release (the "1998 Release"),[2] the Commission stated:

> Certain tasks are so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight. Examples include the management of the workforce, such as the hiring, promotion, and termination of employees, decisions on production quality and quantity, and the retention of suppliers. However, proposals relating to such matters but focusing on sufficiently significant social

[1] Staff Legal Bulletin 14C (June 28, 2005).

[2] Exchange Act Release No. 40018 (May 21, 1998)

> policy issues (e.g., significant discrimination matters) generally would not be considered to be excludable, because the proposals would transcend the day-to-day business matters and raise policy issues so significant that it would be appropriate for a shareholder vote.
>
> (footnotes omitted)

By stating that a proposal relating to "[ordinary business] matters but focusing on sufficiently significant social policy issues" is not excludable (emphasis added), the 1998 Release made clear that a subject's status as a significant social policy issue trumps its characterization as an ordinary business matter. A 1976 release introducing the "significant social policy issue" analytic framework (the "1976 Release") described the analytic process similarly:

> Specifically, the term "ordinary business operations" has been deemed on occasion to include certain matters, which have significant policy, economic or other implications inherent in them. For instance, a proposal that a utility company not construct a proposed nuclear power plant has in the past been considered excludable under former sub-paragraph (c)(5). In retrospect, however, it seems apparent that the economic and safety considerations attendant to nuclear power plants are of such magnitude that a determination whether to construct one is not an "ordinary" business matter. Accordingly, proposals of that nature, as well as others that have major implications, will in the future be considered beyond the realm of an issuer's ordinary business operations, and future interpretative letters of the Commission's staff will reflect that view.[3]

The substantial legislative and regulatory activities around rail security, as well as the robust public debate over how to secure our nation's rail infrastructure from terrorist attack, support the assertion that rail security is a significant social policy issue, thus precluding application of the ordinary business exclusion (Rule 14a-8(i)(7)) to the Fund's Proposal. Therefore, while BNSF may rightly assert in Section I.A. the No-Action Request that "the *threat* of terrorism is an ongoing and ever-present reality that requires *daily* attention", the fact that rail security is a significant social policy issue renders the proposal appropriate for a shareholder vote.

---

[3] Exchange Act Release No. 12999 (Nov. 22, 1976).

B. Rail Security Is A Significant Social Policy Issue

Our assertion that rail security is indeed a significant social policy issue is something that the Fund—along with certain Congressional Representatives—took up with the Commission last year.

In 2007, the Fund appealed to the Commission to exercise its discretion under 17 C.F.R.§ 202.1(d) and review a determination by the Division of Corporation Finance that Norfolk Southern Corporation may exclude from its proxy materials a shareholder proposal on rail security submitted by the Fund. The Fund held that the subject matter of the proposal, rail security, is a significant social policy issue and the focus of widespread public debate, precluding application of the ordinary business exclusion.

In response to the Staff's no-action determinations regarding proposals on rail security, Chairman Dennis Kucinich (D-OH) and Ranking Minority Member Darrell Issa (R-CA) of the U.S. House of Representatives' Committee On Oversight and Government Reform, which has broad oversight jurisdiction over many federal agencies including the S.E.C., wrote to Chairman Cox requesting a staff briefing regarding the Commission's application of the ordinary business exclusion in relation to shareholder proposals.

Noting that under Rule 14a-8(i)(7) company management is not free to exclude from a vote of the shareholders any proposal that deals with sufficiently significant policy issues, Congressmen Kucinich and Issa wrote: "The President and Congress have devoted considerable time and resources to evaluating and improving rail security. . . in the context of protecting homeland security and public safety." The letter explained:

> As you may know, the President asked for $175 million for the transit, passenger rail and freight rail security grant program in DHS in his FY2008 budget request. Congress appropriated an identical sum for the grant program in FY2007 as well. Furthermore, the House Homeland Security Committee has held five hearings and mark-ups on rail security matters in this congress alone, including: on 2/6/07, a Subcommittee hearing on "Update on Federal Rail and Public Transportation Security Efforts;" on 2/12/07, a Subcommittee hearing on "Rail and Mass Transit Security: Industry and Labor Perspectives"; on 2/28/07, a Subcommittee markup of HR 1401 ("Rail and Public Transportation Security Act of 2007"); on 3/5/07, a Full committee hearing on HR 1401 ("Rail

and Public Transportation Security Act of 2007"), and on 3/12/07 Full committee markup of HR 1401 ("Rail and Public Transportation Security Act of 2007").

We believe that the President and the members of the Homeland Security Committee are under the impression that their efforts in this regard concern a significant social policy issue.[4]

Staff Legal Bulletin 14A states that "the presence of widespread public debate regarding an issue is among the factors to be considered in determining whether proposals concerning that issue 'transcend the day-to-day business matters.'"[5] In July 2000, the Division of Corporation Finance stated in "Current Issues and Rulemaking Projects" that it had declined to allow exclusion of a shareholder proposal on "cash balance" pension plans submitted to IBM, despite the Staff's usual characterization of employee benefits-related issues as ordinary business, because "the staff was persuaded that the widespread public debate on the significant social and corporate policy issues raised by conversion from defined-benefit to cash-balance retirement plans caused the subject-matter of this particular proposal to fall outside the realm of 'ordinary business' matters subject to exclusion under Rule 14a-8(i)(7)."[6]

There is currently a widespread public debate about how to secure the U.S. rail network from terrorist attack:

- A CSX freight derailment in Washington, D.C. in November 2007 called public attention to the rail system's ongoing vulnerability and ignited further debate as to the efficacy of the Bush administration's rail security efforts. The Center for American Progress (CAP), a national political policy research and advocacy organization, said the derailment "is a grim reminder that we have yet to adequately address one of the nation's most serious homeland security vulnerabilities."[7]

---

[4] Letter to SEC Chairman Christopher Cox from Rep. Dennis Kucinich and Rep. Darrell E. Issa, on behalf of the House of Representatives' Committee on Oversight and Government Reform (June 5, 2007)

[5] Staff Legal Bulletin 14A (July 12, 2002).

[6] Division of Corporation Finance, "Current Issues and Rulemaking Projects," at 89-90 (July 25, 2000) (available at http://www.sec.gov/pdf/cfcr072k.pdf).

[7] "Derailed Train Exposes Weakness in Rail Security," Center for American Progress (Nov. 13, 2007) (available at: http://www.americanprogress.org/issues/2007/11/derailment.html)

According to NBC News4, Homeland Security officials "said the incident brings another problem to the surface—trains carrying hazardous materials traveling through the nation's capital." Congresswoman Eleanor Holmes-Norton told News4: "We can't keep depending on luck."[8]

- A widely discussed article early this year by Pittsburgh Tribune-Review investigative reporter Carl Prine described how Prine had been able to penetrate lackluster or absent security at 48 chemical plants and the freight rail lines that carry their products, leaving hundreds of business cards to mark his incursions.[9] The New York Times reported similar findings in an inspection by the Federal Railroad Administration, this one following a credible terrorist threat in 2005.[10]

- Federal lawmakers have focused significant attention on rail security throughout 2007. On August 3, 2007, President Bush signed into law the "Implementing Recommendations of the 9/11 Commission Act of 2007." This comprehensive piece of legislation includes significant Rail Security measures which had originally been introduced in such stand alone bills as H.R. 1269 and H.R. 1401, "The Rail and Public Transportation Security Act of 2007." Some of the measures in the law include: $1.2 billion in authorized funding over the next four years for general Railroad Security Enhancements; $650 million over the next four years for Amtrak Security Enhancements; requirement for the development of a "National Strategy for Railroad Transportation Security" within the next 9 months; requirement for Railroad Carrier Security Assessments and Plans; requirements for the development and implementation of a Railroad Security Training Program in consultation with Rail Labor; and employee whistleblower protections.[11]

  Prior to the President signing into law the "Implementing Recommendations of the 9/11 Commission Act of 2007", the House Homeland Security Committee held five hearings and mark-ups on rail security matters in this congress alone,

---

[8] "Clean Up, Questions Begin In Train Derailment," NBC News4 (Nov. 9, 2007) (available at: http://www.nbc4.com/news/14552564/detail.html)

[9] Carl Prine, "Terror on the Tracks," Pittsburgh Tribune-Review (Jan. 14, 2007); see also, e.g., Associated Press, "Probe: Trains Can be Easy Terror Targets" (Jan. 16, 2007).

[10] Walt Bogdanich & Christopher Drew, "Deadly Leak Underscores Concerns About Rail Safety," The New York Times (Jan. 9, 2005).

[11] "President Bush Signs 'Implementing Recommendations of the 9/11' into Law," White House Press Release (Aug. 3, 2007) (available at: http://www.whitehouse.gov/news/releases/2007/08/20070803-1.html); see also "President Signs Rail Security Legislation Into Law," Brotherhood of Locomotive Engineers and Trainmen Press Release (Aug. 3, 2007) (available at: http://www.bletdc.org/2007/08/president-signs-rail-security.php)

including: on 2/6/07, a Subcommittee hearing on "Update on Federal Rail and Public Transportation Security Efforts;" on 2/12/07, a Subcommittee hearing on "Rail and Mass Transit Security: Industry and Labor Perspectives"; on 2/28/07, a Subcommittee markup of HR 1401 ("Rail and Public Transportation Security Act of 2007"); on 3/5/07, a Full committee hearing on HR 1401 ("Rail and Public Transportation Security Act of 2007"), and on 3/12/07 Full committee markup of HR 1401 ("Rail and Public Transportation Security Act of 2007").[12]

House Homeland Security Chairman Bennie Thompson announced in January 2007 that rail security would be the focus of the committee's first piece of legislation in 2007, and in 2006, Thompson asked the Government Accountability Office to review the Transportation Security Administration's rail security initiatives.[13] In the Senate, the Surface Transportation and Rail Security Act of 2007 was passed by the Committee on Commerce, Science and Transportation in February.[14]

- The steps the private sector should be taking are also a matter of intense public discussion. Testimony from Jack Riley, the RAND Corporation's Director of Public Safety and Justice, in 2004 before the Senate Committee on Commerce, Science and Transportation highlighted the fact that "[t]o a considerable extent, the security of the nation's freight rail system is in the hands of the private sector," which must compete with other modes of transportation.[15] Stephen Flynn, a senior national security fellow at the Council on Foreign Relations, has criticized rail companies for failing to provide information on hazardous cargos to local first responders.[16]

- In particular, significant controversy surrounds the issue of whether rail companies should be required to reroute hazardous cargo around major cities that could be targets of terrorist attacks, with supporters of such rerouting

[12] Letter to SEC Chairman Christopher Cox from Rep. Dennis Kucinich and Rep. Darrell E. Issa, on behalf of the House of Representatives' Committee on Oversight and Government Reform (June 5, 2007)

[13] Chris Strohm, "House Member Puts Rail Security at Top of His Panel's Agenda," GovExec.com (Jan. 29, 2007).

[14] Press Release, "Senate Commerce Committee Approves Security Bills, Nominations" (Feb. 14, 2007) (available athttp://commerce.senate.gov/public/index.cfm?FuseAction=PressReleases.Detail&PressRelease_id=248742&Month=2&Year=2007).

[15] Statement of Jack Riley, Director of RAND Public Safety and Justice, Before the Committee on Commerce, Science and Transportation, United States Senate, at 9 (Mar. 23, 2004) (available at http://www.rand.org/pubs/testimonies/2005/RAND_CT224.pdf).

[16] Eben Kaplan, "Rail Security and the Terrorist Threat," Council on Foreign Relations Backgrounder at 3-4 (Mar. 12, 2007).

singling out Norfolk Southern and CSX for their refusals to reroute.[17] On March 12, 2007, Senator Joseph Biden proposed an amendment to the 9/11 Commission bill to require such rerouting.[18] Senator Biden had previously introduced the Hazardous Materials Vulnerability Reduction Act of 2005.[19]

- Local governments have also been taking steps to fill perceived gaps. Washington, DC passed a law in 2005, now under challenge by CSX, prohibiting hazardous cargo from coming within 2.2 miles of the US Capitol.[20] Similar proposals were introduced in Boston, Chicago and Baltimore.[21]

- The Center for American Progress (CAP), in a report issued in 2005, made the case for increased corporate disclosure of the type sought in the Proposal as a strategy for combating terrorism. CAP argued that in addition to informing shareholders about key business issues, fuller disclosure regarding security issues (excluding classified or other sensitive information) would improve corporate processes and emphasize the centrality of security concerns to companies' core businesses.[22]

As these examples demonstrate, rail security, including the measures being undertaken by the private sector, is a significant social policy issue. The connection between rail security and the threat of another major terrorist attack in the U.S. engages the attention of the media and the public at large. Legislators and regulators are actively engaged in trying to reduce the vulnerability of the U.S. system to terrorist attack and, in the course of doing so, are raising public awareness of the issue even further through hearings and press outreach.

C. BNSF's Examples of Recent and Longstanding SEC Decisions Are Not Applicable

---

[17] See Press Release by Friends of the Earth, "New Rail Security Rules Leave Communities At Risk" (Dec. 15, 2006) (available at http://www.foe.org/new/releases/december2006/railroadsecurityrisk121506.html); "Government Proposes Rail Security Plan," USA Today (Dec. 15, 2006).

[18] Press Release by Sen. Joseph Biden, "Biden Calls for Rerouting Hazardous Chemical Shipments Away From Population Centers" (Mar. 12, 2007) (available at http://biden.senate.gov/newsroom/details.cfm?id=270512&).

[19] See Floor Statement at http://biden.senate.gov/newsroom/details.cfm?id=239196&&.

[20] Kaplan, supra note 16, at 3; "Government Proposes Rail Security Plan," supra note 17.

[21] Julia Malone, "Growing Number of Major Cities Want Hazmats Off the Rails in Downtowns, Neighborhoods," Cox Newspapers Washington Bureau (Mar. 26, 2006) (available at http://www.coxwashington.com/reporters/content/reporters/stories/2006/03/26/BC_HAZMATS_RAILCARS25_COX.html).

[22] Robert Housman & Timothy Olson (Center for American Progress), "New Strategies to Protect America: A Market-Based Approach to Private Sector Security," at 8-9 (Aug. 10, 2005) (available at http://www.americanprogress.org/issues/2005/08/after_london_madrid.html).

to Our Proposal

In Section I.B of the No-Action Request, BNSF cites certain recent and longstanding SEC decisions in an attempt to demonstrate that our Proposal should be likewise excluded. As we will explain below, we believe these decisions relate to proposals unlike our Proposal and are therefore not applicable. We further consider BNSF's use of these examples to evidence the Company's failure to recognize that the ordinary business exclusion is not applicable to proposals that focus on matters of significant social policy issues.

BNSF argues that the Staff has recently addressed the Fund's "nearly identical proposals" for information related to the counter terrorism efforts of three other railroad companies: *Kansas City Southern* (Feb. 21, 2007), *Norfolk Southern Corporation* (Feb. 20, 2007), and *Union Pacific Corporation* (Feb. 21, 2007). BNSF says that in each instance the Staff concluded that Rule 14a-8(i)(7) provided some basis for exclusion of our proposals, and "Accordingly, the substantive merits of the Proponent's proposal in this instance should be treated in the same manner as it was in the prior matters."

However, these no-action determinations referenced by BNSF do not apply to our Proposal because the proposals filed at Kansas City Southern, Norfolk Southern Corporation, and Union Pacific Corporation are significantly different from our Proposal. BNSF argues that "The only substantive difference between the Proponent's proposals to these companies and the Proposal to BNSF is that the phrase 'and minimize material financial risk' is included in those proposals but not in our Proposal."

While BNSF characterizes the phrase "and minimize material financial risk" as a minor change bearing no substantive effect on the proposal's intent, we believe the deletion of this phrase is a critical change. Our Proposal is explicitly focused on a significant social policy issue—rail security—and BNSF's efforts to minimize the threats to the environment and the public's health posed by the Company's vulnerability to a terrorist attack on its rail system.

BNSF also argues that proposals relating to the safety of a company's operations have historically been deemed matters of day-to-day operations by the Commission, citing as examples *CNF Transportation Inc.* (Jan. 26, 1998), *Burlington Northern Santa Fe Corp.* (Jan. 14, 2004), *AMR Corporation* (Apr. 2, 1987), and *Union Pacific Corporation* (Dec. 16, 1996). The Company further argues that the

Commission has found that the ordinary business exception applies to proposals requesting companies to provide reports which assess the risk of external events on those companies, citing as examples *Pfizer Inc.* (Jan. 24, 2006), *The Chubb Corp.* (Jan. 25, 2004), and *The Ryland Group, Inc.* (Feb. 13, 2006).

These examples are not applicable to our Proposal, which does not: request that management annually disclose its safety policies and safety data; report on the development and implementation of new safety technologies; report on the nature and extent of review of operational safety; report on safety systems; or report on the economic effects or potential business impact of an external risk. While our Proposal may relate to matters of specific safety policies, safety systems, and external risks, unlike any of the proposals cited above, our Proposal focuses on a sufficiently significant social policy issue that transcends ordinary business matters.

D. Our Proposal is a Broad Question of Policy and is Precluded from the Application of the Ordinary Business Exclusion

In Section I.C. of the No-Action Request, BNSF argues that our Proposal requests information that is not a broad question of policy but instead a matter of ordinary business operations. The Company refers to Staff Legal Bulletin No. 14C (June 28, 2005), which distinguishes proposals that deal generally with the risk or liability of operations to the company from those that focus on minimizing or eliminating particular operations that may adversely affect the environment or the health of the general public:

> To the extent that a proposal and supporting statement focus on the company engaging in an internal assessment of the risks or liabilities that the company faces as a result of its operations that may adversely affect the environment or the public's health, we concur with the Company's view that there is a basis for it to exclude the proposal under rule 14a-8(i)(7) as relating to an evaluation of risk. To the extent that a proposal and supporting statement focus on the company minimizing or eliminating operations that may adversely affect the environment or the public's health, we do not concur with the Company's view that there is a basis for it to exclude the proposal under rule 14a-8(i)(7).[23]

BNSF argues that, "Like similar proposals which the Commission has

[23] Staff Legal Bulletin 14C (June 28, 2005).

determined to be excludable under Rule 14a-8(i)(7), the Proposal and Supporting Statement in this instance focus on potential risks and liabilities to BNSF, not on minimizing operations that affect the environment or public health."

We believe that any efforts that BNSF makes, or fails to make, to safeguard the security of its operations from a terrorist attack and/or other homeland security incident will directly affect the environment and the public's health. We therefore believe the Proposal is inherently about the Company's efforts to minimize or eliminate threats to the environment and the public's safety resulting from the Company's vulnerability to a terrorist attack on its rail system. Furthermore, our supporting statement explicitly states that the Fund seeks disclosures that would allow shareholders "to evaluate the steps the Company has taken to minimize risks to the public arising from a terrorist attack or other homeland security incident."

In this vein, our Supporting Statement details the potential for a public health and environmental catastrophe in the event that BNSF's operations suffer a terrorist attack or other homeland security incident. It explains that, according to the United States Naval Research Lab, "a one 90-ton tank car carrying chlorine, if targeted by an explosive device, could create a toxic cloud 40 miles long and 10 miles wide, which could kill 100,000 people in 30 minutes."

While the Proposal does indeed reference the harm that an outside terrorist event could cause to the railroad and thereby references the risks and liabilities that the Company faces as a result of terrorist threats, the focus remains on the Company's efforts to minimize or eliminate threats to the environment and the public's safety resulting from the Company's vulnerability to a terrorist attack. Just because the Proposal includes language regarding risks to the Company does not make the Proposal necessarily excludable. As Staff Legal Bulletin 14C explicitly states: "The fact that a proposal relates to ordinary business matters"—in this case, ordinary business being the risks and liabilities that BNSF faces—"does not conclusively establish that a company may exclude the proposal from its proxy materials."[24]

A shareholder proposal, by its very nature, must be company-specific. It must ask the company to take a specific action, or risk being excluded as not within the Commission's definition of a proposal. Proposals that address a broader public policy debate without providing a nexus to the specific company to which the proposal is submitted risk exclusion on the ground that the proposal is beyond the Company's

[24] Staff Legal Bulletin 14C (June 28, 2005).

power to implement.

Furthermore, the fact that significant social policy issues can have financial ramifications for companies cannot, under any sensible construction of the ordinary business exclusion, be the basis for allowing omission. Such an interpretation would undermine the functioning of the shareholder proposal rule as a vehicle for raising important matters affecting investment value.

II. Our Proposal is Not Materially Misleading in Violation of Rule 14a-9, as Charged by BNSF

BNSF alleges that our Proposal is materially misleading in violation of Rule 14a-9 in three respects. We contend that our Proposal is not misleading as alleged for the reasons set forth below.

A. Reference to Penn State University Report

In Section II.C. of the No-Action Request, BNSF claims that our supporting statement "gives the impression that BNSF is partly responsible as one of the 'glaring holes in rail security'" discussed in a Penn State University report on June 12, 2007 to which we refer.

We believe that this is a misreading of our supporting statement and fails to acknowledge that our supporting statement discusses the general importance of rail security to public safety in an effort to underscore the need for further disclosure and accountability in this area—not to demonize BNSF. We believe a fair reading would infer that our reference to the Penn State University Report: establishes the importance of rail security in the public arena; points to the vulnerability of the nation's rail system to terrorist attacks; and underscores the need for further disclosure from the Company on its efforts to safeguard the security of its operations (and thereby, to safeguard the public's health and the environment) from a terrorist attack or other homeland security incident.

Further, BNSF argues that its programs are cited in the Penn State University report as examples of the types of safety programs recommended for the rail industry. We believe that this line of argument belongs in the Company's statement in opposition in the proxy and does not serve as a basis for exclusion of the proposal.

B. References to BNSF's Rail Workers

In the Fund's supporting statement, it reports that "[r]ail workers throughout our Company report that BNSF has failed to implement significant security improvements to deter or respond to a terrorist attack on the U.S. rail network, which could potentially devastate communities in our country and destroy our Company."

In Section II.B. of the No-Action Request, BNSF argues that this statement "contains vague and unquantifiable terminology, such as 'significant security improvements' and 'potentially devastate'", further claiming that "[w]ithout proper authority for its contention or more specific measures of the proposed risk, the statement is not verifiable and thus merely a thinly veiled attempt to paint BNSF employees as a whole as disgruntled and concerned for their safety."

Preceding the reference to BNSF's rail workers, our supporting statement notes that BNSF is involved with the transportation, storage and handling of hazardous materials including chemicals, explosives, radioactive materials, gases, poisons and corrosives. The statement further notes that the United States Naval Research Lab reported that a one 90-ton tank car carrying chlorine, if targeted by an explosive device, could create a toxic cloud 40 miles long and 10 miles wide, which could kill 100,000 people in 30 minutes.

As explained in the Fund's supporting statement, the Penn State University report reveals a need for an increase in terrorism preparedness training for rail workers. A survey of rail workers, including frontline BNSF engineers and maintenance of way employees, revealed that despite warnings by the FBI that the rail network is a likely target of al Qaeda, rail carriers have done little in the face of clear and present danger. The results of the survey were published in a report entitled "High Alert: Workers Warn of Security Gaps on Nation's Railroads," by the International Brotherhood of Teamsters in 2005.[25]

Our reference to the potential for devastation to communities and our Company is based on the fact that BNSF transports, stores and handles hazardous materials; the rail car explosion scenario depicted by the United States Naval Research Lab's report includes the death of 100,000 people; and the worker survey raises questions

[25] "High Alert: Workers Warn of Security Gaps on Nation's Railroads," International Brotherhood of Teamsters (September 2005) (available at: http://www.teamster.org/divisions/rail/pdfs/railsecuritybook.pdf)

regarding BNSF's efforts to safeguard its operations. We believe a fair reading would infer that the Fund used the reference to BNSF's workers to highlight the need for further disclosure and accountability in this area—not to "paint BNSF employees as a whole as disgruntled and concerned for their safety."

BNSF further argues that the statement regarding BNSF rail workers "is highly suspect because it implies that rail workers are privy to sufficient information to enable them to evaluate BNSF's counter-terrorism efforts. However, many of BNSF's efforts and successes are the result of high level programs and strategies known only by management." The Company further argues that many of its counter-terrorism measures "cannot be disclosed outside of management due to government mandate or agreements with other carriers regarding certain jointly-developed and implemented strategies."

While BNSF makes a compelling argument as to why these workers may not be privy to certain high level programs and strategies known by management, we believe this argument belongs in the Company's statement in opposition in the proxy statement and does not constitute a basis for exclusion of the Proposal.

C. References to Other Rail Companies

In Section II.C. of the No-Action Request, BNSF argues that "The Proponent's statement gives the misleading impression that BNSF lags behind its peers in disclosing its counter terrorism measures." It further argues that "BNSF's disclosures are actually consistent with the U.S. industry standard."

In calling attention to the fact that "other rail companies, such as Canadian Pacific Railway, have disclosed extensive detail of both security actions taken to protect their infrastructure and personnel and their cost", the Fund is underscoring the fact that certain companies, such as Canadian Pacific Railway, are taking the lead in best practices in this area by providing investors with important information on this social policy issue.

Drawing comparisons to the practices of other companies in BNSF's industry is not a basis for excluding the Proposal. If BNSF seeks to measure itself only against particular U.S. peers and justify its practices based on this measure, we believe that argument belongs in the Company's statement in opposition in the proxy statement and does not serve as a basis for exclusion of the Proposal.

III. Conclusion

For the foregoing reasons, the Fund respectfully requests that the Division take action to enforce inclusion of its proposal in BNSF's 2008 Proxy Materials.

The Fund is pleased to be of assistance to the Staff on this matter. If you have any questions or need additional information, please do not hesitate to contact Jamie Carroll, IBT Program Manager, at (202) 624-8990.

Sincerely,

C. Thomas Keegel
General Secretary-Treasurer

CTK/jc

cc: Jeffrey T. Williams

EXHIBIT D

Jeffrey T. Williams
Senior General Attorney

Burlington Northern
Santa Fe Corporation
P. O. Box 961039
Fort Worth, Texas 76161-0039
2500 Lou Menk Drive
Fort Worth, Texas 76131-2828
tel 817 352-3466
fax 817 352-2397
Jeffrey.williams@bnsf.com

December 19, 2007

BY UPS OVERNIGHT MAIL

Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F Street, N.E.
Washington, D.C. 20549

Re: Burlington Northern Santa Fe Corporation - Shareholder Proposal Submitted by the International Brotherhood of Teamsters' General Fund

Ladies and Gentlemen:

This letter is submitted by Burlington Northern Santa Fe Corporation ("BNSF") in response to the letter dated December 7, 2007 (the "Proponent's Response") addressing our no-action request letter dated November 19, 2007 (the "No-Action Request") to the Securities and Exchange Commission with respect to a proposal (the "Proposal") submitted for inclusion in BNSF's 2008 proxy statement by the International Brotherhood of Teamsters General Fund (the "Proponent"). The Proponent's Response is attached as Exhibit A, the No-Action Request is attached as Exhibit B, and the Proponent's Proposal is attached as Exhibit C.

We reiterate to the Commission that BNSF intends to omit the Proposal from its 2008 proxy statement and other proxy materials (the "2008 Proxy Materials") pursuant to Rule 14a-8(j) under the Securities Exchange Act of 1934, as amended (the "Exchange Act"). We respectfully repeat the request, set forth in the No-Action Request, that the staff of the Division of Corporate Finance (the "Staff") confirm that it will not recommend any enforcement action to the SEC if, in reliance on certain provisions of Commission Rule 14a-8 under the Exchange Act as explained in the No-Action Request or further discussed below, BNSF excludes the Proposal from its 2008 Proxy Materials.

In accordance with Rule 14a-8(j), the Company is filing six copies of this letter and the Exhibits. It is simultaneously forwarding a copy of this letter via overnight courier, with copies of all enclosures, to the Proponent as additional notice of the Company's intention to exclude the Proposal from the Company's 2008 Proxy Materials.

The Proposal states:

> Resolved: That the shareholders of Burlington Northern Santa Fe Corporation ("BNSF" or "Company") hereby request that the Board of Directors make available, omitting proprietary information and at reasonable cost, in BNSF's annual proxy statement, by the 2009 annual meeting, information relevant to the Company's efforts to safeguard the security of their operations arising from a terrorist attack and/or other homeland security incidents.

BASES FOR EXCLUSION

In the No-Action Request, we argued that the Proposal and its supporting statement may be omitted from our 2008 Proxy Materials because they relate to a matter of ordinary business operations and because the supporting statement violates the proxy rules as materially misleading. We will address the reasons provided in the Proponent's Response that the Proponent claims creates a basis for denial of our request, and avoid significant repetition of the contents of the No-Action Request. Therefore, this response letter should be read in conjunction with the No-Action Request.

I. The Proposal May Be Excluded Under Rule 14a-8(i)(7) Because it Pertains to Matters of Ordinary Business Operations, and is Not a Significant Policy Issue

A. Recent SEC Guidelines Clearly Indicate That the Proposal Does Not Focus on a Broad Issue of Social Policy, But Rather on an Ordinary Business Matter

The central tact taken by the Proponent's Response is to refute our claim that the Proposal may be excluded under Rule 14a-8(i)(7) as an ordinary business matter. The Proponent attempts to make this claim by characterizing the Proposal as one that focuses on a "significant social policy issue." In doing so, the Proponent relies chiefly on language taken from Exchange Act Release No. 40018 (the "1998 Release"), Exchange Act Release No. 12999 (the "1976 release"), and Staff Legal Bulletin 14A. Not only does the Proponent's analysis misinterpret these authorities, but more importantly, it fails to give sufficient weight to more recent SEC pronouncements on the matter, specifically, Staff Legal Bulletin 14C (June 28, 2005). As discussed in Section I.C of our No-Action Request, the standard established by this Bulletin makes clear that the Proposal does not focus on a significant social policy issue. Rather it focuses on an ordinary business matter, and, as noted by our No-Action Request, while it may touch on an ancillary policy issue, the SEC has held that such tangential treatment of social policy will not preclude its exercise of the ordinary business exception. *See, e.g. General Electric Co* (Feb. 3, 2005); *Newmont Mining Corp* (Feb. 4, 2004).

The Proponent's Response introduces its argument by referencing language from the 1998 Release and the 1976 Release. The 1976 Release dictates that "certain matters, which have significant policy, economic or other implications inherent in them" to be excluded from Rule 14a-8(i)(7)'s ordinary business matter exception. However, this Release was published more than three decades ago, and is by no means the SEC's final pronouncement on the matter. Indeed, before even delving into the substantive matters raised by the 1976 Release, the SEC

prefaced its discussion by writing that, "[t]he Commission wishes to emphasize that the amendments which it has adopted *are not intended as a final resolution* of the questions and issues relating to shareholder participation in corporate governance and, more generally, shareholder democracy." *SEC Adopting Release No. 12999*, (Nov 22, 1976) (emphasis added). Moreover, the 1976 Release gave no clear guidance with regards to distinguishing between matters that qualify as significant social policy issues versus those that are ordinary business matters. Likewise, the 1998 Release cited by the Proponent does not draw a clear line between ordinary business matters and significant social policy matters. Rather, it simply reiterates that proposals focusing on social policy issues do not qualify as ordinary business matters. *See SEC Adopting Release No. 40018* (May 21, 1998). While Staff Legal Bulletin 14A (released in 2002) does mention that the presence of widespread public debate is one of many factors that help determine whether a proposal focuses on a significant social policy issue, it was not until 2005 that the SEC drew a clear demarcation between ordinary business matters and social policy issues, with its discussion of the matter in Staff Legal Bulletin 14C. As discussed in Section I.C of our No-Action Request, Staff Legal Bulletin 14C depicts the distinction as follows:

> To the extent that a proposal and supporting statement focus on the company engaging in an internal assessment of the risks or liabilities that the company faces as a result of its operations that may adversely affect the environment or the public's health, we concur with the company's view that there is a basis for it to exclude the proposal under rule 14a-8(i)(7) as relating to an evaluation of risk. To the extent that a proposal and supporting statement focus on the company minimizing or eliminating operations that may adversely affect the environment or the public's health, we do not concur with the company's view that there is a basis for it to exclude the proposal under rule 14a-8(i)(7).

Even though this language is the SEC's most recent pronouncement on the matter, the Proponent's Response fails to give Staff Legal Bulletin 14C appropriate weight. Moreover, as explained in Section I.C of our No-Action Request, the standard set forth by the above language makes clear that the Proposal qualifies as an ordinary business matter, because the Proposal and its supporting statement focus on a potential outside risk (terrorism) to BNSF's operations, not on minimizing a particular operation that could adversely affect the environment or public health. While the Proponent's Response attempts to qualify the Proposal as a social policy matter based on the strictures set forth above, its analysis reveals a confused understanding of the SEC's standard. Specifically, the Proponent claims that the Proposal may not be excluded because it focuses on minimizing the impact of terrorist threats. However, terrorist threats do not qualify as BNSF "operations" that BNSF is capable of "minimizing or eliminating [and] that may adversely affect the environment or the public's health," in the words quoted from Staff Legal Bulletin 14C above. Instead, terrorist threats are exogenous risks that BNSF faces as a result of operating a railroad. Indeed, as a common carrier BNSF is obligated by law to carry certain materials, including chemicals and other hazardous materials. It's not a question of whether BNSF should have a policy to protect against the risks of terrorist attacks, but rather now BNSF carries that task out. Management, not shareholders, are equipped to handle that responsibility. Because the Proposal requests that BNSF provide a report on its internal assessment of that outside risk, it falls squarely within the confines of the ordinary business exception set forth above by the SEC's most recent evaluation of the matter.

Furthermore, the Proponent's reliance on the 1976 Release and the 1998 Release expose a flawed understanding of theses SEC pronouncements. While these releases did not create as clear a standard as Staff Legal Bulletin 14C, they both provided a few concrete examples of matters that the SEC viewed as social policy issues, and a company's evaluation of its counter-terrorism efforts does not accord with these examples. Specifically, the 1998 Release cited employment discrimination and other labor-related matters as social policy issues, whereas the 1976 Release referenced a company's decision to build a potentially harmful nuclear power plant. These examples are all risks that companies create for themselves as a result of their operations; they are not outside risks to which companies must react (like terrorism threats). This distinction between internal risks and external risks was eventually elucidated in Staff Legal Bulletin 14C, as discussed above. However, even if one relied solely on the examples of social policy issues used in the 1976 Release and the 1998 Release, a company's analysis of the impact of outside terrorist threats would not fit with those examples, because terrorism is not a risk that the company itself creates. Indeed, as discussed in Section I.B of our No-Action Request, the Commission has generally found that the ordinary business exception applies to proposals requesting companies to provide reports which assess the risk of external events on those companies. *See, e.g., Pfizer Inc.* (Jan. 24, 2006); *The Chubb Corp.* (Jan. 25, 2004); *The Ryland Group, Inc.* (Feb. 13, 2006).

B. The Proponent's Discussion of a Widespread Public Debate is Misguided and Inaccurate

Additionally, the Proponent's claim that the Proposal focuses on a social policy issue because its topic has created "widespread public debate" is both a misapplication of the relevant rule and a mischaracterization of the facts.

As noted above, Staff Legal Bulletin 14A clearly states that the "presence of widespread public debate regarding an issue is *among the factors to be considered* in determining whether proposals concerning that issue" qualify as social policy matters. *Staff Legal Bulletin 14A*, (July 12, 2002) (emphasis added). A natural reading of this language demonstrates that widespread public debate is only one of multiple considerations in determining whether the ordinary business exception applies to a given proposal. However, the Proponent treats this consideration as the dispositive factor in determining the issue, claiming that the Proposal relates to a matter of social policy simply by virtue of the public debate that terrorism has caused. The Proponent does not set forth other reasons for deeming this matter a significant social policy issue. Absent some additional demonstration as to how this matter qualifies as a social policy issue, the Proponent's proof is insufficient.

Moreover, the actual references that the Proponent cites do not even illustrate a widespread public debate on the issue of terrorist threats on rail systems. When the Proponent's citations are taken at face value, they fail to demonstrate that railway terrorism is a significant public concern. For example, the Proponent refers to a CSX freight derailment in Washington D.C. which "called public attention to the rail system's ongoing vulnerability," but the Proponent's Response fails to mention that the derailment was not caused by any sort of terrorist activity. Also, the Proponent cites to a newspaper article from the Pittsburgh Tribune-Review, and claims that this article was widely discussed, but it makes no attempt to demonstrate just

how widespread that discussion was. Likewise, the Proponent states that counter-terrorism efforts in the private sector are matters of "intense public discussion," but it does not demonstrate any such public discussion; instead, the Proponent only references a few statements made by Jack Riley, the RAND Corporation's Director of Public Safety and Justice, and Stephen Flynn, a senior national security fellow at the Council on Foreign Relations. Given Riley's and Flynn's respective job titles, it is a mischaracterization to attribute their statements to the general public, as these men made statements on railway safety incident to their occupations. Additionally, much of the governmental action that the Proponent references (like Senator Biden's proposals and the letter written by Congressmen Kucinich and Issa) is simply the work of a few individual congressmen and senators. Finally, the Proponent fails to mention that no terrorist attack has taken place on U.S. railroads since September 11, 2001, a fact that is of particular importance when determining just how sensitive the public might be to railway safety issues. All told, the Proponent was only able to reference four news stories on the topic of railway safety and some isolated government action. Given that these activities occurred over a four-year period, it is a stretch to characterize such a minor amount of activity as "widespread public debate."

Taken to its logical conclusion, the Proponent's argument essentially creates a system where any issue that receives even a minor amount of media or governmental attention would qualify as a social policy issue. In a world of expanding media outlets, such a position would open the floodgates, allowing all sorts of ordinary business matters to find their way onto companies' proxy statements. Given the SEC's longstanding desire to "to confine the resolution of ordinary business problems to management and the board of directors, since it is impracticable for shareholders to decide how to solve such problems at an annual shareholders meeting" (*SEC Release No. 40018*), it is imperative to exclude the Proposal in this case.

C. The Proponent's Treatment of SEC Precedents is Flawed

In Section I.C of the Proponent's Response, the Proponent argues that its Proposal differs from other proposals that the SEC has recently excluded from companies' proxy statements on the basis of the ordinary business matter exception. This claim is inaccurate.

The most salient SEC precedents in this instance are three no-action letters that were granted to other railroads last year. *See Kansas City Southern* (Feb. 21, 2007); *Norfolk Southern Corporation* (Feb. 20, 2007); *Union Pacific Corporation* (Feb. 21, 2007). We cited these precedents in Section I.B of our No-Action Request, as the proposals at issue in those cases were virtually identical to the Proposal at issue here. As noted in our No-Action Request, the only substantive difference between these precedents and the Proponent's Proposal is that the phrase "and minimize material financial risk" was included in the precedents, but not in our Proposal. The Proponent argues that this variation alone should yield a different result in this case, claiming that the deletion of the reference to financial risk shifts the focus of the letter away from BNSF's assessment of risk. This claim, however, is incorrect, as the Proposal still requires BNSF to engage in an assessment of risk, regardless of whether that assessment includes an evaluation of financial risk. As noted at length in Section I.B of our No-Action Request, the Proposal calls for BNSF to report on efforts to safeguard the security of our operations from a terrorist attack, and such a report would invariably require us to engage in a substantial evaluation of our safety systems and procedures as they relate to the risk of terrorism. It does not

matter whether or not such an evaluation includes an assessment of *financial* risk; the fact that it requires an assessment of *any* business risk makes it an ordinary business operation and therefore excludable under Rule 14a-8(i)(7). Indeed, as noted in our No-Action Request, the SEC has a long-standing history of granting no-action relief in instances where companies are asked to conduct analyses of policy risks and benefits, as such analysis is a fundamental and ongoing part of a company's ordinary business operations. *See, e.g., Dow Chemical* (Feb. 23, 2005); *Xcel Energy Inc.* (Apr. 1, 2003). The fact that the Proponent deleted the words "and minimize material financial risk" from the similar proposals for which no-action relief was granted last year to three other major railroads does not change the analysis. With or without those words, BNSF necessarily must consider material financial risk to the Company as it plans and analyzes all risks attendant to operating a railroad in this day and age, including the risks of transporting chemicals and other hazardous materials, and how to mitigate against those risks. These activities are all ordinary business matters.

Additionally, Section I.B of our No-Action Request cited to numerous longstanding SEC precedents that deemed proposals relating to the safety of a company's operations as pertaining to ordinary business matters. *See CNF Transportation Inc.* (Jan. 26, 1998); *Burlington Northern Santa Fe Corp.* (Jan. 14, 2004); *AMR Corporation* (Apr. 2, 1987); *Union Pacific Corporation* (Dec. 16, 1996). The Proponent claims that these precedents are not applicable because the Proposal in this case does not "request that management annually disclose its safety policies and safety data; report on the development and implementation of new safety technologies; report on the nature and extent of review of operational safety; report on safety systems; or report on the economic effects or potential business impact of an external risk." This assertion is simply not true, because the Proposal, as written, would require us to undertake all of those activities. Specifically, the Proposal makes a very broad request: that BNSF include in its annual proxy statement all "information relevant to the Company's effort to safeguard the security of their operations arising from a terrorist attack and/or other homeland security incidents." There is a myriad of information that is relevant to our counter-terrorism efforts; because the Proposal's information request is so broad, it necessarily includes all of the information that the Proponent claims is not applicable to the Proposal. Stated more explicitly, management's safety policies and data, the development and implementation of new safety technologies, a review of operation safety and safety systems, and the potential impact of an external terrorist risk are exactly the types of information that are "relevant" BNSF's counter-terrorism efforts. Moreover, because the Proposal asks that this information be included "in BNSF's annual proxy statement," it seeks annual disclosure. Accordingly, the precedents cited in our No-Action Request are directly on point, and the Proposal should be excluded accordingly.

D. The Proponent Failed to Contradict BNSF's Argument That the Proposal Meets the SEC's Criteria for Qualifying as an Ordinary Business Operation

In addition to the arguments set forth above, we note that the Proponent has introduced nothing to oppose the arguments raised in Section I.A of our No-Action Request, specifically that the Proposal meets the SEC's criteria for qualifying as an ordinary business matter. The SEC has continually held that a Proposal is an ordinary business matter if (i) the proposal relates to tasks that are "so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight," and (ii) "the

proposal seeks to 'micro-manage' the company." *SEC Release No. 40018.* Our No-Action Request set forth our reasons for why the Proposal meets this standard, and the Proponent's Response has not countered those reasons. Accordingly, we reiterate our request that the SEC find that the Proposal qualifies as an ordinary business matter that may be excluded under Rule 14a-8(i)(7).

II. The Proposal May be Excluded as Materially Misleading Under Rule 14a-9

Section II of our No-Action Request cited three aspects of the Proposal and its supporting statement as being materially misleading in violation of Rule 14a-9. The Proponent's Response claims that the Proposal is not misleading in these respects. We disagree with this assertion for the reasons set forth below:

A. Reference to the Penn State University Report

The Proponent claims that references to the Penn State University report in the Proposal's supporting statement are not meant to demonize BNSF. Instead, it claims that the references to the report simply demonstrate the importance of rail security and the need for companies to continually improve their safety systems. The Penn State University report may well convey these messages when read alone. However, when references to this report are made in the context of the rest of the Proposal's supporting statement, it creates the misleading impression that BNSF is one of the railways criticized by the Penn State University report, a notion that is completely false given the report's praise for BNSF's safety efforts. Specifically, the Proposal and supporting statement, when read as a whole, describe how railway companies often lack proper security, and they decry BNSF for not disclosing more information about its security efforts. Given that context, when the supporting statement references the Penn State University report without mentioning the report's commendation of BNSF's efforts, it creates the impression that BNSF was, like many other railroads, criticized by the report. This false impression could mislead shareholders into voting for the Proposal, because they would want BNSF to be forced to disclose information regarding its safety efforts, in order to accelerate greater safety implementations.

Furthermore, as noted above and in our No-Action Request, the Penn State University report actually states that BNSF has implemented the types of safety programs recommended for the rail industry. The Proponent claims that we should not have placed these facts in our No-Action Request, as they do not serve as a basis for exclusion of the proposal. This assertion reveals a misunderstanding of Rule 14a-9. Specifically, the Proposal's omission of this material fact makes the Proposal itself misleading, because it gives the impression that BNSF has not stayed abreast of relevant changes in safety technology and systems. This false impression could certainly mislead shareholders voting on the Proposal, as described in the paragraph above. Accordingly, we maintain our position that referencing the Penn State University report without discussing its praise for BNSF is materially misleading in violation of Rule 14a-9.

B. Reference to BNSF's Rail Workers

The Proposal's supporting statement also contains references to statements made by BNSF rail workers. Section II.B of our No-Action Request argues that these references are misleading, because they are surrounded by vague and unquantifiable terminology and also because our rail workers are not in a position to evaluate our counter-terrorism efforts. The Proponent's Response makes no attempt to clarify the vague language, nor does it counter our contention that such language is unclear. Moreover, the Proponent's Response attempts to explain the rail workers' statements themselves by referencing a survey titled "High Alert: Workers Warn of Security Gaps on Nation's Railroads." The fact that the Proponent can only make the workers' statements less misleading by contextualizing them with a reference to this survey means that the Proposal *itself* is still misleading since it does not also reference this survey. Also, this survey polled rail workers from many different companies, not just BNSF. Therefore, attributing all of the statements therein to BNSF employees is materially misleading in violation of Rule 14a-9.

Additionally, the Proponent argues that our assertion regarding the workers' ignorance of safety strategies and systems does not constitute a basis for exclusion and should rather be used in our statement of opposition in the proxy statement. However, we maintain our position that omitting this material fact from the Proposal's supporting statement is materially misleading, because it may give shareholders the impression that the rail workers' statements were made with the benefit of full information with regard to our counter-terrorism tactics. Therefore referencing statements made by BNSF employees without explaining the questionable reliability of those statements is materially misleading and therefore excludable under Rule 14a-9.

C. References to Other Rail Companies

The Proponent argues that its reference to other rail companies is solely meant to "underscor[e] the fact that certain companies . . . are taking the lead in best practices" with respect to information disclosure. However, this claim is disingenuous, because in the Proposal's supporting statement, the reference to such other companies is juxtaposed to a claim that "BNSF makes only passing mention" to railway safety in its reports. The positioning of these clauses is clearly meant to give voters the impression that BNSF lags behind its peers with regard to safety disclosures, a notion that is simply untrue (as detailed in our No-Action Request). Moreover, the Proponent's assertion that other rail companies such as Canadian Pacific Railway "have disclosed *extensive* detail of both security actions taken to protect their infrastructure and personnel and their cost" (emphasis added) is also misleading, as it is simply untrue. In fact, Canadian Pacific's 2006 Annual Report provided very limited disclosure on its overall security efforts and even less information regarding its counter-terrorism efforts. The most significant statement that this report made with regards to terrorism is that it is "a certified carrier with the U.S. Customs and Border Protection's (CBP) Customs — Trade Partnership Against Terrorism program and the CBSA's Partners in Protection program. C-TPAT and PIP are partnership programs that seek to strengthen overall supply chain and border security." *See* Canadian Pacific Railway Company, 2006 Annual Report. This information hardly qualifies as an "extensive" disclosure. Also, despite the Proponent's assertion to the contrary, Canadian Pacific did not mention anything with regards to the "cost" of its security actions.

Finally, while the Proponent argues that our comparability to other railways is not, on its own, a basis for exclusion, we maintain our position that omission of this fact from the Proposal's supporting statement creates the misleading impression that BNSF's safety disclosures do not meet the industry standard. Such a false suggestion may well manipulate shareholders into voting for the Proposal, in an attempt to increase BNSF's disclosures. The proposal is therefore materially misleading and excludable under Rule 14a-9.

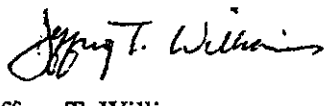
III. Conclusion

For the reasons set forth above and in the No-Action Request, BNSF continues to believe that the Proposal may properly be omitted from our 2008 Proxy Materials, and we request the Staff's concurrence with its views. To the extent that the reasons set forth in this letter are based on matters of law, pursuant to Rule 14a-8(j)(2)(iii) this letter also constitutes an opinion of counsel of the undersigned as an attorney licensed and admitted to practice in the States of Illinois and Texas.

If the Staff has any questions with respect to the foregoing, or if for any reason the Staff does not agree that we may omit the Proposal from our 2008 Proxy Materials, please contact me at (817) 352-3466. I may also be reached by facsimile at (817) 352-2397 and would appreciate it if you would send your response to us by facsimile to that number. The Proponents' legal representative, C. Thomas Keegel, may be reached by telephone at (202) 624-6800 and at the International Brotherhood of Teamsters, 25 Louisiana Avenue, NW, Washington, DC 20001. We request that the Staff notify the undersigned if it receives any correspondence on the Proposal from the Proponent or other persons, unless that correspondence has specifically confirmed to the Staff that BNSF or its undersigned counsel have timely been provided with a copy of the correspondence. In addition, BNSF agrees to promptly forward to the Proponent any response from the Staff to this letter that the Staff transmits by facsimile to BNSF only.

Please acknowledge receipt of this letter and the enclosures by date-stamping the enclosed copy of this letter and returning it in the enclosed stamped, self-addressed envelope.

Very truly yours,



Jeffrey T. Williams
Senior General Attorney

cc: C. Thomas Keegel
Roger Nober

Enclosures

Department of Homeland Security
Management Directive System
MD Number: 11056
Issue Date: 12/16/2005

SENSITIVE SECURITY INFORMATION (SSI)

I. Purpose

This Management Directive (MD) establishes Department of Homeland Security (DHS) policy regarding the recognition, identification, and safeguarding of Sensitive Security Information (SSI).

II. Scope

This MD is applicable to all persons who are permanently or temporarily assigned, attached, detailed to, employed, or under contract with DHS.

III. Authorities

A. Homeland Security Act of 2002, Public Law 107-296, 116 Stat. 2135 (2002), as amended

B. Aviation and Transportation Security Act, Public Law 107-71, 115 Stat. 597 (2001)

C. Maritime Transportation Security Act of 2002, Public Law 107-295, 116 Stat. 2064 (2002), as amended

D. 49 U.S.C. § 114(s), Nondisclosure of Security Activities

E. 49 CFR § 1520, Protection of Sensitive Security Information, May 18, 2004

F. DHS Management Directive 0460.1, Freedom of Information Act Compliance

G. DHS Management Directive 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, January 6, 2005.

IV. Definitions

A. ***Access***: The ability or opportunity to gain knowledge of information.

B. ***Classified National Security Information ("Classified Information")***: Information that has been determined, pursuant to Executive Order 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

C. ***Component***: As used in this MD, directorates, agencies, and offices that comprise DHS.

D. ***Designate/Designation***: As used in this MD and as it applies to the identification of SSI, designate/designation refers to the original determination made by the Secretary, the Administrator, Transportation Security Administration (TSA), or the TSA Director of the SSI Program Office, pursuant to 49 CFR §1520.5(b)(16), that information not otherwise categorized as SSI under 49 CFR §1520.5(b)(1) through (15), warrants designation as SSI. It also includes a determination to protect detailed information about screening locations in accordance with 49 CFR §1520.5(b)(9)(iii).

E. ***DHS Covered Person***: As used in this MD, a DHS covered person is a DHS individual or entity covered or regulated by the SSI regulation, specifically an individual or entity with DHS transportation security or transportation security-related responsibilities in accordance with 49 CFR §1520.7(h). DHS covered persons have the authority to access and/or generate SSI and are subject to the requirements of this MD and other SSI implementing MD's, procedures, and guidance.

F. ***For Official Use Only (FOUO)***: The term used within DHS to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. Information affecting the National Security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958, "Classified National Security Information," as amended, or its predecessor or successor orders, is not to be considered FOUO. FOUO is not to be considered classified information. SSI is not FOUO as SSI is governed by statute.

G. ***Mark/Marking***: As used in this MD, mark/marking refers to the application of the SSI protective marking and distribution limitation statement required by 49 CFR §1520.13 and other associated markings by any DHS covered person to qualified information based on the criteria cited in 49 CFR §1520.5(b), the extraction of SSI information from existing SSI-marked source documents for use in a newly created document, or in accordance with other SSI Program Office-issued and/or approved implementing guidance.

H. ***Need-to-know***: As used in this MD, an individual or entity has a need-to-know SSI when they require access to specific SSI to accomplish assigned transportation security or transportation security-related tasks, as determined by an authorized holder of SSI in accordance with 49 CFR §1520.11.

I. ***Record***: As defined in 49 CFR §1520.3, the term record includes any document, presentation, spreadsheet, database, report, etc., used to present information regardless of media or format.

J. ***Redact***: As used in this MD, the permanent obscuring of SSI from a record to permit appropriate release to non-covered persons.

K. ***Sensitive Security Information (SSI)***: SSI is information that would be detrimental to transportation security if publicly disclosed, and is defined in 1520.5(b), as amended. SSI requires protection against public disclosure. 49 U.S.C. 114(s) limits the disclosure of information obtained or developed in carrying out certain security or research and development activities to the extent that it has been determined that disclosure of the information would be an unwarranted invasion of personal privacy; reveal a trade secret or privileged or confidential commercial or financial information; or be detrimental to transportation security. SSI is an information management system of sharing transportation security information with covered persons who have a need to know, without compromising security.

L. ***SSI Coordinator***: An official within an office who has been delegated responsibility for administration, coordination, and oversight of SSI within the applicable office. SSI Coordinators shall be appointed by Supervisors/Managers of offices that access and/or generate SSI. Supervisors/Managers shall serve as SSI Coordinators for their respective office until appointment of an SSI Coordinator.

M. ***SSI Program Manager***: Senior official, appointed pursuant to Section V.D. or V.G. of this MD, to oversee the administration and management of SSI within a Component or directorate. For TSA, the Director, SSI Program Office serves as the SSI Program Manager.

V. Responsibilities

A. The DHS Chief Security Officer shall:

1. Promulgate Department-wide policy governing the recognition, identification, and safeguarding of SSI.

2. Conduct periodic reviews of Components that access and/or generate SSI for effective management and practical application of SSI, to include random reviews of SSI records for consistent and appropriate application and use of SSI.

3. Coordinate with the Director, SSI Program Office, the development of any security classification guide that may identify information that would warrant protection as SSI.

4. Serve as a permanent member and provide technical advice and assistance to the DHS SSI Oversight Committee. Such appointment may be delegated.

B. TSA Administrator shall:

1. Serve as the delegated authority for implementation, management, and oversight of SSI within DHS pending a reevaluation of authorities and functional responsibilities to be completed by December 31, 2006. Such authority may be delegated.

2. Coordinate with other government agencies, such as the Department of Transportation, to ensure effective management and practical application of SSI, and consistent and appropriate application and use of SSI. Such coordination may be delegated.

3. Administer implementation, management, and oversight of SSI within TSA, and to the extent defined within this directive, within DHS, through appointment of a senior official to serve as the Director, SSI Program Office. Such official shall have the authority to review and approve or deny requests to designate, pursuant to 49 CFR §1520.5(b)(16), new types of SSI that would be detrimental to security if publicly disclosed, where that information is not otherwise protected as SSI under 49 CFR §1520.5(b)(1) through (15), and to review and approve or deny requests to protect information as SSI pursuant to 49 CFR §1520.5(b)(9)(iii).

4. Ensure that periodic and random reviews of TSA are conducted for effective management and practical application, and consistent and appropriate application and use of SSI. Such reviews shall assess compliance with regulations, policies, procedures, and guidance governing SSI recognition, identification, and safeguarding.

5. Ensure appointment of at least one employee in each TSA office that generates/accesses SSI to serve as SSI Coordinator, and grant each Coordinator authority to make determinations on behalf of DHS that records generated by that office are appropriately marked SSI.

C. Director, SSI Program Office shall:

1. Serve as the SSI Program Manager for TSA pursuant to Section V.E. below.

2. Participate in the coordination and publication of regulations and procedural guidance for the implementation and management of SSI within DHS. Serve as the approval authority for publication of Component- level SSI guidance and procedures.

3. Issue or approve detailed guidance, with common but extensive examples, on what type of information requires protection as SSI. Such guidance, when issued, shall serve as the primary basis and authority for the recognition and marking of information as SSI by DHS covered persons.

4. Establish, provide guidance for, and approve training programs for DHS persons who access or generate SSI records.

5. Establish and implement specialized training programs for DHS officials designated as SSI Program Managers or with designation authority.

6. Establish, provide guidance for, and approve processes and programs for the audit, oversight, and inspection of the management and practical application of SSI, to include random reviews of SSI records for consistent and appropriate application and use of SSI within DHS.

7. Establish, implement, and serve as Chair of the DHS SSI Oversight Committee.

8. Conduct periodic reviews and self-inspections of TSA for effective management and practical application of SSI, and consistent and appropriate application and use of SSI. Self-inspections shall be conducted in accordance with Section VI.G. of this MD.

9. Ensure appointment of TSA office-level SSI Coordinators. TSA SSI Coordinators shall be appointed as necessary within sixty (60) days of publication of this MD. As many SSI Coordinators may be appointed as are necessary to effectively implement and manage SSI recognition, identification, and safeguarding within the respective TSA offices.

10. Maintain an up-to-date record of all TSA SSI Coordinators.

D. Under Secretary, Science and Technology; Under Secretary, Preparedness; Under Secretary for Policy; Assistant Secretary, Office of Intelligence and Analysis; Assistant Secretary, Immigration and Customs Enforcement (ICE); Commissioner, U.S. Customs and Border Protection (CBP); and the Commandant, U.S. Coast Guard (USCG) shall:

1. Administer implementation and management of SSI within the respective Components through appointment of a senior official to serve as the SSI Program Manager for each respective Component. The appointed SSI Program Manager shall represent their respective entity on the DHS SSI Oversight Committee. SSI Program Managers shall be appointed within thirty (30) days of the publication of this MD.

2. Ensure appointment of at least one employee in each office that generates/accesses SSI to serve as SSI Coordinator, and grant each Coordinator authority to make determinations on behalf of DHS that records generated by that office are appropriately marked SSI.

3. Ensure that periodic and random reviews are conducted for effective management and practical application, and consistent and appropriate application and use of SSI. Such reviews shall assess compliance with regulations, policies, procedures, and guidance governing SSI recognition, identification, and safeguarding.

4. Where necessary, develop and implement, in coordination with the Director, SSI Program Office, supplemental internal Component SSI procedures specific to the management and administration of SSI within the Component. Such supplemental procedures shall be approved by the SSI Program Office prior to implementation.

E. SSI Program Manager shall:

1. Serve as the senior Component official responsible for management, implementation, and oversight of SSI within the Component.

2. Represent the Component to the SSI Oversight Committee.

3. Conduct periodic reviews and self-inspections of the respective Component for effective management and practical application of SSI, and consistent and appropriate application and use of SSI. Self-inspections shall be conducted in accordance with Section VI.G. of this MD.

4. Ensure appointment of office-level SSI Coordinators. SSI Coordinators shall be appointed as necessary within sixty (60) days of publication of this MD. As many SSI Coordinators may be appointed as are necessary to effectively implement and manage SSI within the respective offices. Maintain an up-to-date record of all Component SSI Coordinators and provide a copy to the TSA Director, SSI Program Office.

F. SSI Coordinator Shall:

1. Facilitate the administration and oversight of SSI within the applicable office.

2. Assist office personnel in the appropriate use and application of SSI and make determinations that records generated by that office are appropriately marked SSI.

3. Conduct periodic reviews and self-inspections of the respective office for effective management and practical application of SSI, and consistent and appropriate application and use of SSI. Self-inspections shall be conducted in accordance with Section VI.G. of this MD.

4. Ensure training of office personnel who access and/or generate SSI.

5. Keep abreast of SSI policies and procedures and maintain liaison with the Component SSI Program Manager.

G. Heads of Other Components shall:

1. Ensure compliance with the standards for recognition, identification, and safeguarding of SSI as cited in this MD and other implementing MDs.

2. Where appropriate based on the extent of contact and use of SSI, appoint a senior official to serve as the Component SSI Program Manager. The appointee shall represent the Component on the DHS SSI Oversight Committee and fulfill additional responsibilities as cited in Section E above.

3. Where appropriate, conduct periodic reviews of the respective Component for effective management and practical application of SSI, and consistent and appropriate application and use of SSI.

4. Where appropriate, appoint at least one employee in each office that generates/accesses SSI to serve as SSI Coordinator, and grant each Coordinator authority to make determinations on behalf of DHS that records generated by that office are appropriately marked SSI.

H. DHS SSI Oversight Committee shall:

1. Be chaired by the TSA Director, SSI Program Office, with membership consisting of Component SSI Program Managers appointed pursuant to this MD.

2. Establish a committee charter that outlines the authority, scope, and responsibilities of the committee. Development of the charter shall be a coordinated effort of the membership and approved by the TSA Administrator.

3. Be used as a forum for the discussion of policies and procedures related to the implementation, management, and oversight of SSI within DHS and an exchange of information related to lessons learned and best practices.

I. DHS employees, contractors, consultants, and other DHS covered persons to whom access to SSI is granted shall:

1. Be aware of and comply with the marking and safeguarding requirements for SSI as outlined in this MD and TSA-published or approved implementing regulations, directives, procedures, and guidance.

2. Be aware that divulging SSI without proper authority could result in administrative or disciplinary action, civil penalty, or other enforcement or corrective action.

3. Participate in formal classroom or computer-based training sessions presented to communicate the requirements for recognizing, identifying, and safeguarding SSI.

VI. Policy

A. General

1. Statutory and regulatory history: Prior to September 11, 2001, the Department of Transportation (DOT) Federal Aviation Administration (FAA) promulgated the regulation protecting SSI at 14 CFR Part 191 beginning in 1976, in accordance with anti-terrorism legislation passed by Congress in 1974. Following the terrorist attacks on the United States, Congress passed the Aviation and Transportation Security Act (ATSA), which established the Transportation Security Administration (TSA) and transferred the responsibility for civil aviation security to TSA. Among the statutory authorities previously administered by FAA that ATSA transferred was the authority in 49 U.S.C. § 40119, governing the protection of certain sensitive but unclassified information related to transportation security, which was transferred to 49 U.S.C. § 114(s). On February 22, 2002, TSA published a final rule transferring the bulk of FAA's aviation security regulations, including FAA's SSI regulation, to TSA. The TSA SSI regulation is now codified at 49 CFR Part 1520. In November 2002, Congress enacted the Homeland Security Act of 2002 (HSA), which transferred TSA to the newly established DHS. In connection with this transfer, the HSA also amended Section 40119 to vest similar SSI authority in the Secretary of DOT. Following the enactment by Congress of the Maritime Transportation Security Act in November 2002, TSA and DOT expanded the SSI regulation to incorporate maritime security measures implemented by USCG regulations and clarified preexisting SSI provisions in an interim final rule (IFR) issued on May 18, 2004, and effective June 17, 2004. The DOT SSI regulation is at 49 CFR Part 15, and the TSA SSI regulation remains at 49 CFR Part 1520. TSA and DOT subsequently issued a technical amendment to the SSI regulation on January 7, 2005, clarifying that land mode covered persons also have a need to know SSI.

2. TSA, through the SSI Program Office, shall issue, provide, and/or approve appropriate regulations, directives, procedures, and other guidance pertinent to the effective management and practical application, and consistent and appropriate application and use of SSI DHS-wide.

3. MDs and guidance issued by other Components for implementation within their respective Components shall be coordinated through and approved by the SSI Program Office prior to publication.

4. SSI shall only be used per the intent of Congress to protect information that would be detrimental to transportation security if publicly disclosed. It is not intended to be used to conceal Government mismanagement or other circumstances embarrassing to a Government agency. Pursuant to 49 U.S.C§114(s)(2) and 49 CFR. §1520.15(c), SSI may not be withheld from authorized committees of Congress. Further, pursuant to 49 CFR §1520.11(b)(1), SSI must be shared with members of Congress, their staffs, DHS or TSA management, the Comptroller General (Government Accountability Office), the TSA Office of Internal Affairs and Program Review, the DHS Office of Inspector General, Freedom of Information Act (FOIA) offices, any other official Government investigative body, or any other Federal employee if access to the information is necessary in the performance of the employee's official duties.

5. Under 49 CFR §1520.15(a), information properly marked as SSI is exempt from release under FOIA. Each Component is responsible for review and validation of SSI markings in their FOIA review process. Each Component shall draft FOIA SSI review policy and procedures and submit them to the SSI Program Office for approval within six (6) months of the publication of this MD. In accordance with 49 CFR §1520.15(b), to the extent practicable, redaction of the SSI shall be used to allow for the maximum release of non-SSI that is not otherwise exempt under FOIA.

6. This MD becomes effective upon the date of publication. Standards cited in existing SSI guidance published by Components prior to publication of this MD that are less than those cited in this MD are null and void. Any documents containing such standards shall be revised within six months of publication of this MD. Revised guidance issued pursuant to this MD shall be coordinated with and approved by the SSI Program Office prior to publication.

B. SSI Guidance

1. The SSI regulation, 49 CFR §1520.5(b)(1) through (16), provides fifteen categories [49 CFR §1520.5(b)(1) through 49 CFR §1520.5(b)(15)] of information that have been determined to be SSI. The SSI regulation also has one category, 49 CFR §1520.5(b)(16), and one part of one category, 49 CFR §1520.5(b)(9)(iii), under which an official, authorized pursuant to this MD, may designate that certain information not otherwise falling within the SSI categories represented in (b)(1) through (b)(15) is SSI.

2. The SSI Program Office shall issue guidance that significantly expands upon the descriptions for categories of information that must be marked and protected as SSI as cited in 49 CFR §1520.5(b)(1) through (15). To the extent possible, such guidance shall provide DHS covered persons with an accurate source for recognizing when and when not to apply the SSI marking and shall include common examples of specific types of information to be marked and protected as SSI. When published, this guidance shall serve as the primary authority and source for the recognition and marking of SSI by DHS covered persons.

C. Original Designation of Information as SSI

1. The Secretary, the TSA Administrator, and the TSA Director of the SSI Program Office, are authorized to designate information as SSI, pursuant to 49 CFR §1520.5(b)(16), that is not otherwise categorized as SSI under 49 CFR §1520.5(b)(1) through (15). This authority includes a determination to protect detailed information about screening locations in accordance with 49 CFR §1520.5(b)(9)(iii).

2. Only delegated officials as cited in C.1. above shall have the authority to designate information as SSI that is not otherwise covered under 49 CFR §1520.5(b)(1) through (15).

3. If information is identified or developed that would be detrimental to transportation security if publicly disclosed but it is not otherwise categorized as SSI under 49 CFR §1520.5(b)(1) through (15), it shall be transmitted through the applicable Component SSI Program Manager to the Director, SSI Program Office or the appropriate official cited in Section VI.C.1. above, for review and determination as to whether or not the information warrants protection as SSI. Such information shall be marked and protected as SSI on an interim basis in accordance with policies and procedures issued or approved by the SSI Program Office, pending a final assessment by the Director, SSI Program Office.

4. A record shall be maintained of each original SSI designation made. The record shall include the date, subject or title, and a detailed synopsis of the information. When the designation is made by an official other than the Director, SSI Program Office, a copy of the record and the information to be protected shall be transmitted to the TSA SSI Program Office within thirty (30) days following designation. Whenever possible, to maintain consistency, such designations should be done in consultation with the SSI Program Office prior to designation.

5. Information designated as SSI shall be marked in accordance with 49 CFR §1520.13. Additionally, the front page, title page, and/or the first page shall include the notation *"Designated SSI Pursuant to 49 CFR §1520.5(b)(16),"* or, *49 CFR §1520.5(b)(9)(iii),* as applicable. Where the official making the SSI designation is not otherwise evident, the additional notation *"Designated by (Name and Position of authorized official)"* shall be added.

6. Once information is properly designated as SSI under 1520.5(b)(9)(iii) or 1520.5(b)(16), the designation must be communicated to appropriate parties with a need to know.

D. Marking SSI

1. Any DHS covered person shall mark information as SSI if it meets the criteria for SSI as cited in 49 CFR §1520.5(b) and implementing guidance issued or approved by the SSI Program Office. Where there is doubt as to the applicability of an SSI category, the information shall be marked as SSI on an interim basis and submitted to the applicable office SSI Coordinator or Component SSI Program Manager for final assessment. If the information is believed to warrant protection as SSI but is not substantially governed by a category of information under 1520.5(b)(1) through (15) the SSI Program Manager shall refer the information as cited in VI.C.3. of this MD.

2. Information meeting the SSI criteria shall be marked in accordance with 49 CFR §1520.13. Additionally, the following markings shall be applied:

a. Subjects, titles, paragraphs, subparagraphs, charts, graphs, and similar portions (portion markings) need not be portion marked unless the record contains other types of information that does require portion marking, i.e., classified information, or, the information is to be transmitted outside of DHS to Congress or Congressional committees. When used, such portion markings shall be reviewed by the Component SSI Program Manager (in the case of TSA, the TSA Director, SSI Program Office) prior to dissemination. The parenthetical abbreviation (SSI) shall be used.

b. Portion markings will be applied to portions of a document within a classified document that contain only SSI. The parenthetical abbreviation (SSI) shall be used.

c. The Director, SSI Program Office, with the participation of the SSI Oversight Committee, shall conduct a study on the application of an authority line and the feasibility of using portion markings for all SSI records. No later than one year following publication of this MD the Director, SSI Program Office, through the SSI Oversight Committee, shall submit to the TSA Administrator and DHS Office of Security, a report detailing the results of the study and recommendations and justifications for the use or non-use of portion markings.

E. Duration of SSI and SSI Reviews

1. Information designated or marked as SSI will remain SSI unless determined releasable by the responsible designating agency official: TSA Administrator, the Commandant of the USCG, the TSA Director, SSI Program Office, or other authorized offices, in accordance with policies and procedures issued or approved by the SSI Program Office.

2. The TSA Director, SSI Program Office, shall coordinate with the USCG and the SSI Oversight Committee on the development and implementation of appropriate policy and procedures for the loss or removal of the SSI designation from information that has no current or future security implications under 49 CFR §1520.5(c).

3. In accordance with 49 CFR §1520.15(a) and Section VI.A.5 above, Component SSI Program Managers or other authorized Component offices may review and redact SSI records upon requests for public release under the Freedom of Information Act (FOIA) in accordance with policies and procedures issued or approved by the SSI Program Office.

4. Such offices may also redact SSI records in response to other public requests, e.g., litigation (civil, criminal, or employment), reports intended for public release, and other requests, in accordance with policies and procedures issued or approved by the SSI Program Office

F. Challenging SSI

1. Any authorized holder of SSI who believes the information has been improperly or erroneously marked as SSI is encouraged to challenge the marking. Such challenges may be done either informally or formally.

a. Informal challenges may be made directly by the holder of the information to the person that applied the SSI marking who shall reevaluate the marking against the criteria cited in 49 CFR §1520.5(b)(1) through (15) and implementing guidance published or approved by the TSA Director, SSI Program Office.

b. A formal challenge may be submitted, in writing, to the person that applied the SSI marking or to the applicable Component SSI Program Manager, the SSI Program Office, the applicable office SSI Coordinator, or the DHS Office of Security. An appeal to the decision made by the recipient of the challenge may be filed with the TSA Director, SSI Program Office. A further appeal to the decision made by the TSA Director, SSI Program Office, may be made to the TSA Administrator. The decision of the TSA Administrator shall be final.

c. Individuals submitting a challenge shall not be subject to retribution of any kind for bringing such actions. Anonymity can be requested by processing the challenge through the SSI Program Office or the DHS Office of Security. The SSI Program Office or the DHS Office of Security shall honor a challenger's request for anonymity and fully consider and appropriately process the challenge.

G. Audits and Inspections

1. Nothing in this directive shall diminish the authority of the Office of Inspector General to conduct audits, inspections, or investigations, in accordance with the Inspector General Act of 1978, as amended, 5 USC App., and DHS Management Directive 0810.1.

2. The DHS Office of Security shall, either independently or in conjunction with reviews conducted pursuant to DHS MD 11041, Protection of Classified National Security Information/Program Management, conduct periodic oversight and compliance reviews of SSI within DHS.

3. The TSA Director, SSI Program Office, shall develop, issue, or approve policies, procedures, and guidance for the implementation and management of self-inspection programs for Components that access or generate SSI. No later than sixty (60) days after publication of this MD, the SSI Program Office shall create, under the auspices of the SSI Oversight Committee, and publish or approve appropriate guidance and checklists to facilitate the conduct of self-inspections by SSI Program Manager's and SSI Coordinators. The DHS Office of Security shall also provide a means to monitor and track self-inspection program implementation.

4. SSI Program Managers shall conduct a self-inspection of their applicable Component SSI program no later than ninety (90) days from the publication of this MD and not later than every eighteen (18) months thereafter. The results of self-inspections conducted pursuant to this MD shall be reported to the SSI Program Office within thirty (30) days after completion. Discrepancies cited during the self-inspection shall be reconciled in a timely manner and follow-up by the SSI Program Manager or the SSI Program Office will be accomplished as needed.

5. SSI Coordinators shall conduct a self-inspection of the applicable office SSI program no later than 120 days from publication of this MD and no later than every twelve (12) months thereafter. The results of self-inspections conducted pursuant to this MD shall be reported to the applicable SSI Program Manager within thirty (30) days after completion. Discrepancies cited during the self-inspection shall be reconciled in a timely manner and follow-up by the SSI Coordinator or the SSI Program Manager will be accomplished as needed.

6. Self-inspections shall assess compliance with regulations, policies, procedures, and guidance governing SSI recognition, identification, and safeguarding.

H. Sharing, Dissemination and Access

1. SSI shall not be disseminated in any manner (orally, electronically, visually, or in any other manner) to unauthorized personnel. The TSA Administrator may determine in writing that information that might otherwise be considered SSI may be publicly released in the interest of transportation security or public safety under 1520.5(b) in accordance with procedures issued or approved by TSA. Under 1520.9(a)(2), the TSA Administrator and the Commandant of the USCG may also determine in writing that specific SSI may be released to non-covered persons in accordance with policies and procedures issued or approved by the SSI Program Office.

2. Access to SSI is based on "need to know" as determined by the holder of the information. Where there is uncertainty as to a person's need-to-know, the holder of the information will request dissemination instructions from his or her next-level supervisor or the originator of the information. Need to know is determined in accordance with 1520.11 and procedures issued or approved by the SSI Program Office. A Federal employee has a need to know SSI if access to the information is necessary for performance of the employee's official duties, and a person acting in the performance of a contract with or grant from DHS has a need to know SSI if access to the information is necessary to performance of the contract or grant. For specific SSI, DHS may make a finding under 1520.11(d) in accordance with procedures issued or approved by the SSI Program Office that only specific persons or classes of persons have a need-to-know. Under 1520.11(a), a DHS covered person has a need to know specific SSI if they need the SSI to: (1) "...carry out transportation security activities ...; (2) ... [receive] training to carry out transportation security activities ...; (3) ... supervise ... transportation security activities ...; (4) ... provide technical or legal advice to a covered person regarding transportation security requirements ...; or (5) ... represent a covered person in connection with any judicial or administrative proceeding regarding [transportation security]...".

3. A security clearance is not required for access to SSI. However, in accordance with 1520.11(c), a security background check or other procedures may be required by TSA or the USCG to receive specific SSI. The SSI Program Office must approve any SSI background check or processing requirements or procedures developed by the USCG or any other Component.

4. SSI shall be shared with other agencies, Federal, state, tribal, or local governments and law enforcement officials, provided a need-to-know in accordance with Part 1520.11 has been established and the information is shared in support of transportation security or in the furtherance of a coordinated and official governmental activity.

5. In accordance with 1520.11(b)(1) and 1520.15(c), SSI shall be shared with Congress, Congressional committees and staffers, the Government Accountability Office, the Office of Inspector General, and other similar entities acting within their official governmental capacities.

I. Storage and Handling

1. When unattended, SSI will, at a minimum, be stored in a locked container or in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know, such as a locked room, or an authorized area where access is controlled by a guard, cipher lock, or card reader. Additional guidance can be obtained through the SSI Program Office.

2. IT systems that store SSI will be certified and accredited for operation in accordance with Federal and DHS standards. Consult the DHS Information Technology Security Program Handbook for Sensitive Systems, Publication 4300A, or additional guidance published by the TSA SSI Program Office for more detailed information.

3. When removed from an authorized storage location and persons without a need to know are present, or where casual observation would reveal SSI to unauthorized persons, measures such as an unmarked folder, envelope, or SSI cover sheet shall be used to prevent unauthorized or inadvertent disclosure.

J. Transmission

1. When transmitting SSI, the SSI marking must be applied to the transmittal document (letter, memorandum, or fax). The transmittal document must contain a disclaimer noting that it is no longer SSI when it is detached from the SSI it is transmitting (transmittal e-mails do not need to contain this disclaimer), and a warning that if received by an unintended or different recipient, the sender must be notified immediately.

2. When discussing or transmitting SSI to another individual(s), all DHS covered persons must ensure that the individual with whom the discussion is to be held or the information is to be transferred has a valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise accessing the information.

3. SSI shall be mailed in a manner that offers reasonable protection of the sent materials and sealed in such a manner as to prevent inadvertent opening and show evidence of tampering.

4. SSI may be mailed by U.S. Postal Service First Class Mail or an authorized commercial delivery service such as DHL or Federal Express.

5. SSI may be entered into an inter-office mail system provided it is afforded sufficient protection to prevent unauthorized access, e.g., sealed envelope.

6. Electronic Transmission.

a. Transmittal via Fax. Unless otherwise restricted by the originator, SSI may be sent via non-secure fax. Where a nonsecure fax is used, the sender will coordinate with the recipient to ensure that the materials faxed will not be left unattended or subjected to possible unauthorized disclosure on the receiving end.

b. Transmittal via E-Mail or Other Electronic Messaging Systems

(1) SSI transmitted via email should be protected by encryption or transmitted within secure communications systems. When this is impractical or unavailable, SSI may be transmitted over regular email channels in accordance with policies and procedures issued or approved by the SSI Program Office.

(2) SSI shall not be sent to personal email accounts except under unique and urgent circumstances when immediate transmission of information is required in the interest of transportation security and transmittal through approved means is unavailable or impractical.

(3) The use of other electronic messaging systems must be approved by the SSI Program Office, responsible IT security offices, and appropriate Component SSI Program Managers.

c. DHS Internet/Intranet and Secure Portals

(1) SSI will not be posted on a DHS or any other internet (public) website or unprotected DHS or Component Intranet site.

(2) SSI may be posted on approved government-controlled or sponsored encrypted or otherwise protected portals (applications or data networks), such as the Homeland Security Information Network (HSIN), USCG HomePort, or TSA's WebBoards. Such posting shall be in accordance with guidance published or approved by the SSI Program Office and appropriate IT security offices.

K. Destruction.

1. In accordance with 1520.19(b), SSI will be destroyed when no longer needed and its continued retention is not otherwise required under records retention regulations. Destruction may be accomplished by:

a. "Hard Copy" materials will be destroyed by shredding, burning, pulping, or pulverizing, such as to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste.

b. Electronic records may be deleted in accordance with policies or procedures issued or approved by the SSI Program Office. Electronic storage media (compact discs, personal computers, etc.) shall be sanitized appropriately by overwriting or degaussing. Contact the SSI Program Office or the local IT security personnel for additional guidance.

c. Paper products containing SSI will not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

L. Incident Reporting

1. The loss, compromise, suspected compromise, or unauthorized disclosure of SSI must be reported. Incidents involving SSI in DHS IT systems will be reported to the Component Computer Security Incident Response Center in accordance with IT incident reporting requirements. The SSI Program Office shall, in coordination with the DHS SSI Oversight Committee, develop, publish or approve procedures for reporting, mitigating, and investigating incidents involving the improper handling, suspicious or inappropriate requests for, or unauthorized disclosures of SSI.

2. Each Component shall have its own delegated authority to pursue enforcement action of violations of the SSI regulation in accordance with Part 1520.17, other applicable statutes and regulations, and procedures issued or approved by the SSI Program Office.

M. Program Status Reporting

1. No later than January 15 of each year, each SSI Program Manager shall report, through the SSI Program Office to the DHS Office of Security, the total number of SSI records that were generated as SSI in their entirety for the preceding calendar year. SSI in their entirety means any document, the entire content of which the creator of the document believes to be SSI. Any document that the creator of the document believes contains a combination of SSI and information that is not SSI is not considered SSI in its entirety and therefore not reportable. The report shall include information as cited in Section VI.C.4. of this MD. DHS Office of Security shall compile this information into a single report for submission to the House and Senate Committees on Homeland Security no later than January 31 of each calendar year.

2. In addition to the information provided per M.1. above, each SSI Program Manager shall include the number of SSI Coordinators within their respective Components.

VII. Questions

Questions or concerns regarding this MD should be addressed to the DHS Office of Security or the SSI Program Office at ssi@dhs.gov.

EXHIBIT F

GAO

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

November 30, 2007

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

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

Subject: *Transportation Security Administration's Processes for Designating and Releasing Sensitive Security Information*

Since the September 11, 2001, terrorist attacks, federal agencies have faced the challenge of protecting sensitive information from terrorists and others without a need to know while sharing this information with parties who are determined to have such a need. One form of protection involves identifying and marking such information sensitive but unclassified—information that is generally restricted from public disclosure but not designated as classified national security information.

As part of post-September 11 efforts to better share information critical to homeland protection, sensitive but unclassified information has undergone scrutiny by Congress and GAO. In March 2006, we reported results from our survey of 26 federal agencies, from which we found that most of the agencies lacked policies and procedures for designating and releasing sensitive but unclassified information. As a result, we recommended governmentwide implementation of (1) guidance for determining what information should be protected with sensitive but unclassified designations, (2) provisions for training on making designations and for controlling and sharing information with other entities, and (3) a review process to determine how well the program is working.[1]

[1] GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.: Mar. 17, 2006).

The Department of Homeland Security's (DHS) Transportation Security Administration (TSA) requires that certain information be protected from public disclosure as part of its responsibility for securing all modes of transportation. TSA, through its authority to protect information as sensitive security information (SSI), prohibits the public disclosure of information obtained or developed in the conduct of security activities that, for example, would be detrimental to transportation security. According to TSA, SSI 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.

In February 2005, TSA established its SSI office to develop and implement TSA policies concerning the handling, training, and protection of such information. Through this office, TSA has established regulations that allow for the sharing of SSI with covered persons having a need to know—including airport and aircraft operators, foreign vessel owners, and TSA employees.[2] If, however, persons who do not otherwise have a need to know request access to SSI, TSA may share or release such information if it determines the information no longer requires protection as SSI. Also, in the course of a civil proceeding, a requesting party or the party's attorney may be granted access to SSI after being cleared through a background check. This is permissible if the party has established that it has a substantial need for relevant SSI and that it is unable, without undue hardship, to obtain the substantial equivalent by other means. Furthermore, TSA or the judge in the civil proceeding must determine that the sensitivity of the information at issue does not present a risk of harm to the nation.

Congress has had ongoing interest in whether TSA is consistently and appropriately designating information as SSI and balancing the trade-off between the need to protect SSI and the need to provide useful information to the public. Section 525 of the DHS Appropriations Act, 2007 (Public Law 109-295), required the Secretary of DHS to revise Management Directive (MD) 11056, which establishes DHS policy regarding the recognition, identification, and safeguarding of SSI, to (1) review requests to publicly release SSI in a timely manner and establish criteria for the release of information that no longer requires safeguarding; (2) release certain SSI that is 3 years old, upon request, unless it is determined the information must remain SSI or is otherwise exempt from disclosure under applicable law; and (3) provide common and extensive examples of the 16 categories of SSI (see app. I for a list of the categories) to minimize and standardize judgment by persons identifying information as SSI.[3] The law further prescribed steps that must be taken during the course of a civil proceeding in the U.S. District Courts to provide a party with access to relevant SSI. This provision also required us to report to the Committees on Appropriations of the Senate and House of Representatives on DHS's progress and procedures in implementing these requirements not later than 1 year from the date of the law's enactment (October 4, 2006).

In addition to answering this mandate, we are following up on a June 2005 report in which we recommended that DHS direct the Administrator of TSA to establish (1) guidance and procedures for using TSA regulations to determine what constitutes SSI, (2) responsibility for the identification and determination of SSI, (3) policies and procedures within TSA for

[2] "Covered person" is defined at 49 C.F.R. § 1520.7 and includes persons permanently or temporarily assigned, attached, or detailed to, employed by, or under contract with DHS. Section 1520.11 establishes the circumstances under which a person has a need to know SSI, such as when a person requires access to specific SSI to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or the Department of Transportation.

[3] See Pub. L. No. 109-295, § 525, 120 Stat. 1355, 1381-82 (2006).

providing training to those making SSI determinations, and (4) internal controls[4] that define responsibilities for monitoring compliance with SSI regulations, policies, and procedures and communicate these responsibilities throughout TSA.[5]

To respond to the mandate and update the status of all four of our recommendations, we assessed DHS's

- status in establishing criteria and examples for identifying SSI;
- efforts in providing training to those that identify and designate SSI;
- processes for responding to requests to release SSI, including the legislative mandate to review various types of requests to release SSI; and
- efforts in establishing internal controls that define responsibilities for monitoring SSI policies and procedures.

To address these objectives, we reviewed applicable DHS management directives, policies and procedures, and other related documents, and interviewed TSA and DHS officials involved in, the SSI designation, training, document review, and oversight processes. While our review focused on the policies and procedures developed by TSA, we also interviewed officials involved in the SSI designation, training, document review, and oversight processes for four other DHS components to better understand the use of SSI throughout DHS. We compared the internal controls in place with the standards for internal control in the federal government to determine whether TSA's internal controls are designed to provide reasonable assurance that monitoring exists to help ensure compliance with SSI regulations, policies, and procedures.[6] We also used as criteria GAO-developed core characteristics of a strategic training program to assess whether TSA has created and implemented the training necessary for staff to make SSI determinations.[7] We determined that the data were sufficiently reliable for the purposes of our review. We based our decision on an assessment of existing documentation on program operations and interviews with knowledgeable officials about the source of the data and TSA's policies and procedures for collecting and maintaining the data.

On October 4, 2007, we provided a copy of our briefing slides to your staff. This report conveys the information that was provided in these slides (see app. I).

We conducted our work from May 2007 through October 2007 in accordance with generally accepted government auditing standards.

[4] Internal control is an integral component of an organization's management that provides reasonable assurance that the following objectives are achieved: (1) effectiveness and efficiency of operations, (2) reliability of financial reporting, and (3) compliance with applicable laws and regulations.
[5] See GAO-05-677, *Transportation Security Administration: Clear Policies and Oversight Needed for Sensitive Security Information* (Washington, D.C.: June 29, 2005).
[6] GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).
[7] GAO, *A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G (Washington, D.C.: March 2004).

Results

DHS, primarily through TSA's SSI Office, has addressed all of the legislative mandates from the DHS Appropriations Act, 2007, and taken actions to satisfy all of the recommendations from our June 2005 report.

DHS revised its MD to address the need for updating SSI guidance, and TSA has established more extensive SSI criteria and examples that respond to requirements in the DHS Appropriations Act, 2007, and our 2005 recommendation that TSA establish guidance and procedures for using TSA regulations to determine what constitutes SSI. Further, TSA has documented the criteria and examples in various publications to serve as guidance for identifying and designating SSI. TSA has also shared its documentation of the criteria and examples with other DHS agencies. For example, the U.S. Coast Guard and U.S. Customs and Border Protection either have developed or are in the process of developing their own SSI examples to correspond with the types of SSI that their agencies encounter. Additionally, officials we interviewed from other DHS components have recognized opportunities to adapt TSA's criteria to their offices' unique needs. Furthermore, TSA has appointed SSI coordinators at all program offices to, among other things, implement SSI determination policy. This action responds to our 2005 recommendation that TSA establish responsibility for identifying and determining SSI.

TSA's SSI Office is in the process of providing SSI training to all of TSA's employees and contractors in accordance with its recently established policies and procedures, an action that responds to our 2005 recommendation. The office uses a "train the trainer" program in which it instructs SSI program managers and coordinators who are then expected to train appropriate staff in their respective agencies and programs. Several aspects of the SSI training program that we evaluated are consistent with GAO-identified components of a strategic training program. TSA has taken actions to incorporate stakeholder feedback and establish policies to collect data to evaluate its training program and foster a culture of continuous improvement. For example, the SSI Office assesses the accuracy of the designations made by various DHS agencies and contacts the agencies, when necessary, to correct any problems. Additionally, TSA has taken action to coordinate training activities within and among DHS agencies. For instance, the SSI Office shares its guidance with other DHS components so that program managers can create customized training programs that will meet the needs of their staff.

Consistent with the legislative mandate, DHS has taken actions to update its processes to respond to requests to release SSI. Specifically, DHS revised MD 11056 in accordance with the DHS Appropriations Act, 2007, to incorporate a provision that all requests to publicly release SSI will be reviewed in a timely manner, including SSI that is at least 3 years old. Between February 2006 and January 2007, the SSI Office received 490 requests to review records pertaining to the release of SSI, the majority of which came from government entities (62 percent). The SSI Office worked with the requesting government entity to agree upon a time frame for processing the request. Within the same 12-month period, 30 percent of requests were initiated by the public under the Freedom of Information Act (FOIA).[8] The SSI Office has established a process for reviewing information requested through the FOIA process in 5 days, unless the information consists of more than 100 pages. The remaining 8 percent of requests within the 12-month period came from individuals in connection with litigation, including civil proceedings within the U.S. District Courts. According to TSA,

[8] The Freedom of Information Act is the primary process for releasing information to (and for withholding information from) information to the public, as appropriate. See 5 U.S.C. § 552. SSI, by statute, is exempt from disclosure under FOIA.

parties have sought SSI in nine civil proceedings since the enactment of the DHS Appropriations Act, 2007, in October 2006. In one such proceeding, the litigant requested that TSA make a final determination on the request for access to SSI. TSA, in accordance with the law, made a final determination in which it released some of the requested SSI but withheld other SSI because of the sensitivity of the information or because it was not relevant to the litigation. TSA's SSI Office stated that all information that is at least 3 years old that does not warrant continued protection as SSI is released upon request. The SSI Office uses a controlled access database to document the completion of its steps in reviewing requests to release SSI, which serves as a quality control mechanism.

The internal controls that TSA designed for SSI are consistent with governmentwide requirements and respond to our 2005 recommendation. For example, standards for internal controls in the federal government state that areas of authority and responsibility be clearly defined by a supportive management structure and that controls be in place to ensure that management's directives are carried out. The revised DHS MD 11056 outlined areas of authority for the monitoring of and compliance with SSI policy. Further, the MD established managers and coordinators within DHS agencies and programs, respectively, to communicate SSI responsibilities to DHS staff. Standards for internal controls in the federal government also call for monitoring activities to assess the quality of program performance over time and ensure that problems raised during quality reviews are promptly resolved. TSA program managers and coordinators are required to periodically complete self-inspections on the use of SSI for their respective office or agency.

Agency Comments

We provided a draft of this report to DHS for review and comment. DHS did not submit any formal comments. However, TSA provided technical comments and clarifications, which we incorporated, as appropriate.

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

If you or your staff have any questions concerning this report, please contact me at (202) 512-6510 or by e-mail at Larencee@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report were Glenn Davis, Assistant Director; Brian Sklar; Nicole Harris; Thomas Lombardi; Katherine Davis; Carolyn Ikeda; and Michele Fejfar.

Eileen Regen Larence

Eileen R. Larence, Director
Homeland Security and
Justice Issues

Enclosure

GAO

Transportation Security Administration's (TSA) Processes for Designating and Releasing Sensitive Security Information (SSI)

Briefing to the Appropriations Committees
October 4, 2007

1

GAO

Introduction

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

2

GAO

Introduction

- SSI constitutes one category of "Sensitive but Unclassified" (SBU) information – information generally restricted from public disclosure but that is not classified national security information.
  - SSI is an SBU category specifically required by statute (other examples include Protected Critical Infrastructure Information and Privacy Act information).
  - Categories of SBU information not specifically mandated by statute include For Official Use Only and Law Enforcement Sensitive Information.
- The Freedom of Information Act (FOIA) is the primary process for releasing information to (and for withholding information from) the public, as appropriate. See 5 U.S.C. § 552. SSI, by statute, is exempt from disclosure under FOIA.

3

GAO

Introduction

- TSA, through its SSI authority, prohibits the public disclosure of information obtained or developed in the conduct of security activities that would be detrimental to transportation security.
- According to TSA, SSI is generated by TSA, other DHS agencies, airports, aircraft operators, and other regulated parties, when they are establishing or implementing security programs or documentation to address security requirements.
- SSI regulations allow for the sharing of SSI with covered persons having a need to know–including airport operators, aircraft operators, foreign vessel owners, TSA employees, and other persons.[1]
- According to TSA, safeguarding information as SSI allows controlled information sharing with covered persons to meet TSA's mission to protect the nation's transportation systems.

[1] "Covered person" is defined at 49 C.F.R. § 1520.7 and includes persons permanently or temporarily assigned, attached, or detailed to, employed by, or under contract with DHS. Section 1520.11 establishes the circumstances under which a person has a need to know SSI, such as when a person requires access to specific SSI to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or the Department of Transportation.

4

GAO

Introduction

TSA's SSI Office:

- Was established in February 2005 to develop and implement TSA policies concerning SSI handling, training, and protection.
- Provides guidance and training to other DHS agencies that use SSI, such as U.S. Customs and Border Protection, and serves as the Chair of the SSI Oversight Committee, which meets monthly to share SSI guidance and best practices.
- Reviews requests for SSI, including FOIA requests that might contain SSI.
- Is not responsible for ensuring the appropriate use of SSI markings by other DHS agencies. The exception to this rule occurs when the SSI Office is asked by other agencies to assist in responding to a request to release SSI. In such cases, the SSI Office reviews the information and provides a determination to the other agency as to whether the information has been appropriately marked as SSI.

5

GAO

Introduction

- There is ongoing congressional interest in whether TSA is applying the SSI criteria consistently and appropriately and balancing the trade-off between the need to protect SSI and the need to provide useful information to the public.
- One example of an instance is when an individual might seek SSI in connection with a civil proceeding in a U.S. District Court. TSA will make an initial determination on whether the party has a substantial need for any of the specific SSI to which access is sought and whether the sensitivity of the issue is such that any provisions of access would present a risk of harm to the nation.

6

GAO

Introduction

Section 525 of the DHS Appropriations Act, 2007 (Public Law 109-295), requires the Secretary of DHS to revise Management Directive (MD) 11056–which establishes the department's policy regarding the recognition, identification, and safeguarding of SSI–to provide for the following:[2]

- review requests to publicly release SSI in a timely manner and release information that no longer requires safeguarding as SSI;
- release certain SSI that is 3 years old upon request unless it is determined the information must remain SSI or is otherwise exempt from disclosure under applicable law; and
- provide common and extensive examples of the 16 categories of SSI (see attachment 1 for a list of the categories) to minimize and standardize judgment by persons identifying information as SSI.

The law further prescribes steps that must be taken during the course of a civil proceeding in the U.S. District Courts when a party seeking access to SSI demonstrates a substantial need for the information and cannot, without undue hardship, obtain the substantial equivalent of the information by other means.

This law also requires GAO to report to the Committees on Appropriations of the Senate and the House of Representatives on DHS progress and procedures in implementing these requirements not later than 1 year from the date of enactment of the Act (October 4, 2006). This briefing responds to that mandate.

[2] See Pub. L. No. 109-295, § 525, 120 Stat 1355, 1381-82 (2006).

7

GAO

Introduction

In June 2005,[3] we recommended that DHS direct the Administrator of TSA to establish:

- guidance and procedures for using TSA regulations to determine what constitutes SSI;
- responsibility for the identification and determination of SSI;
- policies and procedures within TSA for providing training to those making SSI determinations; and
- internal controls that define responsibilities for monitoring compliance with SSI regulations, policies, and procedures and communicate these responsibilities throughout TSA.

[3] See GAO-05-677, *Transportation Security Administration: Clear Policies and Oversight Needed for Sensitive Security Information* (Washington, D.C.: June 29, 2005).

8

GAO

Objectives

To respond to the mandate and update the status of our recommendations, we established four objectives. Specifically, we assessed DHS's:

1. status in establishing criteria and examples for the identification of SSI;
2. efforts in providing training to those that identify and designate SSI;
3. processes for responding to requests to release SSI, including the legislative mandate to review various types of requests to release SSI; and
4. efforts in establishing internal controls that define responsibilities for monitoring SSI policies and procedures.

9

GAO

Scope and Methodology

To address the objectives we:

- reviewed applicable DHS management directives, policies and procedures, and other documents related to SSI designation, training, document review, and the oversight process, and
- interviewed TSA and DHS officials involved in the SSI designation, training, document review, and oversight process.

10

GAO

Scope and Methodology

- Our review focused on the policies and procedures developed by TSA's SSI Office, but we also interviewed officials from four additional DHS agencies to better understand the use of SSI throughout DHS.
- We compared the internal controls in place with the standards for internal control in the federal government to determine whether TSA's internal controls are designed to provide assurance that monitoring is in place and a control environment and activities have been established.[4]
- We also used as criteria GAO-developed core characteristics of a strategic training program to assess whether TSA has created and implemented the training necessary for staff to make SSI determinations.[5]
- We determined that the data were sufficiently reliable for the purposes of our review. We based our decision on an assessment of existing documentation on program operations, and interviews with knowledgeable officials about the source of the data and TSA's policies and procedures for collecting and maintaining the data.
- We conducted our work from May 2007 through October 2007 in accordance with generally accepted government auditing standards.

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

[5] GAO, *A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, GAO-04-546G (Washington, D.C.: March 2004).

11

GAO

Results in Brief

TSA has established SSI criteria and examples, and several DHS agencies have recognized opportunities to adapt the SSI criteria to their unique needs:

- DHS revised its MD to address the need for SSI criteria and examples in accordance with the law.
- TSA has shared its documentation of SSI criteria and examples with other DHS agencies to help them identify and designate SSI.[6]
- Officials we interviewed from DHS agencies that work with or generate SSI products stated that they have developed, or are in the process of developing, their own SSI examples to correspond with the types of SSI that their agencies encounter.

[6] In the context of this research, we use the term "designate" to include the identification and marking of information as SSI. It should be noted that the SSI Office uses the term "designate" to mean an original SSI determination in writing. See 49 C.F.R. § 1520.5(b)(9)(ii), (16). Under the DHS MD, only the DHS Secretary, the TSA Administrator, and the Director of the SSI Office have the authority to designate SSI.

12

GAO

Results in Brief (cont'd)

TSA is providing SSI training, and aspects of the training program are consistent with several GAO-identified components of a high-quality training program:

- The SSI Office has developed an SSI training program and has shared this program with DHS agencies that use and generate SSI.
- TSA documentation from mid-September 2007 shows that 93.5 percent of TSA personnel (all employees and contractors) assigned to headquarters and 95.5 percent of TSA personnel assigned to airports have completed online SSI training.[7]
- The SSI Office uses a "train the trainer" model in which it trains SSI program managers and coordinators who are then expected to train appropriate staff in their agency.
- Several aspects of the SSI training program are consistent with GAO-identified components of a high-quality training program. For example, TSA is soliciting feedback to evaluate the quality of the SSI training that it is providing.

[7]The SSI Office stated that all TSA employees have not completed the online SSI training because of normal attrition, military leave, and disability leave.

13

GAO

Results in Brief (cont'd)

TSA has policies and procedures to respond to all three types of SSI requests, and a mechanism is in place to document its processes:

- The SSI Office has a procedure in place to respond to requests from government entities, FOIA-related requests, and requests stemming from civil proceedings.
- TSA plans to publish a Notice of Proposed Rulemaking to articulate the process for providing SSI to parties in connection with civil proceedings in U.S. District Courts.
- The SSI Office has a process for recording its steps when reviewing requests to release SSI that serves as a quality control mechanism.

14

GAO

Results in Brief (cont'd)

TSA has established internal controls for SSI and created mechanisms to communicate these controls, which are consistent with internal control standards for the federal government:[6]

- DHS revised its MD to define responsibilities for monitoring the compliance with SSI regulations, policies, and procedures.
- The MD establishes SSI program managers and coordinators to communicate SSI responsibilities with staff in their respective offices and agencies.
- Various tools are used to monitor the compliance with SSI regulations, policies, and procedures including self-inspections, agency audits, and SSI Office reviews based on requests to release SSI.
- The internal controls TSA designed for monitoring compliance with SSI regulations, policies, and procedures are consistent with internal control standards for the federal government.

[6]GAO/AIMD-00-21.3.1.

15

GAO

Objective #1--Criteria and Examples for the Identification of SSI

DHS revised MD 11056 in accordance with section 525 of the DHS Appropriations Act, 2007, to address the need for common and extensive examples of individual categories of SSI. In response to this mandate, as well as GAO's past recommendation, DHS issued a revised MD (MD 11056.1) and the TSA SSI Office issued the following guidance:

- Advanced Application Guide: provides SSI criteria and examples for each of the categories,
- One-Page Summary List of SSI Criteria: provides SSI criteria and explanatory notes for each category,
- SSI Identification Guides: provide guidance for identifying SSI within the context of specific DHS programs, and
- SSI Reviewers' Guide: provides a more detailed version of the Advanced Application Guide that SSI Office analysts use to review requests for SSI.

16

GAO

Objective #1–Criteria and Examples for the Identification of SSI

- TSA has shared its SSI criteria and examples with other DHS agencies to help them identify and designate SSI.
- Officials we interviewed from DHS agencies that work with or generate SSI products stated that they have developed, or are in the process of developing, their own SSI examples to correspond with the types of SSI that their agencies encounter. For example:
  - U.S. Coast Guard worked with the SSI Office to develop an SSI Identification Guide that provides examples of the application of SSI criteria to documents generated by the Coast Guard; and
  - U.S. Customs and Border Protection has identified the need to create its own SSI Identification Guide and is currently working with the SSI Office to create the guidance.

17

GAO

Objective #1–Criteria and Examples for the Identification of SSI

- Using the SSI criteria and examples provided by the SSI Office, DHS agencies that use SSI identify certain records as containing SSI. Section 537 of the DHS Appropriations Act, 2006 (Public Law 109-90), enacted October 2005, mandated that DHS provide an annual list of all DHS documents that are designated SSI in their entirety for the period October 1, 2005, through December 31, 2005. Beginning on January 31, 2007 (and annually thereafter), the DHS Secretary is to provide a report on all documents designated SSI in their entirety for the prior calendar year. Therefore, the report provided to Congress in 2006 covered a 3-month period (it was due no later than January 31, 2006), whereas the report provided in January 2007covered the entire prior calendar year, 2006.
- There were 118 documents in the report provided by DHS in 2007.[9] Below are the DHS agencies that generated documents from the 2006 list and their relative percentage of documents generated:
  - Coast Guard (50 percent),
  - Office of Science and Technology (37 percent), and
  - TSA (13 percent).
- As a result of policy updates made by the SSI Office, 282 documents generated by TSA determined to be SSI in their entirety as reported to Congress in 2006 no longer met the criteria for continued SSI protection in their entirety. Therefore, if requested, some of the information contained in these documents could be publicly released. The removal of the 282 documents also helps to explain the smaller number of SSI documents DHS reported to Congress in 2007, particularly from TSA.

[9] According to the report DHS provided to Congress in 2007, U.S. Customs and Border Protection did not report any documents that it generated and determined were SSI in their entirety.

18

GAO

Objective #2–Training for Those Who Generate and Use SSI

In response to GAO's recommendation to provide training to staff that generate SSI, TSA:

- Requires new employees to take 60-minute online SSI training within the first week of employment. TSA documentation from mid-September 2007 shows that 93.5 percent of TSA personnel (all employees and contractors) assigned to headquarters and 95.5 percent of TSA personnel assigned to airports have completed the online training or completed the live training.[19]
- Provides recurring training to SSI coordinators from offices within DHS agencies that use SSI.
- Provides 60-minute live training to TSA and selected DHS employees.
- Develops specialized training for TSA contractors, SSI coordinators, and others as needed.

[19] TSA documentation shows that 3,097 out of 3,309 TSA personnel in headquarters and 49,526 out of 51,930 personnel assigned to airports have completed online SSI training.

19

GAO

Objective #2–Training for Those Who Generate and Use SSI

- Although the SSI Office provides training to all SSI program managers and coordinators from the DHS agencies that use or generate SSI, the program manager from each DHS agency that handles SSI is responsible for customizing and evaluating the sufficiency of his or her SSI training to meet the agency's unique program needs.
- The SSI Office is utilizing a "train the trainer" model in which it trains SSI program managers and coordinators who are then expected to tailor the materials to train the appropriate staff in their agency or office.

20

GAO

Objective #2–Training for Those Who Generate and Use SSI

TSA's training and development efforts reflect the following core characteristics that GAO has identified for a strategic training process:[11]

Stakeholder Involvement, Accountability, and Recognition: incorporate stakeholder feedback throughout the training process and establish accountability mechanisms to hold managers and employees responsible for learning in new ways.

- The SSI Office collects stakeholder feedback on its training program through training evaluation forms, its e-mail address, over the phone, and through the DHS SSI Oversight Committee.
- In an attempt to establish accountability for whether training has led to accurate SSI identifications, the SSI Office requires program managers and coordinators to complete self-evaluations that include evaluations of a selection of SSI designations in their respective office or agency.
- SSI coordinators are required to complete a self-inspection every 12 months, and SSI program managers are required to complete a self-inspection every 18 months.

[11] GAO-04-546G.

21

GAO

Objective #2–Training for Those Who Generate and Use SSI

Effective Resource Allocation and Partnerships and Learning from Others: provide the appropriate level of funding and resources to ensure that training is achieving its missions and goals, and coordinate within and among agencies to achieve economies of scale.

- The creation of the DHS SSI Oversight Committee provides a mechanism for interagency coordination.
- The SSI Office shares its guidance with other DHS components so that program managers can create customized training programs that will meet the needs of their staff.
- According to TSA officials, additional funding would allow the SSI Office to provide more training and to create a national conference for SSI coordinators.

22

GAO

Objective #2–Training for Those Who Generate and Use SSI

Data Quality Assurance and Continuous Performance Improvement: establish policies to collect quality data and use these data to evaluate the training program, and foster a culture of continuous improvement by assessing and refining the training program.

- The SSI Office provides all DHS staff that complete live SSI training with a training evaluation form to evaluate both the content of the training and the quality of instruction.
- During its process of responding to requests to release SSI, the SSI Office evaluates the accuracy of designations made by various DHS agencies. If the SSI Office finds that the information has been inaccurately identified as being SSI, it can contact the DHS agency that made the original designation to identify the error. This allows DHS agencies to follow up with refined training to correct the problem as necessary.
- The SSI Office began conducting audits within TSA in September 2007 to evaluate whether SSI is being appropriately marked and protected at various airports. The SSI Office invited other program managers to attend the audits so that lessons learned from the audits may be incorporated by other DHS agencies.

The aspects of the SSI training program evaluated in this study are consistent with GAO identified components of a high-quality training program.

23

GAO

Objective #3–Processes for Responding to Requests to Release SSI

Between February 2006 and January 2007, the SSI Office received 490 requests to review records pertaining to the release of SSI. For January 2007 through April 2007, the SSI Office reported the percentage of the total requests to review records by each type of request it processes, as follows:

1. requests from government entities (62 percent);
2. FOIA requests that may contain SSI (30 percent); and
3. requests from individuals in connection with litigation, including civil proceedings, within U.S. District Courts (8 percent).[12]

On most occasions, the SSI Office is able to respond to all types of requests within 7-14 days. TSA documentation indicates that the SSI Office is able to meet this goal in 92 percent of all requests. The SSI Office stated that it is not able to complete all requests within its 7-14 days due to the size and complexity of certain requests, as well as the client's needs and the SSI Office's workload.

[12] According to TSA, additional programming to the SSI Office database would be required to show the percentage for the three types of SSI requests (litigation, FOIA, and other) for February 2006 – January 2007.

24

GAO

Objective #3–Requests for SSI by Government Entities

- Requests for SSI from government entities can include requests from federal, state, local, or tribal governments.
- The SSI Office works with the requesting government entity to agree upon a time frame for processing the request.
- All requests for SSI, including requests from government entities, are reviewed by the SSI Office through a nine-step process (see attachment II for more details on this process).

25

GAO

Objective #3–Requests for SSI through the Freedom of Information Act

- The SSI Office has established a process for reviewing information requested through the FOIA process in 5 days, unless the request contains more than 100 pages.
- The SSI Office and FOIA Office coordinate to establish deadlines for FOIA requests that contain more than 100 pages.
- Officials from the TSA FOIA Office stated that the SSI Office responds to FOIA requests in a timely manner.
- The SSI Office has provided training to the department's FOIA Office staff members so that they can make basic determinations on whether a FOIA request might include SSI.

26

GAO

Objective #3–Process for Responding to Requests to Release SSI That Is at Least 3 Years Old

- The information that should be designated as SSI, based on the application of the current identification (ID) guidance, may change over time, given changing circumstances. For example, the TSA Administrator may decide to publicly disclose information previously designated as SSI to increase public awareness of an issue or security program.
- At the time of a request to release SSI, all requested information is to be reviewed against the SSI categories and current precedents for applying each category. This process is to occur with all requested SSI, regardless of the age of the information.
- According to SSI Office officials, the content of the information being requested is the relevant factor to be considered, not the age of the information.
- All SSI that is at least 3 years old that does not warrant continued protection as SSI is released upon request.

27

GAO

Objective #3–Requests for SSI during Civil Proceedings

- According to TSA's Office of Chief Counsel, persons who do not otherwise have a "need to know" sought SSI 48 times in connection with civil proceedings since TSA was established. Since the enactment of Public Law 109-295 in October 2006, 9 such requests for SSI have been made in connection with civil proceedings.
- Prior to the passage of Public Law 109-295, TSA did not permit SSI access in civil proceedings by persons who did not otherwise have a need to know. TSA did submit SSI to courts for *in camera* review.[13]
- Section 525(d) of Public Law 109-295 prescribes steps that must be taken during the course of a civil proceeding in the U.S. District Courts when a party seeking access to SSI demonstrates a substantial need for the information and that it cannot, without undue hardship, obtain the substantial equivalent of the information by other means.
- Since the enactment of this provision, one litigant has requested that TSA make a final determination on a request for SSI access in connection with civil proceedings. TSA complied with this request and, in accordance with the law, issued a final determination releasing some of the requested SSI while withholding other SSI because of the sensitivity of the information or because it was not relevant to the litigation.

[13] *In camera* review means a trial judge's private consideration of evidence.

28

GAO

Objective #3–Requests for SSI during Civil Proceedings

According to TSA documentation:

- If TSA or the judge decides that a party in a civil proceeding has demonstrated that it has a substantial need for relevant SSI and that it is unable without undue hardship to obtain the substantial equivalent of the information by other means, and if TSA or the judge has determined that the sensitivity of the SSI at issue does not present a risk of harm to the nation, TSA will begin a background check of the requesting party or the party's attorney who has been designated to view the SSI.
- Once TSA has received a party's payment to conduct the background check, and the party has completed an SSI threat assessment questionnaire and been fingerprinted, it takes approximately 3 weeks to complete the background check.
- If TSA determines that there is risk to the nation to provide a party or a party's attorney with SSI based on the results of the background check, TSA will deny the applicant's request. At that time, the party may designate a new attorney to access SSI on its behalf. If this occurs, TSA will conduct a background check on the new attorney.
- The determination of whether SSI will be released to a party in civil proceedings is a joint determination made by TSA's Office of Chief Counsel and the SSI Office.

29

GAO

Objective #3–SSI Office Efforts to Establish Quality Controls for Responding to SSI Requests

The SSI Office's use of a controlled access database to document the completion of its steps in the review of requests to release SSI serves as a quality control mechanism. This is achieved by:

- incorporating controls in the database so that the previous step must be documented before information can be entered in the next step of the review process; and
- requiring that a senior analyst within the SSI Office approve the SSI review and document his or her approval in the database prior to releasing information formerly protected as SSI.

TSA is also currently drafting a Notice of Proposed Rulemaking in anticipation of establishing its processes and procedures for responding to requests for SSI during civil proceedings.

30

GAO

Objective #4–DHS SSI Internal Controls Are Consistent with Internal Control Standards for the Federal Government

TSA has established internal controls for SSI and created mechanisms to communicate these controls that are consistent with internal control standards for the federal government.[14]

Control Environment and Control Activities: areas of authority and responsibility to be clearly defined by a supportive management structure and controls in place to ensure that management's directives are carried out.

- Areas of authority for the monitoring and compliance of SSI policy are outlined in the revised DHS MD (MD 11056.1) and other agency and departmental guidance.
- SSI program managers and coordinators have been established in the MD to communicate SSI responsibilities with DHS staff.

[14] GAO/AIMD-00-21.3.1.

31

GAO

Objective #4–DHS SSI Internal Controls Are Consistent with Internal Control Standards for the Federal Government

Monitoring: information is used to assess the quality of program performance over time and problems raised during quality reviews are promptly resolved.

- Controls are in place to provide oversight for each agency's generation and designation of SSI including self-inspection reporting methods. The self-inspection process requires SSI program managers and coordinators to, among other monitoring activities, evaluate a portion of records marked as containing SSI.
- Agencies may also utilize audits of the identification and use of SSI. TSA is in the process of conducting such an audit.
- The SSI Office reviews information in response to requests to release SSI, regardless of the agency that originally identified the information as SSI.

The aspects of the SSI internal controls for monitoring activities that we evaluated are consistent with internal control standards for the federal government.

32

GAO

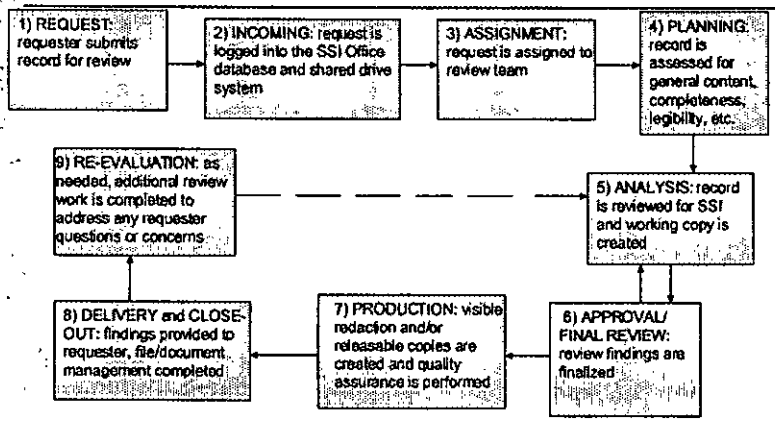
Attachment #1–Categories of SSI as Established by TSA at 49 C.F.R. § 1520.5(b)

1. Security program and contingency plans;
2. security directives;
3. information circulars;
4. performance specifications;
5. vulnerability assessments;
6. security inspections or investigative information;
7. threat information;
8. security measures;
9. security screening information;
10. security training materials;
11. identifying information of certain transportation security personnel;
12. critical aviation or maritime infrastructure asset information;
13. systems security information;
14. confidential business information;
15. research and development; and
16. other information determined to be SSI in accordance with the statute (as designated in writing by the DHS Secretary, the TSA Administrator, or the Director of the SSI Office)

33

GAO

Attachment #2–SSI Office's Nine-Step Process for Reviewing Document Requests[15]



[15] GAO analysis of information provided by the TSA SSI Office.

34

(440627)

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

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

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

Public Affairs

Chuck Young, Acting Manager, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

PRINTED ON RECYCLED PAPER

EXHIBIT G

U.S. Department of Homeland Security
601 South 12th, Street
Arlington, VA 22202

Transportation Security Administration

March 26, 2007

Mr. Bill Heileman
General Director
Resource Protection Solutions
BNSF Railway Company
6651 Burlington Boulevard
Fort Worth, Texas 76131

Dear Mr.Heileman:

This letter is to confirm that you are meeting with Transportation Security Administration (TSA) representatives on April 4-5, 2007, to discuss BNSF Railway Company's (BNSF) security plan and the process and procedures used in the execution of this plan.

As discussed, TSA is resuming the Corporate Security Review (CSR) Program to evaluate the progress of the freight rail industry in the implementation of their security programs. Since the inception of the TSA Freight Rail Division in 2002, TSA has been working closely with the carriers to determine the level of security throughout the industry. In coordination with freight rail stakeholders, TSA has issued guidelines and recommended protective measures to enhance freight rail security, particularly the protection of toxic inhalation hazardous materials shipped by rail. The CSRs will not only assess how your company's security plan addresses hazardous materials, but will also review and assess security improvements in these areas:

- Communication of Security Plan
- Audit of Security Plan
- Cyber Security
- Protection of Critical Assets
- Security Training
- Personnel Security

This CSR will provide BNSF an opportunity to update TSA on system-wide improvements as they relate to the implementation of BNSF's security plan.

BNSF's participation in this review is voluntary. TSA will designate information provided in support of this CSR as Sensitive Security Information (SSI) under 49 CFR Part 1520. This information is considered as part of a vulnerability assessment "created,

held" and "approved by the ... DHS." 49 CFR § 1520.5 (a) (5). Additionally, the regulation extends SSI protection to all documents submitted, generated, and resulting from this CSR. Documents designated as SSI are exempt from release under the Freedom of Information Act. 49 CFR § 1520.15. When submitting documents in support of the CSR to TSA, the following statement shall be affixed to the front cover/title page of the document, and placed at the foot of each page:

"SENSITIVE SECURITY INFORMATION/FOR OFFICIAL USE ONLY
***WARNING:* This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**

In preparation for our visit, we ask that you have the following items available for us for our scheduled visit.

1. Organizational chart
2. Copy of the security plan
3. Maps or schematics of rail lines
4. List of critical infrastructure
5. Security awareness training curriculum
6. Operational protective measures enacted during the Homeland Security Alert System

Prior to our on-site review, we will be sending you the following items: Agenda to include CSR topics for discussion, TSA CSR Presentation, and SSI guidance.

Mr. James Dunn, Ms. Emilie Guerin, and Ms. Amanda Mulhern will be the representatives attending the review. I look forward to meeting with you. If you have any questions or need additional information, please do not hesitate to contact me at 571-227-1246.

Sincerely yours,

Emilie Guerin
Branch Chief, Stakeholder Relations
TSA, Freight Rail Security

INTERNATIONAL BROTHERHOOD OF TEAMSTERS

JAMES P. HOFFA
General President

25 Louisiana Avenue, NW
Washington, DC 20001

C. THOMAS KEEGEL
General Secretary-Treasurer

202.624.6800
www.teamster.org

RECEIVED
2008 FEB 12 PM 3:31
OFFICE OF CHIEF COUNSEL
CORPORATION FINANCE

February 11, 2008

U.S. Securities and Exchange Commission
Office of the Chief Counsel
Division of Corporation Finance
100 F Street, NE
Washington, D.C. 20549-1090

Re: Appeal of Burlington Northern Santa Fe Corporation from no-action determination regarding shareholder proposal submitted by the Teamsters General Fund

Dear Sir or Madam:

By letter dated January 25, 2008 (the "Appeal"), Burlington Northern Santa Fe Corporation ("BNSF" or "Company") asked that the Division of Corporation Finance (the "Staff") reconsider the position taken in its letter dated December 27, 2007, which denied BNSF's request for no action with respect to a shareholder proposal (the "Proposal") submitted to BNSF by the Teamsters General Fund (the "Fund") for inclusion in BNSF's 2008 proxy materials.

The Proposal requests that the Company make available, omitting proprietary information and at reasonable cost, in BNSF's annual proxy statement, by the 2009 annual meeting, information relevant to the Company's efforts to safeguard the security of its operations arising in the event of a terrorist attack and/or other homeland security incidents.

In letters dated November 19, 2007, (the "No-Action Request") and December 7, 2007 ("BNSF's Response"), BNSF argued that the Proposal was excludable under Rule 14a-8(i)(7) and Rule 14a-8(i)(3). In its letter dated December 27, 2007, the Staff responded that it does not believe that BNSF may omit the proposal in reliance on either rule.

In the Appeal, BNSF now claims that it has "identified additional arguments and lines of analysis that were not addressed by the No-Action Request or BNSF's Response" and urges the Staff to confirm that it will not recommend any enforcement action if BNSF excludes the Proposal from its 2008 proxy materials.

We believe that BNSF should not be permitted to exclude the Proposal from its 2008 proxy materials pursuant to Rule 14a-8 for the reasons set forth below, and for the reasons set forth in the Fund's letter dated December 7, 2007 (the "Fund's Response"), which responded to the No-Action Request. We will avoid significant repetition of the contents of the Fund's Response, on which we continue to rely as a basis for denial of BNSF's No-Action Request. We respectfully request that this letter be read in conjunction with the Fund's Response.

BASES FOR INCLUSION

I. The Proposal Does Not Seek Disclosure of Sensitive Security Information and Would Not Cause BNSF to Violate Federal Law

In Section I of the Appeal, BNSF argues that it may exclude the Proposal in reliance on Rule 14a-8(i)(2) because the Proposal, if implemented, "would cause BNSF to violate federal law." Specifically, BNSF claims that the Proposal "makes a very broad request for information," and that "the information in BNSF's possession that meets this request, however, has been deemed 'Sensitive Security Information,' the disclosure of which would violate a variety of federal regulations and statutes to which BNSF is subject."

BNSF goes on to detail certain federal regulations pertaining to "Sensitive Security Information," (SSI) noting that the Transportation Security Administration (TSA) has confirmed that BNSF's security plan is SSI. It also explains that "Even without a specific SSI determination by TSA, certain categories of information are identified by regulation as SSI, and BNSF would be prohibited from disclosing SSI, including but not limited to security plans and procedures, contingency plans, and vulnerability assessments." BNSF further contends that implementation of the Proposal would cause BNSF to violate various other federal regulations that pertain to the transportation of hazardous materials.

The Fund absolutely respects BNSF's obligations under federal law, and the Proposal is not meant to compel the disclosure of SSI or other related information that would violate federal regulations. Furthermore, the Fund does not seek any disclosures that would compromise the security of the railroad industry or—as BNSF puts it—provide "terrorists with a blueprint to BNSF's most sensitive security

procedures." On the contrary, as both long-term shareholders of BNSF and citizens of the communities in which BNSF operates, we have a strong interest in BNSF adhering to federal law and safeguarding SSI, just as we have a strong interest in BNSF providing information on what the Company is doing to minimize or eliminate risks to the environment and the public posed by BNSF's vulnerability to a terrorist attack on its rail system.

In specifying that the requested disclosures omit proprietary information, the Fund believed that the Proposal, as originally submitted, excluded information from the requested disclosure which would violate federal regulations. However, BNSF explains that it understands "proprietary information" to refer only to confidential business information that is developed and exploited for commercial gain.

Therefore, if the Staff deems it necessary, the Fund is prepared to add a clause to the resolved statement to clarify that it seeks only disclosures that BNSF is able to provide under federal law and regulations. More specifically, the Fund is willing to edit the resolved clause to state: "That the shareholders of Burlington Northern Santa Fe Corporation ('BNSF' or 'Company') hereby request that the Board of Directors make available, omitting proprietary information *and information for which disclosure would violate federal regulations*, at reasonable cost, in BNSF's annual proxy statement, by the 2009 annual meeting, information relevant to the Company's efforts to safeguard the security of their operations arising from a terrorist attack and/or other homeland security incidents." (Suggested change in italics.) By adding this clause, we believe the Fund could make a minor edit that would clarify that the Proposal seeks only disclosures which would not violate the strictures of TSA regulations.

In this vein, we believe that there is a variety of rail security efforts that the Company can disclose without violating federal law, and we further believe that disclosure of these efforts would provide shareholders with important information on how the Company is operating in relation to a significant social policy issue. For example, the Department of Homeland Security (DHS) explains on its website a number of initiatives that it is undertaking to enhance rail security. In the section titled "Securing Our Nation's Rail Systems," DHS states that it is taking the following rail security measures regarding training teams and deploying manpower and resources to the field; developing, testing, and activating new technologies; and conducting site assessments to improve the ability of state, local, and private sector partners to strengthen security:

- "Providing Mass Transit Inspectors to Our Largest Rail Systems: Through the Surface Transportation Security Inspection Program (STSI), TSA has deployed 100 inspectors, assigned to 18 field offices across the country, to provide support to our nation's largest mass transit systems. These officials perform frequent inspections of key facilities including stations and terminals for suspicious or unattended items, among other potential threats. Inspectors are actively engaged in performing Security Analysis and Action Programs (SAAP), which constitutes a systematic examination of a stakeholder's operations to assess compliance with security requirements, identifies security gaps, develop best practices, and gather information on the system, its operations, and its security resources and initiatives."

- "Providing Training to Local Authorities: TSA has funded eight Land Transportation Anti-Terrorism Programs (LTATP) conducted by the Federal Law Enforcement Training Center (FLETC) for FY 2006. The LTATP program provides training to local authorities in protecting land transportation infrastructure including rail, light rail, mass transit, and bus operations. Attendees at this training consist primarily of local law enforcement and transit system security directors and security coordinators. Thus far in FY 2006, 180 of these officials have completed the LTATP."

- "Developing New Surveillance Camera Systems: TSA and S&T are leading a project to develop software designed to detect human anomalous behavior for use with surveillance/CCTV camera systems."

- "Completing Thousands of Criticality Assessments: TSA has completed over 2,600 criticality assessments for systems across the nation, including 848 for rail systems and 1,778 for mass transit systems. 50 Site Assistant Visits (SAVs) have been completed across the nation's mass transit, bus, tunnel, and terminal systems. 132 Buffer Zone Protection Plans (BZPPs) have also been completed."

- "Performing Rail Corridor Assessments For Hazardous Materials: In High Threat Urban Areas (HTUA) rail corridors, DHS components are conducting assessments where hazardous materials may pose significant risks. In these processes, DHS cooperates closely with the Federal Railroad Administration, the Pipeline and Hazardous Materials Safety Administration, and relevant railroads and private entities."[1]

[1] "Securing Our Nation's Rail Systems", Department of Homeland Security (available at: http://www.dhs.gov/xprevprot/programs/editorial_0895.shtm)

These are but a sample of the rail security efforts detailed by DHS on its website. Without revealing security sensitive information, DHS's disclosures provide insight into the range of rail security work performed by the organization and offer important details on the breadth of the organization's efforts and the various security factors taken into consideration (that is, working with local security and law officials, security inspections of key facilities, criticality assessments in high threat urban areas, developing new surveillance and detection technology, etc.).

While we recognize that DHS is a different entity than BNSF and presumably has different regulations governing its disclosures, we believe that DHS's disclosures exemplify the kind of disclosures and the level of detail that BNSF can easily provide to its shareholders without compromising its security or violating federal regulations.

II. The Proposal Focuses on Rail Security—a Significant Social Policy Issue—and the Company's Operations Related Thereto, Precluding Application of the Ordinary Business Exclusion

A. Recent SEC Interpretations and Staff Guidance Confirm That a Proposal's Focus is Critical in Determining Whether It is Appropriate for a Shareholder Vote

BNSF states that "when examining whether a proposal may be excluded under Rule 14a-8(i)(7), the first step is to determine whether the proposal raises any significant social policy issue. . . .If the proposal does raise a significant social policy issue, it is not the end of the analysis." The Company claims that "the Staff has concurred with the exclusion of shareholder proposals that raise a significant social policy issue when other aspects of the report or action sought in the proposals implicate a Company's ordinary business." It further states: "We believe that most Rule 14a-8(i)(7) determinations considered by the Staff do not revolve around whether the subject matter of a proposal has raised a significant social policy issue, but instead depend on whether the specific actions sought by the proposal or some other aspect of the proposal involve day-to-day business matters."

While we agree that a determination as to whether a proposal raises any significant social policy issue is not the end of the analysis, we argue that the next step is not a determination as to "whether the specific actions sought by the proposal or some other aspect of the proposal *involve* day-to-day business matters" (emphasis added). We believe that the 1998 Release and Staff Legal Bulletin 14C make clear that the next step is a determination as to whether the proposal *focuses* on day-to-day

business matters and how the social policy issue impacts the company, or whether it *focuses* on the applicable social policy issue and how the Company's related efforts may impact the environment or the public's health.

According to the Exchange Act Release No. 40018 ("1998 Release"), there are two considerations used in determining whether a proposal is excludable under the ordinary business exemption:

> The first-relates to the subject matter of the proposal. Certain tasks are so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight. Examples include the management of the workforce, such as the hiring, promotion, and termination of employees, decisions on production quality and quantity, and the retention of suppliers. However, proposals relating to such matters but focusing on sufficiently significant social policy issues (e.g., significant discrimination matters) generally would not be considered to be excludable, because the proposals would transcend the day-to-day business matters and raise policy issues so significant that it would be appropriate for a shareholder vote. The second consideration relates to the degree to which the proposal seeks to "micro-manage" the company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment.[2]

By stating that a proposal relating to "[ordinary business] matters *but* focusing on sufficiently significant social policy issues" is not excludable (emphasis added), the 1998 Release makes clear that a subject's status as a significant social policy issue trumps its characterization as an ordinary business matter. (Therefore, although BNSF argues that homeland security concerns "require the Company's daily attention," the fact that rail security is a significant social policy issue makes the Proposal appropriate for a shareholder vote.)

By stating that the second consideration "relates *to the degree to which* the proposal seeks to 'micro-manage' the company by probing *too deeply* into matters of a complex nature" (emphasis added), the 1998 Release makes clear that in evaluating proposals under Rule 14a-8(i)(7), a central consideration must be whether the proposal delves too deeply into the day-to-day management of the company—not whether it involves or touches on the day-to-day management of the company at all.

---

[2] Exchange Act Release No. 40018 (May 21, 1998)

Staff Legal Bulletin 14C further distinguishes that the focus of the proposal is crucial in determining the applicability of Rule 14a-8(i)(7). The Bulletin states:

> Each year, we are asked to analyze numerous proposals that make reference to environmental or public health issues. In determining whether the focus of these proposals is a significant social policy issue, we consider both the proposal and the supporting statement as a whole. To the extent that a proposal and supporting statement focus on the company engaging in an internal assessment of the risks or liabilities that the company faces as a result of its operations that may adversely affect the environment or the public's health, we concur with the Company's view that there is a basis for it to exclude the proposal under rule 14a-8(i)(7) as relating to an evaluation of risk. To the extent that a proposal and supporting statement focus on the company minimizing or eliminating operations that may adversely affect the environment or the public's health, we do not concur with the Company's view that there is a basis for it to exclude the proposal under rule 14a-8(i)(7).

Together, we believe these authorities underscore that proposals focusing on significant social policy issues may involve day-to-day business matters so long as the focus remains on the policy issue and the Company's related actions. For reasons that we will elucidate below, the Proposal indeed focuses on rail security and the Company's actions regarding rail security—actions that directly affect the health of the environment and the general public.

B. The Proposal Focuses on the Company's Efforts Regarding Rail Security, Not its Overall Safety and Emergency Response Programs

BNSF argues that "the Proposal's reference to 'homeland security incidents' encompasses a wide range of security considerations separate from and in addition to a potential 'terrorist attack' that BNSF must address every day." In fact, BNSF argues that—because the Federal Emergency Management Agency (FEMA) and the United States Customs Services and the Animal and Plant Inspection Service are among the responsibilities transferred to the Department of Homeland Security—'other homeland security incidents' could refer to earthquakes, floods, hurricanes, landslides, thunderstorms, tornados, wild fires and winter storms. Therefore, according to BNSF: "Regardless of whether the Company's efforts to safeguard its assets from a potential terrorist attack transcends the Company's ordinary business, the Proposal clearly also requests that the Company report on actions it has taken to safeguard the security of its operations from incidents and threats that are routine and that have been faced by railroads for more than 150 years."

We believe that this argument demonstrates BNSF's deliberate failure to acknowledge the Proposal's clear focus on the issue of rail security as related to potential terrorist attacks. In Staff Legal Bulletin 14C, the Staff explains that in determining whether the focus of the proposals is a significant social policy issue it considers "both the proposal and the supporting statement as a whole."[3] The resolved clause requests a report on the Company's "efforts to safeguard the security of their operations arising from a terrorist attack and/or other homeland security incidents." The Proposal's supporting statement includes:

- a statement regarding the critical need for shareholders to be able "to evaluate the steps the Company has taken to *minimize risks to the public arising from a terrorist attack* or other homeland security incident;"
- a discussion of the train bombings in London and Madrid—highly coordinated terrorist attacks that "highlight *the vulnerability of railways as prime targets for terrorist attacks*;"
- references to "Securing and Protecting America's Rail System: U.S. Railroads and Opportunities for Terrorist Threats"—a Penn State University report that exposes "*glaring holes in rail security and therefore, opportunities for terrorism* in the U.S. system" and that uncovers "*the need for an increase in terrorism preparedness training for rail workers in order to improve rail security and protect the public*;" and,
- reports that BNSF rail workers have stated their belief that the Company "has failed to implement significant security improvements *to deter or respond to a terrorist attack on the U.S. rail network, which could potentially devastate communities in our country* and destroy our Company."
  (Emphasis added)

Given the full context of the proposal and the supporting statement, we believe that the Proposal leaves no doubt as to its focus on BNSF's efforts regarding rail security as related to potential terrorist attacks—efforts that are inextricably linked to the health of the environment and the general public. Therefore, while the Proposal references 'other homeland security incidents,' we believe that the full context of the Proposal makes clear that the homeland security incidents to which the Proposal refers are those related to terrorist attacks and not earthquakes, floods, hurricanes, landslides, thunderstorms, tornados, wild fires and winter storms.

Furthermore, on DHS's website, in explaining the efforts involved regarding rail security, DHS clearly uses the context of terrorism to frame its efforts. DHS

[3] Staff Legal Bulletin 14C (June 28, 2005).

introduces the subject by stating:

> Since the terrorist attacks of September 11, 2001, the 7/7 London subway bombings, and the Madrid rail bombings, the Department of Homeland Security has taken several steps to manage risk and strengthen our nation's rail and transit systems by: Providing funding to state and local partners; Training and deploying manpower and assets for high risk areas; Developing and testing new technologies, and; Performing security assessments of systems across the country.[4]

As already discussed in this letter, DHS goes on to give extensive detail regarding its efforts related to rail security—all of which address potential terrorist attacks. It discusses at length the various teams DHS is training (including law enforcement personnel, canine teams, and inspection personnel) to deter and protect against potential terrorist actions; various new screening techniques and technologies which could be deployed quickly to systems facing a specific terrorist threat; pilot technologies and studies underway in major American cities; and criticality assessments that have been conducted by the Transportation Security Administration (TSA) to determine best practices, weaknesses, and vulnerabilities across the nation.[5] Notably, the discussion lacks any references to earthquakes, landslides, winter storms, et al.

C. The Proposal Seeks an Evaluation and Report on Actions the Company is Taking Regarding Rail Security, Actions Which Directly Affect the Health of the Environment and the General Public

BNSF states that "the fact that even one prong of a proposal may invoke a significant policy issue does not automatically mean that prong does not involve ordinary business matters." As an example, it cites *General Motors Corp.* (avail. Apr. 4, 2007), in which the Staff found that a proposal requested that the board adopt an executive compensation program that tracks progress in improving the fuel economy of GM vehicles was excludable under Rule 14a8(i)(7) because "the thrust and focus of the proposal is on ordinary business matters." BNSF goes on to reference Staff Legal Bulletin 14C, which sets forth the standards for evaluating whether proposals concern significant social policy issues or ordinary business matters.

While we acknowledge that implicating a significant social policy does not automatically preclude application of the ordinary business exemption, we believe

[4] Department of Homeland Security, http://www.dhs.gov/xprevprot/programs/
[5] Department of Homeland Security, http://www.dhs.gov/xprevprot/programs/editorial_0895.shtm

that Staff Legal Bulletin 14C makes clear that *focusing* on a significant social policy issue does preclude application of the ordinary business exclusion. Here again, we think the focus of the proposal is critical, and we believe the Proposal's focus is clearly on the issue of rail security and BNSF's related efforts.

Using the language of Staff Legal Bulletin 14C, the Proposal does not focus on an evaluation of the risks or liabilities facing BNSF in the event of a terrorist attack but rather focuses on BNSF's efforts to minimize or eliminate risks to the environment and the public posed by the Company's vulnerability to a terrorist attack on its rails system. This vulnerability is defined by BNSF's rail security efforts, which qualify as BNSF operations that the company is capable of altering to avoid adversely affecting the environment or the public's health.

BNSF's argument that the Proposal "does not request a report on 'minimizing or eliminating operations that may adversely affect the environment or the public's health,'" reflects BNSF's failure to understand the inextricable tie between rail security and the health and safety of the environment and the general public. As argued in the Fund's Response, any efforts that BNSF makes, or fails to make, to safeguard the security of its operations from a terrorist attack and/or other homeland security incident will directly affect the environment and the public's health. We, therefore, believe the Proposal is inherently about the Company's efforts to minimize or eliminate threats to the environment and the public's safety.

BNSF argues that "shareholder proposals need not explicitly request an 'evaluation of risk' to be excludable on that basis under Rule 14a-8(i)(7)." In this vein, the company argues that the Proposal is similar to other proposals involving social policy issues that the Staff concurred could be excluded under Rule 14a-8(i)(7) as relating to "evaluation of risk," including *Pulte Homes Inc.* (Mar. 1, 2007), *Wells Fargo & Co.* (Feb. 16, 2006), *The Dow Chemical Co.* (Feb. 23, 2005), and *American International Group, Inc.* (Feb. 19, 2004).

In each of these cases, we believe the proposals are not applicable to our Proposal because they are unlike our Proposal in focus. More specifically, we believe that the proposals at these companies focused on the companies engaging in internal assessments of risk and liabilities related to outside issues that could affect the environment or the public's health. For example, the *Pulte Homes Inc.* proposal requested that the company assess its response to regulatory, competitive, and public pressure to increase energy efficiency. The *Wells Fargo & Co.* proposal requested that the board evaluate effects of global climate change on the Company's business. *The Dow Chemical Co.,* proposal concerned the impacts that outstanding Bhopal issue may pose on Dow Chemical. The *American International Group, Inc.*

proposal asked for a report on the economic effects of major health pandemics on the Company's business strategy. Unlike these proposals, our Proposal does not focus on the Company's ordinary business.

Furthermore, the Staff recently rejected arguments much like the ones BNSF advances here. In addition to the determination that BNSF is appealing, the Staff also concluded that other proposals substantially similar to the Proposal could not be excluded on ordinary business grounds. See *Kansas City Southern* (avail. Jan. 9, 2008) and *Norfolk Southern Corporation* (avail. Jan. 14, 2008). We do not believe that BNSF's arguments regarding an evaluation of risk raise any new arguments beyond what the Staff has already considered in these cases.

BNSF also argues that it has identified "a number of SEC staff no-action precedents in which the respective proposals could be read to implicate broad social policy issues, but because of the nature of the companies' businesses, were held to pertain to ordinary business matters that the companies dealt with on a daily basis." For example, it notes *Verizon Communications Inc.* (avail. Feb. 22, 2007), *Newmont Mining Corp.* (avail. Feb. 5, 2005), and *Wal-Mart Stores, Inc.* (avail. Mar. 24, 2006), *Peregrine Pharmaceuticals Inc.* (avail. July 31, 2007), and *General Election Co.* (avail. Feb. 10, 2000). We believe that in each of these cases—as with the cases noted above—the proposals are unlike our Proposal in focus; they fail to focus on social policy issues that transcend ordinary business and instead focus on the companies' ordinary business.

We think that *Exxon Mobil Corp.* (avail. March 18, 2005)—which is cited in Staff Legal Bulletin 14C as an example of a proposal that is not excludable—is a strong example of a proposal that involved the nature of the Company's business but focused on a significant social policy issue. The proposal requested a report "on the potential environmental damage that would result from the company drilling for oil and gas in protected areas." Although drilling for oil and gas is certainly part of Exxon Mobil's ordinary business, the proposal focused on the Company's operations in protected areas—extraordinary operations that could adversely affect the environment and that play a significant role in a social policy issue. Similarly, while certain safety and security measures are a part of BNSF's ordinary business, the Proposal focuses on the Company's rail security efforts related to the threat of terrorism—extraordinary efforts that could adversely affect the general public and the environment and that play a significant role in a social policy issue.

Additionally, *Exxon Mobil Corp.*, also serves as an example of a proposal that touches on risk, but remains focused on a significant social policy issue. For example, the supporting statement of the proposal at Exxon Mobil said: "we

strongly believe, in addition to recognizing the issue, there is a need to study and disclose the impact on our Company's value from decisions to do business in protected and sensitive areas. This would allow shareholders to assess the risks created by the Company's activity in these areas as well as the Company's strategy for managing these risks." (Emphasis added) The proposal also stated: "preserving sensitive ecosystems will enhance our Company's image and reputation with consumers, elected officials, current and potential employees, and investors;" "some of our major competitors have already enacted such a policy;" and "Vote YES for this proposal, which will improve our Company's reputation. . ." (Emphasis added) Although BNSF argues that "the Proposal implicates an assessment of the risks faced by BNSF's operations," we believe that—like the proposal at Exxon Mobil—our Proposal is focused on a significant social policy issue and the Company's related actions.

III. BNSF Has Not Substantially Implemented the Proposal

BNSF argues that it has substantially complied with the Proposal, claiming that it already provides information that is responsive to the Proposal on its website "and through other media." It then goes on to detail "a number of measures that BNSF has taken to ensure the safety of its trains and the cargo that it transports," which are described on the Company's website.

While some of these measures do indeed include measures that are pertinent to terrorist attacks, BNSF fails to provide on its website—or through other media—centralized, comprehensive information on the Company's overall efforts to safeguard its operations from a terrorist attack or other related homeland security incident. To be clear, by "centralized" and "comprehensive," the Fund does not mean that it seeks a full exposé on the specific and security-sensitive features of BNSF's security plans. Rather, the Fund seeks a one-stop set of disclosures that lay out BNSF's overall rail security efforts, addressing a variety of factors of concern to the general public and providing enough detail to provide shareholders and the general public with a clear picture of how BNSF is addressing an issue that directly affects them. Though BNSF accuses the Proposal of being vague, we believe that the Proposal unambiguously requests direct and accessible information regarding the Company's rail security efforts.

In the Appeal, BNSF provides a set of directions to navigate its website, and these directions themselves demonstrate the failure of the company to make rail security information clear and accessible to shareholders. For example, the Company notes that under the "Customer Tools" tab, there is a section called "Resource Protection," wherein the company provides links and information

detailing "a number of measures that BNSF has taken to ensure the safety of its trains and the cargo that it transports." First of all, we do not think that this set of directions reflects intuitive navigation, given that "Customer Tools" does not indicate a section that would provide information of importance to general stakeholders. Secondly, in the "Resource Protection" section, although there is a "Homeland Security" link, that page does not provide a comprehensive snapshot of the Company's efforts to safeguard its operations from a terrorist attack. What the "Homeland Security" page does say is:

> The Resource Protection Solutions Team is composed of the Police, Homeland Security, Training and Development Solutions, Load, Ride, and Claims Solutions, Special Investigations, and Administrative Solutions Teams. These teams are responsible for the protection of all BNSF resources covering 33,000 route miles in 28 states and two Canadian provinces, and more than 38,000 BNSF employees. Physical facilities include hundreds of buildings and more than 5,000 locomotives and 190,000 freight cars. Daily freight and passenger train starts average 1,200, and 232, respectively. Click here to learn more.[6]

In clicking through "to learn more," there is a two page brochure discussing the Resource Protection Solutions Team. This document boasts that "Team members are from different racial, ethnic and cultural backgrounds. They celebrate their differences and similarities." The brochure also explains that "Investigations are conducted in areas of larceny, forgery, narcotics, homicide, robbery, burglary, auto theft and a variety of special assignments. Officers may specialize in training, canine, firearms, crime prevention and other areas."[7]

While the Resource Protection Solutions Team is charged with a variety of important responsibilities, and while the brochure does indeed provide stakeholders with information on the Company's general efforts to abate crime, this overview of this Team and the linked brochure provide stakeholders with zero information on BNSF's rail security efforts related to terrorism. In fact, the words "terrorist" or "terrorism" are nowhere on the "Homeland Security" page or the linked brochure.

Underneath the overview of the Resource Protections Solutions Team, BNSF lists the following links: Barrier Seal Requirements, Contacts, Cable Protection, CPS Article Directory, Citizens for Rail Security (CRS), C-TPAT Certification, e-

---

[6] Burlington Northern Santa Fe Corporation, http://www.bnsf.com/tools/resourceprotection/homeland_security.html

[7] Burlington Northern Santa Fe Corporation, General Brochure on the Resource Protection Solutions Team, http://www.bnsf.com/tools/resourceprotection/pdf/general_brochure.pdf

RAILSAFE Program, On Guard Program, TIPS Center, Resource Operations Communications Center (ROCC), Seal Integrity & STAT Programs, and Trespasser Abatement. Of these 12 links, we think that only four have names that would indicate a possible relation to rail security efforts regarding terrorist attacks. Namely, we think that Citizens for Rail Security, e-RAILSAFE Program, On Guard Program, and Trespasser Abatement are the only link titles that indicate some possible relation to safeguards against terrorist attacks, and we feel that even this statement is generous.

While these links do indeed provide some limited information on rail security efforts the company is making (as explained by BNSF in the Appeal), shareholders visiting the website do not have access to a clear description of the Company's overall efforts regarding the threat of terrorism or a related homeland security incident, do not have a clear path for obtaining the scattered information that is provided, and therefore cannot get a clear picture of BNSF's efforts in this area. In the Appeal, BNSF states the programs listed on the website "all relate to security measures that BNSF has taken to protect its railroad from all kinds of safety risk, including terrorist threats." Shareholders would have to navigate through and read all of these sections to try to piece together the details regarding BNSF's terrorist-related efforts. BNSF boasts that "when one runs a search for 'Homeland Security,' the function yields over 40 results, most of which are pertinent to the Proponent's information request." We believe that BNSF shareholders should not have to read through 40 different links to try to piece together the scattered information about the Company's efforts in this area, and even if shareholders did undertake this task, the result would not be comprehensive or adequate.

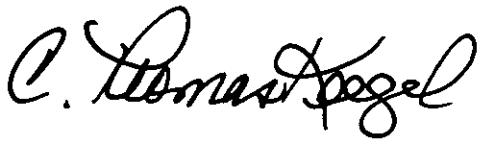
BNSF claims that it "strives to inform its shareholders with regard to these matters to the extent that it can do so without violating the law or jeopardizing the safety of its railroad." We believe that the Company's failure to provide on its website a clear, comprehensive and centralized discussion of its efforts to safeguard the security of its operations arising from a terrorist attack or related homeland security incident, along with the Company's extended fight to keep the Proposal out of its 2008 proxy materials, demonstrates that BNSF in no way strives to inform its shareholders of its efforts in this area, and fails to recognize the importance of transparency regarding company operations that could have catastrophic effects on the general public and the environment.

IV. Conclusion

For the foregoing reasons, the Fund respectfully requests that the Division reaffirm the position taken in its letter dated December 27, 2007.

The Fund is pleased to be of assistance to the Staff on this matter. If you have any questions or need additional information, please do not hesitate to contact Jamie Carroll, IBT Program Manager, at (202) 624-8990.

Sincerely,



C. Thomas Keegel
General Secretary-Treasurer

CTK/jc

cc: Roger Nober, Burlington Northern Santa Fe Corporation
Jeffrey Williams, Burlington Northern Santa Fe Corporation
William V. Fogg, Cravath, Swaine & Moore LLP

CRAVATH, SWAINE & MOORE LLP

WORLDWIDE PLAZA
825 EIGHTH AVENUE
NEW YORK, NY 10019-7475

TELEPHONE: (212) 474-1000
FACSIMILE: (212) 474-3700

CITYPOINT
ONE ROPEMAKER STREET
LONDON EC2Y 9HR
TELEPHONE: 44-20-7453-1000
FACSIMILE: 44-20-7860-1150

WRITER'S DIRECT DIAL NUMBER

212-474-1131

ROBERT D. JOFFE
ALLEN FINKELSON
RONALD S. ROLFE
PAUL C. SAUNDERS
DOUGLAS D. BROADWATER
ALAN C. STEPHENSON
MAX R. SHULMAN
STUART W. GOLD
JOHN E. BEERBOWER
EVAN R. CHESLER
MICHAEL L. SCHLER
RICHARD LEVIN
KRIS F. HEINZELMAN
B. ROBBINS KIESSLING
ROGER D. TURNER
PHILIP A. GELSTON
RORY O. MILLSON
FRANCIS P. BARRON
RICHARD W. CLARY
WILLIAM P. ROGERS, JR.
JAMES D. COOPER
STEPHEN L. GORDON
DANIEL L. MOSLEY
GREGORY M. SHAW
PETER S. WILSON

JAMES C. VARDELL, II
ROBERT H. BARON
KEVIN J. GREHAN
STEPHEN S. MADSEN
C. ALLEN PARKER
MARC S. ROSENBERG
SUSAN WEBSTER
TIMOTHY G. MASSAD
DAVID MERCADO
ROWAN D. WILSON
PETER T. BARBUR
SANDRA C. GOLDSTEIN
PAUL MICHALSKI
THOMAS G. RAFFERTY
MICHAEL S. GOLDMAN
RICHARD HALL
ELIZABETH L. GRAYER
JULIE A. NORTH
ANDREW W. NEEDHAM
STEPHEN L. BURNS
KATHERINE B. FORREST
KEITH R. HUMMEL
DANIEL SLIFKIN
JEFFREY A. SMITH
ROBERT I. TOWNSEND, II

WILLIAM J. WHELAN, III
SCOTT A. BARSHAY
PHILIP J. BOECKMAN
ROGER G. BROOKS
WILLIAM V. FOGG
FAIZA J. SAEED
RICHARD J. STARK
THOMAS E. DUNN
JULIE SPELLMAN SWEET
RONALD CAMI
MARK I. GREENE
SARKIS JEBEJIAN
JAMES C. WOOLERY
DAVID R. MARRIOTT
MICHAEL A. PASKIN
ANDREW J. PITTS
MICHAEL T. REYNOLDS
ANTONY L. RYAN
GEORGE E. ZOBITZ
GEORGE A. STEPHANAKIS
DARIN P. MCATEE
GARY A. BORNSTEIN
TIMOTHY G. CAMERON
KARIN A. DEMASI
LIZABETHANN R. EISEN

DAVID S. FINKELSTEIN
DAVID GREENWALD
RACHEL G. SKAISTIS
PAUL H. ZUMBRO
JOEL F. HEROLD
ERIC W. HILFERS
GEORGE F. SCHOEN
ERIK R. TAVZEL
CRAIG F. ARCELLA
TEENA-ANN V. SANKOORIKAL
ANDREW R. THOMPSON
DAMIEN R. ZOUBEK
LAUREN ANGELILLI
TATIANA LAPUSHCHIK
ERIC L. SCHIELE

SPECIAL COUNSEL
SAMUEL C. BUTLER
GEORGE J. GILLESPIE, III

OF COUNSEL
CHRISTINE BESHAR

February 19, 2008

Burlington Northern Santa Fe Corporation - Shareholder Proposal Submitted by the International Brotherhood of Teamsters' General Fund

Ladies and Gentlemen:

This letter is submitted on behalf of Burlington Northern Santa Fe Corporation ("BNSF") to inform the Staff that BNSF hereby formally withdraws its motion for reconsideration, dated January 25, 2008. BNSF is withdrawing its motion for reconsideration in accord with the International Brotherhood of Teamsters General Fund's (the "Proponent") decision to withdraw the proposal it submitted for inclusion in BNSF's 2008 proxy statement and other proxy materials. A letter from the Proponent stating that it has withdrawn the proposal it submitted to BNSF is enclosed.

If the Staff has any questions with respect to the foregoing, please contact me at (212) 474-1131.

Very truly yours,

William V. Fogg

Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F Street, N.E.
Washington, D.C. 20549

Encl.

EMAIL

INTERNATIONAL BROTHERHOOD OF TEAMSTERS

JAMES P. HOFFA
General President

25 Louisiana Avenue, NW
Washington, DC 20001

C. THOMAS KEEGEL
General Secretary-Treasurer

202.624.6800
www.teamster.org

February 19, 2008

BY FACSIMILE: 817.352.7154
BY U.S. Mail

Mr. James H. Gallegos
Vice President and Corporate
General Counsel
Burlington Northern Santa Fe Corporation
2500 Lou Menk Drive
Fort Worth, TX 76131-2828

Dear Mr. Gallegos:

In light of the agreement reached on February 15, 2008, I hereby withdraw the resolution filed on behalf of the Teamsters General Fund to be included in the Company's 2008 Proxy Statement.

If you should have any further questions about the withdrawal of this proposal, please direct them to Jamie Carroll of the Capital Strategies Department at (202) 624-8990.

Sincerely,

Louis Malizia
Assistant Director
Capital Strategies Department

LM/jc

END