**Before**
**The Department of Transportation**
**And**
**The Transportation Security Administration**
**Washington, D.C. 20528**

In the Matter of )
)
) RIN 1652 AA08
PROTECTION
OF SENSITIVE SECURITY INFORMATION )
Docket # TSA 2003-15569

To: Office of the General Counsel

## COMMENTS OF THE COALITION OF JOURNALISTS FOR OPEN GOVERNMENT

The Coalition of Journalists for Open Government is an alliance of journalism-related organizations that came together because of a concern over the increasing secrecy at all levels of government. We believe this diminishing access to public records and meetings, which prevents the citizenry from being fully informed, is detrimental to public policy and is a principal factor in the public's growing distrust of and disengagement from government.

We have reviewed the regulations affecting the Transportation Security Administration, Coast Guard and Department of Transportation (49 CFR 14 and 49 CFR 1520) that went into effect June 17, 2004 and offer the following comments.

The regulations must be more narrowly and specifically drawn. TSA, the Coast Guard and DOT have been given the important, indeed awesome, task of protecting our nation's transportation systems. But in taking on that responsibility, they assume an equal obligation to do no harm to those same systems – to their efficiency, their effectiveness, their integrity or the quality of their governance.

The present and proposed reach of these regulations is vast. They encompass all transportation-related activities of other federal government entities, of state

governments, of thousands of municipalities and regional authorities. They cover all aspects of security from the qualifications of airport screeners or of bus drivers to the safety of chemical storage facilities at seaports. Unfortunately, the language of the regulations, the lack of criteria to be used in determining what information should be protected, and the overbroad delegation of the authority to designate information as Sensitive Security Information are certain to create abuses of good public policy and to deny people their rights as citizens.

Public accountability does not have to be sacrificed for security; in fact, accountability enhances security. That is precisely what is at stake here here.

We are deeply concerned that unrestricted use of the Sensitive Security Information (SSI) designation – a process with no review for efficacy or propriety – will have a seriously adverse impact on traditional citizen and media oversight of the governance of our seaports, airports and transit systems. We can easily see how information that is, or may come to be, in the possession of the TSA, the Coast Guard and the DOT will be hastily designated sensitive security information, with no consideration being given to the broader, non-security consequences of denying that information to the public.

Moreover, the issuance of these regulations creates a new, fourth level of classification without any of the restraints against overindulgence in secrecy that are built into the existing system for safeguarding our nation's most important military, intelligence and foreign policy information.

These regulations will result in vast amounts of information being designated Sensitive Security Information and withheld from the public for unknown lengths of time. There appear to be no limits to the type of information that might be gathered or generated as SSI and then sealed. Local and state officials, bound by non-disclosure agreements, may be forced to deny access to records that state law and local ordinance require be made available to citizens. Information needed by civic activists or organizations to maintain oversight and challenge local officials on their management of public facilities may be withheld, even when the information's relevance to any possible terrorist threat is at best tenuous.

Because there is not just a likelihood but clearly an intent on the part of the TSA and the DOT to use the Sensitive Security Information designation to subsume transportation-related records of many other governmental entities, we believe it is important to remind and to emphasize that much of the information that will be marked SSI is information currently in the public record in the 50 states and the thousands of municipalities affected. Those states have laws and policies that demand transparency. Those laws are in place because open records are essential to citizen oversight and to insuring accountability in the public management of those transportation facilities.

TSA, the Coast Guard and DOT, in moving to withhold or withdraw some or all of these records from the public domain in the name of national security, must recognize the potential consequences of the diminished public oversight that will result. They should re-craft these regulations to minimize the loss of access to information that might be designated COI -- Critical Oversight Information. What is COI? It is, most simply, any information a citizen might use to judge whether his or her public servants are serving well. It is information that speaks to the quality and integrity of their performance as policy makers, managers or employees of our seaports, airports and transit systems. It is budget information and details on revenue and spending. It is information about personnel and their qualifications, training and performance. It is information about the construction and maintenance of new public assets, including the myriad change orders that seem an inevitable feature of the government contract process. It is information about deals with carriers and suppliers and vendors and tenants. It is also information about public convenience and use of the public areas – and about personal safety.

That is a long list. Obviously, much of the information that is Critical Oversight Information has a connection to security. Without restraints built into the TSA/DOT/Coast Guard regulations and without restraint exercised by those given the authority to mark information as SSI, much that is COI could be withheld or withdrawn from public inspection.

We urge TSA/DOT and the Coast Guard to acknowledge this dilemma and to take it into account in modifying the regulations.

One mechanism to resolving the dilemma would be to build in review of information submitted or independently gathered as SSI in order to identify and extract any Critical Oversight Information whose disclosure does not pose a clear and present danger to the security of the particular transportation facility or system.

Another would be for the three agencies to acknowledge in the rewritten regulations that they are taking possession of what is community property – information that legally and properly belongs to the people – and that in doing so they accept a fiduciary responsibility to provide citizen oversight and to act on that information as would a concerned citizen. This might lead to a unique form of whistle-blowing, but if the records reveal information of actionable mismanagement or of breaches of sound public policy, it is a proper outcome.

Where a decision is made to remove information from the public domain and to deny the citizens of the states an opportunity to use that information to hold their local officials accountable, the federal agencies responsible must accept and assume that burden. The agencies become, however inconveniently, a guardian ad litem of the records they keep from the public as SSI. In denying access, they assume an obligation to thoroughly analyze the information kept from the public and to use it wisely on the public's behalf, not only in matters of national security but also by responding to any other public policy problems that may be raised by the information contained in those records. If the information suggests the need for any form of remedial action, it becomes the responsibility of the records guardian to assure that that action is taken.

That is an awesome additional responsibility – but the alternative is to leave a vacuum, something that should be as unacceptable in public policy as it is in the law.

We urge that, as TSA, the Coast Guard and DOT act to insure the security of our nation's transportation system, they recognize the potential collateral damage. We believe this damage can be minimized, perhaps even avoided, through a narrow construction of SSI, a limited authority to designate information as SSI, a thoughtful and thorough review of SSI designations that looks for unintended consequences, an automatic sunsetting, subject to review, and a willingness to act as a trustee for the public when an SSI marker, while fully warranted, nonetheless denies citizens the information needed to act for themselves on non-security matters.

As we move into specific recommendations for changing the interim rules, we also ask that you remember that privacy and proprietary interests are not valid national security concerns. We recognize there is decade-old litigation that might be cited to argue the contrary, but we would note for the record that we do not believe that personal privacy and/or proprietary business interests can reasonably or properly be considered as national security concerns or relevant to transportation security.

We would hope that TSA, the Coast Guard and DOT will not use either of those criteria to deny access to transportation records on national security grounds. If the only reason to consider withholding information is privacy or a proprietary interest, the agencies should review it under the FOIA law and act accordingly. If information meets both a "privacy" and "detrimental to transportation security" test, then class it as SSI under the latter, not the former.

**Who can designate information as SSI**

The regulations appear to indiscriminately delegate the authority to designate SSI within all of DHS and DOT. Rather than restricting this power to thoroughly-trained personnel, the regulations seem to extend the authority to any and all "covered persons" and to do so without giving them criteria or standards upon which to base their judgments.

We have read and reread the published regulations and can find no clear statement as to who within those departments will have the specific authority to determine if a record is of sufficient national security sensitivity to warrant its being withheld from the public by the federal government or as a consequence by state or local officials as well.

Indeed, the Congressional Research Report of June 9 describes Sensitive Security Information as being "born protected," as if records of whatever security weight or importance will be given this special status simply by virtue of being created in the course of security research or because the document is submitted by state or local government or a regional authority or by a private company in response to a broad request for security information.

Section 1520.1 (and 15.1) simply says that the authority may be delegated within the agency. Section 1520.9 seems to give that authority to any "covered person" through

(b)(4) and 1520.13, which direct covered persons to mark as SSI any unmarked SSI in their possession. That can only be done, of course, if they have made a determination that what they have is SSI. Because there is no straightforward designation of who may designate SSI, the cited language seems to grant the authority to anyone within DOT or DHS – including applicants, trainees, interns, volunteers -- and to a wide range of non-government personnel – 12 categories of persons in all.

We also believe that those making SSI designations within TSA, the Coast Guard and DOT should have special training, much as FOIA officers do, because they are being asked to make difficult balancing decisions among competing values. All of us value security, but any security gained from the regulations is of considerably less comfort if it comes with a loss of faith and confidence in our local, state and national governments to safeguard our other values.

We urge TSA, DOT and the Coast Guard, in reviewing and rewriting their regulations, to clearly and emphatically differentiate between those who are empowered to take away the public's right to inspect the records of its government and those who are simply called upon to use that information as part of their responsibility for insuring some aspect of security within our transportation systems. We would also urge that the agencies limit the number of persons who can make those critical decisions to withhold information, and that those given this solemn responsibility be carefully chosen for their broad understanding of public policy and be thoroughly trained not just in national security matters but in broader issues of governance and public accountability.

We believe that this authority to withhold public information is a very special trust that must be granted with the greatest care and discretion within each governmental entity and that it should not be extended beyond the responsible government entity.

Accountability and trust must not become victims in the War on Terror.

**On what basis may information be designated SSI**.

Not long ago, we read that the Department of Homeland Security, the parent agency for TSA and the Coast Guard, was inviting the authors of thriller novels to spend a day brainstorming terrorist plots. The idea was to fantasize the wildest of scenarios, so that defenses could be devised for threats no one had yet imagined. We don't fault the

game playing, but if similar imagination is allowed in reviewing documents for SSI designation, it will exceed the sum of all our fears.

There are no clear standards for what might constitute SSI. The regulations merely spell out the categories of information to be considered for inclusion as SSI. There are no criteria to guide those who must decide which items of information within any one of the categories are appropriate for safeguarding. The only guideline appears to be the statutory adjective, "detrimental," which is repeated in the regulations. Does this mean "in any way" injurious or harmful, or causing "any kind" of damage, as a strict constructionist – or perhaps someone choosing to cover the traces of local mismanagement – might choose to interpret it? Or are there qualifying elements that should be considered by a thoughtful person concerned about how effectively local airport officials are doing their overall job, not just maintaining security?

The regulations at 1520.5(b)(1) provide that any security program or contingency plan "received by" DOT or DHS is automatically SSI. That stands as an open invitation for abuse. We can imagine a potentially controversial security unit reorganization, or staffing level changes, being hidden because the information has been submitted as SSI. We can imagine a contract for emergency medical services let without bid, then shielded from public review by including it with documents submitted as SSI. We can imagine a runway inspection showing vulnerabilities – and shoddy construction work by a no-bid contractor – being shielded as SSI. Overly imaginative scenarios?

Less than three years ago, the Detroit News reported on patronage at the city's airport that had cost taxpayers millions of dollars in no bid contracts. They also reported the new, $225 million runway had failed half of its initial performance tests. The reporters reviewed more than 10,000 documents, most of which the airport administrator tried desperately to keep from them. What if the airport chief had submitted many of these to TSA as part of the information being gathered on security? The administrator might still be in that job. Who would have stood up for the public?

Or we might ask Sen. Charles Grassley if our concerns are exaggerated. A year ago, Des Moines police told the Iowa senator that they couldn't discuss <u>any</u> airport security issues with him because, in accepting federal funds, they had signed a non-disclosure agreement against giving out sensitive information.

Based on recent performance within TSA, and the lack of any guidelines in the regulations, we are not sanguine about the decisions that will be made in designating information “sensitive” and withholding it from the American public. The Washington Post reported last October that many pilots and flight attendants believe TSA is muzzling debate on in flight security initiatives by labeling agency's policies and reports as too sensitive for public conversation or disclosure. Pilot representatives said non-disclosure agreements were being used to gag pilots from criticizing the guns-in-the cockpit policy. Sensitive Security Information was cited when a Minneapolis Star Tribune reporter asked what kinds of harmless items carried by passengers tended to trigger airport screening machines. The reporter thought this information would help the traveling public and security operations because many would stop carrying those items, or put them in checked luggage. A TSA spokesperson said that information couldn’t be disclosed: “We have to be careful what we say about this because we don't want to give a road map to the bad guys." Nor would TSA talk about a number instances when terminals or concourses were closed because of what the public ultimately learned were simple human error. That’s hardly something terrorists can plan for. It’s also something easily corrected so it doesn’t happen again. Just recently, Federal Judge Charles R. Breyer, San Francisco, examined information that was sought in a suit over the “no fly” list. He said much of the information sought was “innocuous” or already in the public record. He concluded that TSA had made “frivolous claims of exemption" in refusing to disclose records requested.

We urge you to rewrite the regulations and set clear criteria as to what is “sensitive” and to also provide for thoughtful internal review before information is placed in this new area of classification called SSI. That review should speak to the actual, not imagined, sensitivity of the information, whether it is, in fact, available elsewhere, and to broader policy questions involving public oversight and accountability in local or state governance. We would also urge that any such information be subject to a FOIA review should such a request be made. Allowing for this added review in no way jeopardizes the safeguarding if such protection was initially warranted; it would help to secure the public’s right to know.

**The Regulations Should Do More to Ensure Accountability**

There are a number of areas where the regulations close off information about security issues at the unnecessary expense of governmental accountability. We believe it is possible to both write and enforce these regulations in a manner that lets local taxpayers and transportation system users know more about local security efforts without jeopardizing their safety. We should never see a repeat of a situation, as happened in Miami, in which a local prosecutor drops charges against a thieving employee because TSA declines to make available information about a security system – a system whose presence would be obvious to even the most poorly trained terrorist. Similarly, we hope it will be possible for local airport officials, without having to seek permission from TSA, to let the traveling public know why a security alert was sounded and a concourse or airport cleared and closed for hours.

Section 1520.5b (6) (ii) delays the public release of any TSA inspection report for one year. There may well be occasions when that period of delay is warranted to assure that the vulnerabilities have been corrected. But it seems arbitrarily long as an every-instance mandate. We urge a modification of the language to provide for release "when the problem has been corrected or after one year, whichever is earlier."

1520.5b (9) (i) includes as information automatically designated as SSI, the selection criteria for screeners and (iv) screener test scores. Keeping this information secret makes it impossible to know whether, in fact, the security being provided meets standards the public believes to be adequate. It asks the public literally to put blind faith in the process. We suggest instead that the standards, and information needed to evaluate whether the screeners meet those criteria, be made public. This would serve to reassure the public, and it would require TSA to set a standard sufficiently high that terrorists would not attempt to breach these checkpoints.

That would be genuine safeguarding, not just the appearance of security.

**Infrastructure Information Should Be Vetted for Security Relevance**

Section 1520.5(b)(12) (ii) allows state or local government agencies to submit lists of infrastructure assets. The lists become SSI. They are "born protected," yet the language of the regulation suggests automatic acceptance of the local authority's

determination of which assets are "critical." It also implies that any information then submitted relative to those assets also becomes SSI. In that circumstance, we believe it is reasonable to assume that many, if not most, local officials will treat any related records in their custody as SSI and deny them to the public, whether or not the records have any real bearing on security.

We ask that the regulations be rewritten to state that submission of these lists does not, per se, confer SSI status on records of the assets. The regulations also should make clear that not all information related to those assets may be SSI, and that any information subsequently submitted on those assets will be carefully vetted for relevance to security issues. The regulations should emphasize that state and local officials should not treat public information in their files as SSI until it has specifically been accepted as such by TSA, the Coast Guard or DOT. The regulations should also make clear that information submitted which does not legitimately qualify as SSI will be separated (a reverse redaction) and will be available through an appropriate FOIA request.

We urge particular attention and careful vetting to any records submitted that deal with contractual matters, expenditure of public dollars, and operational issues where there may be accountability questions. The three SSI-designating agencies should also honor requests for a FOIA-like special review when the information being protected for security considerations also goes to the expenditure of tax dollars, fees or other revenues, or other matters of public policy concern.

**"Other Information" Could Mean Almost Anything**

We're not quite sure what "other information" is. But we don't think we like its definition in Section 1520.5(b)(16) as "Any information not otherwise described" that TSA or the secretary of DOT "determines is SSI." That could literally be anything. The definition is so vague and indefinite a provision that it would be problematic even if only the top administrators of DOT, TSA or the Coast Guard were the persons making that determination. But as we've objected elsewhere, this is not the case; the authorization is itself quite broad.

We ask that you delete this provision and contain SSI within the already broad parameters prescribed in the first 15 subsections of 1520.5 (b). Alternatively, we would

urge that the language of (16) be rewritten to limit the decision-making therein to the TSA administrator, the secretary of transportation, and their immediate subordinates.

**Do Not Expand the Ranks of Covered Persons**

TSA and DOT are inviting comments on whether to include as "covered persons" emergency workers and local law enforcement personnel who are not directly involved in safeguarding transportation or even assigned to the transportation facility. Please don't.

We can imagine little, if any, benefit to transportation security in so doing. And we believe it might have just the opposite effect; it might lessen security and create new vulnerabilities.

The question often asked rhetorically about what constitutes a secret might be asked here about "sensitive" information. How many people have to be told before the information is no longer protected?

A more relevant series of questions might be asked.

What information is so critical to public safety that it must be shared in advance with law enforcement or rescue personnel who have only rare, time-of-emergency contact with a transportation facility?

Can these officers and rescue workers reasonably be expected to commit that information to memory? Or will they keep this sensitive security information in readily accessible – and highly insecure – places?

If this is practical information that will assist a police officer in protecting the public, might it also benefit the public accidentally caught in a violent situation? Would the public be safer, and the transportation system more secure, if the public had the knowledge to act on their own? We need only think about the heroic actions of passengers on the last of the planes hijacked on September 11, 2001.

And what are the unintended consequences of this "spread of secrecy." The media, as well as the friends and families of many accident victims and of persons who became unexpectedly ill, have discovered the unintended consequences of the well-meaning Health Insurance Portability and Accountability Act, which provides stiff penalties for medical workers who give out patient information. The penalties pose such a

threat that many family members or friends have found it impossible to obtain more than cursory information about a loved one's condition; sometimes they are told nothing. Many law enforcement officials, even though the act does not cover them, cite HIPAA in refusing to provide the names of accident or crime victims who have been hospitalized.

It does not take an overactive imagination to believe that a similar shutdown of information could result from putting hundreds of thousands of local law enforcement and emergency personnel under "covered person" status, then threatening them with significant financial and even criminal penalties if they discuss anything related to the SSI shared with them.

That same threat of punishment is not likely to stop or slow those who wish to aid our enemies. However, it is certain to keep all manner of information that is not SSI from getting to a public that is entitled to have it. It is likely to block or slow the flow of information to people who need to have it for their individual or collective safety. People must have information to make the right decisions in a time of crisis.

There is, we suggest, enormous insecurity in too much security.

We believe that if this information is truly sensitive – so sensitive that it must denied the public for their own protection – then its distribution should be tightly contained. "Need to know" should not be an easy standard. As the regulations are currently written, there is no standard at all.

**"Convenience" Is Not a FOIA Exemption**

That may seem an uncalled-for statement, but it is prompted by our reading of the summary comments on Section 1520.15. It says of the current approach taken by TSA in handling FOIA requests: "If it is impractical to redact the requested information from the record, the entire record is withheld." We believe that both the FOIA and sound public policy dictate a more rigorous effort to segregate information. The Justice Department's most recent FOIA Guide says that any information that is "reasonably segregable" should be released. An entire record may be withheld only if the non-exempt data is so "inextricably intertwined" that redaction would leave a document that is "essentially meaningless words and phrases." The Justice Department guide seems a reasonable and practical reassurance that should be written into the new regulations.

There is an additional problem in this regard. In 1520.9 and 15.13, a "covered person" is directed to mark as Sensitive Security Information the entire document or record, not just that portion of the information that is legitimately SSI. There is no reference to segregation or separation of non-SSI information through redaction of SSI or otherwise. The regulations as written will have the effect of sealing entire documents when significant portions may not, in fact, qualify in any way for protection. The unintended consequence of that kind of indiscriminate marking can only be to extract from the public record information that is at best tangentially related to security issues but is critical to public oversight. This is information that clearly must remain in the public domain.

**In Creating a Fourth Level of Classification, Study the Lessons**

We urge TSA, the Coast Guard and DOT, as they create what can only be described as a fourth level of classification, to consider the lessons learned from the operation of our current system of classification.

Two days before the regulations under discussion went into effect in June, William J. Leonard, the director of the Information Security Oversight Office, made a speech at a seminar for classification managers.

Leonard cautioned the classifiers that it is not the security marking "that protects truly sensitive information from unauthorized disclosure but rather the people who deal with the information – their knowledge and understanding of the program and faith in the system."

Earlier in these comments, we expressed our concern about the lack of rigor in designating who is "covered" and the permissiveness in allowing any "covered person" to mark information SSI. We re-emphasize that concern here. We believe the approach outlined in the Interim Final Rule will result in significant amounts of information that is not truly SSI being withheld from the public.

We suspect it will also result in an unacceptable amount of SSI not being adequately protected – a point Mr. Leonard makes in discussing what he considers sometimes overzealous classification activity.

We believe several of Mr. Leonard's "basic principles" for making classification work are relevant to the issues being discussed here, and we note them for emphasis: 1)

education and training of those doing the work; 2) proactive review within the agency of classification decisions; 3) well-defined parameters with a high bar for classification; and 4) clear limits on what can be included. As Mr. Leonard cautioned, too little classification increases the potential for harm; inappropriate classification undermines the integrity of the process; and too much "unnecessarily impedes effective information sharing."
We have also been reminded, through the handling of the recent Senate report on pre-war Iraq intelligence, that information is often withheld that is not, by any reading, sensitive. Indeed, the redaction by the CIA of information went beyond unnecessary and has prompted four senators, Bob Graham, Trent Lott, Olympia Snowe, and Ron Wyden to introduce legislation creating an independent review panel to serve as an initial check on those kind of classification decisions. The expansion of SSI as an unofficial but nonetheless real fourth level of classified information deserves no less a double-check.

We acknowledge that balancing the information and security needs of a democratic society is not an easy task. We believe it is particularly difficult in the instances we have discussed, where much of the information of security is interrelated with non-security matters that are important for other public policy reasons.

It is this area of potential collateral damage that prompts our greatest concern, and to which we ask your considered attention. We urge that you carefully redraw the final rule to recognize that there is more than one form of security important to the American people and critical to our form of government.

Respectfully submitted,

Coalition Of Journalists For Open Government

By: Pete Weitzel

American Society of Newspaper Editors
Associated Press Managing Editors
Committee of Concerned Journalists
National Association of Science Writers
Newspaper Association of America
Reporters Committee for Freedom of the Press
Radio-Television News Directors Association
Society of Professional Journalists
Society of Environmental Journalists

July 16, 2004