NTEU
The National Treasury Employees Union

AFGE
AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES • AFL-CIO

BY TELEFAX AND FIRST CLASS MAIL

November 23, 2004

Joe D. Whitley
General Counsel
Department of Homeland
Security
Naval Security Station
Nebraska and Massachusetts
Ave., NW
Washington, D.C. 20528

Dear Mr. Whitley:

We are writing to you on behalf of the tens of thousands of employees of the Department of Homeland Security (DHS) that our unions represent. The purpose of our letter is to register our profound objections to DHS Management Directive Number 11042 (entitled "Safeguarding Sensitive But Unclassified (For Official Use Only) Information") and DHS Form 110000-6 ("Non-Disclosure Agreement").[1]

---

[1] The Directive has apparently been in effect since May 11, 2004. We have been advised that at this time, only new employees at DHS headquarters have been required to sign the Non-Disclosure Agreement, but that this requirement may be imposed department-wide on both new hires and current employees. We have received no assurances that the employees we represent will not be required to sign the Agreement. Indeed, the Washington Post recently reported that all DHS employees would eventually be required to do so. "Homeland Security Employees Required to Sign Secrecy Pledge" (Washington Post, Section A, page 23, November 16, 2004).

While our members fully appreciate the need to safeguard classified and other highly sensitive information against unauthorized disclosure, the Directive and Non-Disclosure Agreement impose restrictions and conditions on DHS employees that go well beyond this legitimate purpose. Indeed, as summarized below, the Directive and Agreement subject employees to the threat of punishment for expressing themselves on a broad range of matters of public concern, in circumstances in which DHS lacks a justification adequate to meet the standards imposed by the First Amendment. Further the Directive violates public policy and our national interest by providing a ready device for officials to suppress and cover up evidence of their own misconduct or malfeasance, by stamping documents "for official use only." Therefore, we request that the Department immediately order the Directive withdrawn, and halt any further distribution of the Non-Disclosure Agreement. In the event that DHS does not take these actions, we will have no choice but to pursue appropriate legal action.

BACKGROUND: THE NON-DISCLOSURE AGREEMENT AND MANAGEMENT DIRECTIVE

The Non-Disclosure Agreement covers three categories of information: "protected critical infrastructure information", "sensitive security information", and "other sensitive but unclassified" information. For purposes of this letter, we will focus on the last category ("other sensitive but unclassified" information). That category is of most urgent concern to us because its breadth is essentially unlimited, and because any DHS employee is authorized to designate any document as "sensitive but unclassified" at his or her discretion.

Thus, the Non-Disclosure Agreement defines "sensitive but unclassified information" ("SBU information") as:

> "an overarching term that covers any information [other than critical infrastructure information or sensitive security information] which the loss of, misuse of, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled [under the Privacy Act], but which has not been specifically authorized under criteria established by Executive Order or an

Act of Congress to be kept secret in the interest of national defense or foreign policy."

SBU includes information categorized as "for official use only" ("FOUO") and "any other identifier used by other government agencies to categorize information as sensitive but unclassified."

The Directive sets forth DHS policy for identifying, safeguarding, and preventing the unauthorized dissemination of SBU information. It identifies eleven categories of information that may be designated "for official use only" including such matters as information of a type that "may be exempt from disclosure" under FOIA, information covered by the Privacy Act and "information that could constitute an indicator of U.S. government intentions, capabilities, operations or activities, or otherwise threaten operations security."

As is readily apparent, these categories themselves are both vaguely defined and extremely broad. Further, any DHS employee can designate information falling within one of these categories as "for official use only." Finally, a supervisor or manager is authorized to designate any information originating under their jurisdiction (even information that does not fall within these categories) as "for official use only."

The Directive states that "FOUO information will not be disseminated in any manner—orally, visually, or electronically--to unauthorized personnel." The Directive does not specify when dissemination is "authorized" except to state that access to FOUO information is based on a "need to know" basis, and that "FOUO information may be shared with other agencies, federal, state, tribal or local government and law enforcement officials provided a specific need to know has been established and the information is shared in furtherance of a coordinated and official government activity."

The Directive states that divulging SBU information "without proper authority could result in administrative or disciplinary action." Similarly, in the Agreement, employees acknowledge that they are aware that violation may result in cancellation of their conditional access to the information covered by the Agreement. They also acknowledge that they are aware that violations of the

Agreement could result in administrative, disciplinary, civil or criminal action. The Agreement specifies that the conditions and obligations imposed apply during the time that the employee is granted conditional access, and "at all times thereafter," unless the employee is released in writing by an authorized representative of DHS.

Further, the Agreement provides that an employee "assigns all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of the information not consistent with the terms of the Agreement." This condition also apparently applies in perpetuity.

Finally, the Agreement contains a purported waiver by employees of their rights to personal privacy. It requires them to confirm that they "understand that the United States Government may conduct inspections at any time or place, for the purpose of ensuring compliance with the conditions for access, dissemination, handling and safeguarding of information under this Agreement." Presumably, this waiver extends to "inspections" that occur in the worksite or in one's personal residence. The waiver also applies to personal belongings.

The possibilities for abuse inherent in a regime that authorizes unlimited searches and provides supervisors unbridled discretion to censor employee speech by simply stamping documents "for official use only," are obvious. In fact, to some extent the Directive itself recognizes this possibility. It admonishes that "designation of information as FOUO is not a vehicle for concealing government negligence, ineptitude, illegalities, or other disreputable circumstances embarrassing to a government agency." Clearly, this ineffective admonition will not prevent officials bent on covering up misconduct from taking full advantage of their authority to stamp documents "FOUO."

LEGAL DEFECTS

The Directive and the Non-Disclosure Agreement are inconsistent with public policy because the regime of censorship they impose is unnecessary to protect against the disclosure of classified or other highly sensitive national security information. Further, the Directive and the Agreement will deprive the public of information they

need to make informed choices and to hold their government accountable. They will stifle protected speech, including whistleblowing, and enable officials to cover-up and hide their misconduct and malfeasance. As shown below, the Directive and Agreement violate both the First and Fourth Amendments. Therefore, we urge you to immediately withdraw the Directive and stop the further dissemination of the Agreement.

1. First Amendment Violations

While the government may impose some restraints on the job-related speech of public employees that would be impermissible if applied to the citizenry at large, it is well settled that public employees retain important rights to free expression under the First Amendment. U.S. v. NTEU, 513 U.S. 454, 465 (1995); Pickering v. Bd. of Educ., 391 U.S. 563, 568 (1968). In evaluating the validity of a restraint on government employee speech, courts must balance the interests of the employee as a citizen commenting upon matters of public concern and the interest of the government, as an employer, in promoting the efficiency of the public service. Pickering, 391 U.S. at 568.

DHS employees have a strong interest as citizens in commenting on matters of public concern. Further, as numerous courts and commentators have observed, the public's interest in hearing what government employees have to say is "manifestly great" because government employees are in a position to offer unique insights into the workings of government. See Sanjour v. EPA, 56 F.3d 85, 94 (D.C. Cir. 1995). Indeed, as we are sure you will agree, the national security is ill-served when reasonable dissent and whistleblowing are discouraged or punished.

The Directive and Non-Disclosure Agreement are particularly troubling because they establish a prior restraint on speech. The Supreme Court has recognized that the impact of a prior restraint on speech is more severe than any single supervisory decision would be because the action chills potential speech instead of addressing actual speech already communicated. See U.S. v. NTEU, 513 U.S. at 468. To defend a prior restriction on employee expression, therefore, the government has a greater burden than it has where an isolated disciplinary action is involved. Id. Specifically, the government must demonstrate that

> the interests of both potential audiences and a vast group of present and future employees in a broad range of present and future expression are outweighed by that expressions' "necessary impact on the actual operation of the Government."

Id. (quoting Pickering v. Bd. Of Educ., 391 U.S. at 571. The government must demonstrate actual harm to justify the suppression of speech; in the absence of such evidence, the employees must prevail. See Sanjour, 56 F.3d at 98.

DHS could not possibly meet its burden of justifying its prior restraint on the speech of its employees because the prohibition is patently overbroad. The range of information that could fall within the category of "sensitive but unclassified" is unlimited, given that any DHS employee has unbridled discretion to stamp any document "for official use only." Obviously, in many instances involving such documents, the public interest in disclosure could outweigh any harm to DHS's operations. The existence of such matters makes it impossible for DHS to discharge its burden, set forth in NTEU, to show that the interests of employees and the public in a broad range of potential future expression would always be outweighed by the "necessary impact on the actual operation of government." In fact, harm to DHS and the public is far more likely to occur if employees are not allowed to speak freely.

The case law is firmly on our side. Courts have routinely struck down as unconstitutional prior restraints on the speech of government employees. See Harman v. City of New York, 140 F.3d 111 (2nd Cir. 1998) (striking down press policy forbidding employees from speaking with media regarding any policies or activities of the agency without first obtaining permission from agency's media relations department); International Assoc. of Firefighters Local 3233 v. Frenchtown Charter Township, 246 F.Supp. 2d 734 (E.D. MI 2003) (fire department restricted employees' communications with the media and public); Kessler v. City of Providence, 167 F.Supp. 2d 482 (D.R.I. 2001) (same); Fire Fighters Assoc. v. Barry, 742 F.Supp. 1182 (D.D.C. 1990) (same).

Further, while non-disclosure agreements requiring pre-clearance review and approval have been upheld in the context of classified information (e.g. Snepp v. United

States, 444 U.S. 507 (1980)), both the D.C. Circuit and the Fourth Circuit have held that the government may not extend such agreements to non-classified materials or to materials that are also available from a public source. McGehee v. Casey, 718 F.2d 1137, 1141 (D.C. Cir. 1983); United States v. Marchetti, 466 F.2d 1309, 1311 (4th Cir. 1983). The DHS Agreement, clearly applies to such non-classified material. Accordingly, it is unconstitutional.

2. **Fourth Amendment Violation**

In addition to the First Amendment infirmities of the Directive and Non-Disclosure Agreement, the Agreement provides that the government "may conduct inspections at any time or place, for the purpose of ensuring compliance with the conditions for access, dissemination, handling and safeguarding of information under this Agreement." Requiring public employees to agree to this broad and undefined waiver of privacy clearly violates the Fourth Amendment.

As discussed above, the Agreement's language ("at any time or place") is broad enough to cover searches outside the workplace (such as the employee's residence), as well as searches at the workplace in areas where the employee has a reasonable expectation of privacy. The Supreme Court has held, however, that "[i]ndividuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer." O'Connor v. Ortega, 480 U.S. 709, 717 (1987).

Individuals cannot constitutionally be required, as a condition of government employment, to consent to warrantless searches of their residences, cars, or other areas off government property where they have an expectation of privacy. Instead, they have a right under the Fourth Amendment to insist that any search be made pursuant to a valid warrant, unless one of the narrow exceptions applies, and they cannot be penalized for exercising that right. See, e.g., Gasho v. United States, 39 F.3d 1420, 1431-32 (9th Cir. 1994); United States v. Prescott, 581 F.2d 1343, 1350-53 (9th Cir. 1978).

Moreover, even at the workplace, federal employees may have a reasonable expectation of privacy in their own purses and briefcases, or other private areas of their offices. Simply because the government in its capacity as

employer may be able to search some areas of offices to retrieve work-related material or to investigate allegations of workplace rule violations based on a

reasonable suspicion does not mean that the government may constitutionally conduct unreasonable searches. See O'Connor v. Ortega, 480 U.S. at 717, 731 (Scalia, concurring). The unreasonableness of a warrantless search into purses, briefcases, or locked drawers is heightened by the apparent absence of any valid regulations or guidelines specifying the scope of the intended searches and their justification. See, e.g., Schowengerdt v. General Dynamics Corp, et al., 823 F.2d 1328, 1333-37 (9th Cir. 1987).

In short, the waiver of privacy rights contained in the Non-Disclosure Agreement cannot withstand scrutiny under the Fourth Amendment. Further, requiring employees to provide advance consent to inspections at any time and any place also contravenes public policy, by providing officials with unbridled discretion which could easily be used to intimidate or discourage DHS employees from engaging in protected speech.

CONCLUSION

Given the constitutional infirmities outlined above, we believe that the implementation of DHS's Directive and Non-Disclosure Agreement is clearly illegal. Moreover, even leaving aside the legal arguments, the broad Directive and Non-Disclosure Agreement undermine important public interests in free speech that actually protect our national

security. For those reasons, we request that the Department promptly order the Directive withdrawn, and halt any further distribution of the Non-Disclosure Agreement.

Sincerely,

Gregory O'Duden
General Counsel
NTEU

Mark Roth (ek)

Mark Roth
General Counsel
AFGE

cc: Thomas J Ridge,
Secretary, DHS