Testimony by Scott Armstrong
Director, Information Trust
to the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment

"Over-classification and Pseudo-classification: The Impact on Information Sharing" Hearing
March 22, 2007

Scott@InformationTrust.org
Information Trust
2620 Quebec St NW
Washington DC 20008-1221

It is an honor to address the issues of Over-classification and Pseudo-classification before this subcommittee, particularly as so many of its experienced and distinguished members have labored to provide leadership on these difficult questions to this and other committees of the Congress.

My views today are my own, but I should note that I have been working closely with the Aspen Institute to sustain a six-year exchange between senior journalists, editors and publishers and high level US government officials from various national security and intelligence agencies, including senior members of the congressional intelligence committees and their staffs. The purpose of the Dialogue on Journalism and National Security has been to address recurring concerns about the handling of sensitive national security information by government officials and representatives of the news media. The discussions have included the Attorney General, the Director of the Central Intelligence Agency and ranking officials from the National Security Council, the Department of Defense, the National Security Agency, the FBI as well as the CIA and the Department of Justice.

The Dialogue began after both Houses of Congress had passed in October 2000 what in effect was America's first Official Secrets Act. President Clinton vetoed that legislation, but the legislation was reintroduced in the summer of 2001.

The Bush administration decided to study the issue further and agreed with the news media that the practical effect of informal, candid and well articulated discussions which produce working understandings in order to protect national security information was preferable largely unenforceable legislation. Ultimately, the public has benefited from probing yet responsible reporting on highly sensitive matters. At the same time, the Dialogue has reduced the likelihood of misunderstandings which could damage the nation's security by inadvertently disclosing sensitive national security details. The Dialogue is currently considering a variety of initiatives to further improve the exchange on the most important and sensitive issues. I look forward to engaging your members and staff in that process.

******

It is fitting that I am following Bill Leonard on this panel. Bill and his predecessor as Director of the Information Security Oversight Office, Steve Garfinkel, have labored for decades with these issues. They have given

honorable service, calling the attention of the executive and legislative branches to the strained operations of a broken system. We affectionately and ironically refer to their Office as ISOO (I SUE), not just because lawful disclosure of unclassified information frequently requires one to sue under the freedom of information act but because we find it necessary to cite the offices' statistics so frequently that the acronym has a life of its own. Bill has laid out quite clearly the dimensions of the problem.

My traditional quibble is the estimate of how much information is unnecessarily classified. Twenty-two years ago, in 1985, when I left the Washington Post to found the National Security Archive, I interviewed Gen. Richard Stilwell (Ret.), the chairman of the Commission to Review DoD Security Policies and Practices. Secretary of Defense Casper Weinberger had tasked Gen. Stilwell with identifying "systemic vulnerabilities" caused by unauthorized disclosures of classified information. The Reagan administration's concern was not leaks of national security information to the news media, but leaks of a more serious nature, the arrests of three retired and one active duty Navy member on charges of espionage

To my surprise, Gen. Stilwell told me – and soon published in his report – that the principal problem was the contempt the classification system had bred throughout government. At a time when the Pentagon estimated 16 million classified documents, Stilwell estimated the number to be at least six times greater. He repeated the oft quoted (and usually misquoted) sentence from Supreme Court Justice Potter Stewart's concurrence in the Pentagon Papers case that "**when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion**." Like Justice Stewart, Gen. Stilwell believed that "**the hallmark of a truly effective internal security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained**."[1]

Gen. Stilwell was the first person to acquaint me with what had become the norm, the proliferation of Special Access programs and other compartmented intelligence controls, which had created a labyrinth of security measures, often unaccountable and sometimes wholly unauthorized.

[1] Justice Potter Stewart, Concurring Opinion in which Justice White joined. 403 U.S. 713, New York Times Co. v. United States.

Gen. Stilwell recommended that classified documents which are not "permanently valuable records of the government" should be retained for five years or less from the date of origin, unless specifically authorized for retention. Privately he estimated that 85% of the information classified at that time in the Pentagon could be declassified without damage to the national security.

Gen. Stilwell estimated that fully 95% of what is classified and controlled government-wide could declassified and decontrolled within a short period without harm to the national security. Gen. Stilwell maintained that purging the system of its overclassified and unnecessarily compartmented contents and significantly raising the threshold to future over-classification and inappropriate security controls would be the single best security measure the government could perform. Many career intelligence professionals I have met since concur.

In the ensuing twenty years, my experience has reinforced the conclusion that the government needs to spend less energy on calculating how to punish unauthorized disclosures of politically sensitive information to the news media and more on distinguishing the truly sensitive information which must be protected. Once information is identified as properly warranting protection, government officials and the news media have shown a willingness to honor reasonable requirements.

Unfortunately, the trend has been in the opposite direction. The national security bureaucracy failed to correct the abuses pointed out in the Stilwell Report and largely failed to accept the sensible recommendation contained in the 1994 report of the Joint Security Commission chaired by Jeffrey Smith to reconfigure security protection systems to fit more contemporary risk assessments[2] and has failed to implement virtually all the systemic reforms recommended in 1997 by the Commission on Protecting and Reducing Government Secrecy chaired by Daniel Patrick Moynihan.[3] The tenuousness of the current system has grown exponentially as layers of unrelated controls are imposed which do little to address excesses and much to compound them.

---

[2] Joint Security Commission, Redefining Security, A Report to the Secretary of Defense and the Director of Central Intelligence, February 28, 1994.

[3] Report of the Commission on Protecting and Reducing Government Secrecy, 1997, Senate Document 105-2 Pursuant to Public Law 236 103rd Congress.

Rather than continue to extrapolate the size of the current failure, I would like to recast the problem in what I hope might be a more practical light. The problems of over-classification and pseudo-classification are not that national security information of overwhelming significance will be forever denied the public by fiat of the executive branch. The Pentagon Papers will still leak because government oversight process aided by whistleblowers will – eventually -- rise to the challenge. However, the insights in those papers were available for more than a decade only to leaders who publicly justified a war with a logic they knew to be failed.

Once again, we find that the absence of empirical support for a war was disguised and withheld for a decade not only from the public but also was hidden piecemeal behind clouds of murky compartmented intelligence about Weapons of Mass Destruction. The intelligence community's failure of analysis was not apparent – even to itself -- until both the executive and legislative branch acted on faulty conclusions.

The problem is not that major errors will not be eventually exposed. Rather the danger is that clumsiness of the current system may cause an over reaction which further imperils the ability of the public and its representatives to get the daily information needed to operate in a free and open society.

Each day, hundreds upon hundreds of news reporters ask top national security officials of the government detailed questions about how things are going. Many of those conversations are officially approved leaks whereby classified information is selectively and anonymously released to selected journalists in order to shape the views and information which is included in their news organizations reporting for the public. Although these briefings are officially condoned and coordinated, in fact much of the discussion is free ranging and covers in detail information which is technically classified and which is sometimes quite sensitive. The recently concluded trial of I. Lewis "Scooter" Libby was replete with examples of these unattributable, but officially sanctioned, sessions of fact spinning meant for public consumption.

In parallel with this set of secret phone conversations and closed door briefings are a second set of conversations which are neither officially sanctioned nor centrally coordinated. No self-respecting national security reporter -- a species of reporter which the Libby trial may have proven to be

seriously endangered -- would publish or broadcast the “official” leaked story without checking the details and perspectives with other officials and well-placed sources whom the reporter knows and respects. Quite often, perhaps more often than not, these additional views come from career professionals whose lack of partisanship is matched by a commitment that the public be get as accurate and fair an account as is possible without compromising security. My experience of more than three decades has been that while these professionals may confirm and document the official line, quite often they tell a different story than that which the current administration – any administration whether Republican or Democratic – would prefer to have as part of the public record.

The information imparted may spur additional reporting directed to new areas or may provide the grist for further clarification of the official line. Such conversations are often more candid and detailed than the announced or leaked story coming from the top. Yet, in the shared experience of most of my colleagues, the information is imparted in a careful and controlled manner which avoids dangerous unauthorized disclosures and may include ample warnings that publication or broadcast of certain details originally articulated in the official line could be damaging to national interests. Because reporting is iterative with one interview following another, constantly circling back to the original sources, there is customarily time for a professional journalist to check facts, to identify bias and personal agendas, to hear from official sources any objections to sensitive and damaging information. Responsible journalism is the ability to answer about the importance and meaning of the facts and analysis comprising the story. The response – before the story is published – is to a full range of sources with many perspectives, who are collectively critical about almost all aspects of any complex story.

The record of the past decade demonstrates that the majority of experienced national security reporters have been willing to follow conservative guidance on such matters. They may continue to pursue a sensitive issue but in the course of doing so are likely become even more expert at how to keep the public informed while avoiding the damaging details which might compromise a security interest.

When an administration goes to extraordinary efforts to control information through an unusually compartmentalized control or through threats against leaks imposed using draconian Non-Disclosure Agreements, the effect is

more direct on internal communications in the administration than it is in successfully discouraging leaks. Almost inevitably more secrets mean more leaks. Rather than discouraging officials from correcting the record, such measures primarily tend to constipate information flow within the government. The first impact is between federal agencies and the policy leadership at the top who hold information so closely that responsible officials are operating in the dark. This in turn impedes the customary exchange of information among federal agencies. Ultimately, the phenomenon results in forcing those working in federal agencies to deprive state and local governments of the information they need to meet their responsibilities to efficiently protect the general citizenry.

Unfortunately, the absence of adequate information-sharing has demonstrable consequences. We live with Homeland Security national threat levels measured routinely as elevated and threat levels for domestic and international flights now calibrated as high. Our first responders are expected to deal with severe threats for which adequate training is often withheld for fear it would surface unacceptable vulnerabilities. At virtually all levels of government, elected officials face the prospect of becoming crisis decision-makers when they know they will have to function substantially in the dark without the quantity or quality of intelligence information necessary to perform their jobs.

These same demands of security abroad and at home give rise to an ever growing, increasingly interrelated nexus of federal, state and local bureaucracies. Agencies are collectively and individual challenged by the need for sufficient secrecy to frustrate the threats of stateless terrorists while also sharing information broadly and openly enough to prepare and coordinate responses of our most sophisticated intelligence sources with our formidable first line of defense -- local law enforcement and first responders.

The Homeland Security Information Sharing Act passed by the House in 2002 became a key part of the Homeland Security Act of 2004[4] mandated the creation of a unique category of information known as “sensitive homeland security information” designed to allow this necessary sharing of information with state and local authorities while withholding it from the general public. This designation has proven difficult for the executive to

[4] PL 107-296

resolve, leaving ambiguities on what information can be disclosed and to whom.

Rather than implement the congressional mandate to foster information sharing, the administration instead dispersed information control authority across a broad range of executive agencies. This has resulted in a disjointed and uncoordinated proliferation of sensitive but unclassified designations to protect poorly defined categories of information. In one instance, the Department of Homeland Security drafted a draconian Non-Disclosure Agreement (NDA) designed to apply to restrictions on tens of thousand federal employees and hundreds of thousand state and local first responders. Though only in force briefly, this NDA[5] was more severe than the NDA's in effect for Sensitive Compartmented Information and a variety of controls over the most sensitive information under the government's control.

This NDA required officials, employees, consultants and subcontractors to protect such "sensitive but unclassified information," which is defined as "an over-arching term that covers any 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 … but which has **not** been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information categorized by DHS or other government agencies as: For Official Use Only (FOUO); Official Use Only (OUO); Sensitive Homeland Security Information (SHSI); Limited Official Use (LOU); Law Enforcement Sensitive (LES); Safeguarding Information (SGI); Unclassified Controlled Nuclear Information (UCNI); and **any other identifier used by other government agencies** to categorize information as sensitive but unclassified."

This overbroad but legally binding requirement was implemented as a condition of access to certain categories on unclassified information. This one form represented a vast increase in government secrecy left in the hands of a virtually unlimited number of supervisors. The restraint on those who signed such an agreement was designed to be in effect perpetually until it was explicitly removed. It operated without statutorily defined criteria, rules, limitations or effective oversight by either the administration or the

[5] DHS Form 11000-6 (08-04) See Attached Exhibit A

Congress. Where it did not provide an explicit rationale for withholding "Sensitive But Unclassified" information under the Freedom of Information Act, it surely provided an incentive to err in favor of using other exemptions to deny release.[6]

Although the NDA was withdrawn by DHS in January 2005, it was used last April at the Department to silence private Wackenhut guards, who were speaking to the press about security breakdowns at the Department's Nebraska Avenue headquarters. Other instances of use SBU constraints by government agencies, contractors and utilities appear to be used most often to discourage and prevent the release to the public of otherwise unclassified and available information. Provisions similar to the DHS NDA have since appeared in other employee and contractor agreements both within DHS and within other departments.[7]

The National Intelligence Reform Act of 2004 provided another challenge to the executive which proved daunting. Congress authorized broad centralized power for the new Director of National Intelligence and urged the new DNI to create a tear-line report system by which intelligence gathered by an agency is prepared so that the information relating to intelligence sources and methods is easily severable from the report to protect such sources and methods from disclosure.

The prospect of such a tear-line system encouraged many observers to believe that the classification process could be improved by concentrating on the guidelines for protecting well defined sources and methods. By making a refined decision to protect that which truly requires protection, more of the remaining information would be available for sharing within the intelligence community as well as with the state and local officials charged with Homeland Security responsibilities. The public would benefit by the designation of which portions of internally published intelligence required protection and which portions – presumably the majority of conclusions – could be expedited for release to the news media and the public.

---

[6] See also DHS directive (MD 11042) on "Safeguarding Sensitive But Unclassified (For Official Use Only) Information," dated May 11, 2004.

[7] See CRS Report RL33303, "Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information, February 15, 2006 Genevieve J. Knezo, Specialist in Science and Technology Policy, Resources, Science, and Industry Division.

A more professional and refined understanding within the national security community of what truly requires protection has another important consequence. The logical extension of a tear-line intelligence regime would also be more uniform and rational contemporary access to intelligence for Congress.

The unrealized tear-line mandate has frustrated the ability of Congress to overcome the most often repeated complaints about the oversight process. Both the intelligence community and the congressional committees who oversee them are critical of mutual failures to communicate intelligence conclusions and congressional queries clearly. The failure to implement systems to communicate more detailed and variegated intelligence product are viewed by many informed observers as being responsible for the cumbersome and sluggish information flow to oversight committees and for the failure of those committees to effectively communicate their concerns.

In recent years, each congress has considered legislation premised on the assumption that unauthorized disclosures by the executive are responsible for a growing national security crisis. When significant national security policy debates are informed largely by unauthorized disclosures, there is inevitably a concern in both political and professional intelligence circles about disclosures which damage the credibility of the nation's senior officials to keep secrets the relationships with their sources and cooperating foreign governments. Nevertheless, until recently, career intelligence professionals have tended not to believe there is a growing crisis of sensitive, damaging information leaking out to reporters who will compromise the nation's secrets. The informal system of news media access to secrets through official and unofficial leaks has tended to balance out without serious damage to specific sources and methods.

Recently however, the administration has spoke out strongly at both political and professional intelligence levels about damage to their interests. There appears to be a debate internally about the extent to which sources and methods are being compromised. This in turn has spurred news media concern about the accuracy and candor of government sources when career officials feel compelled to withhold comment and background information from the news media. Increasingly, officials in certain departments must regularly risk their security clearances and thus potentially their careers and their family's financial security in order to correct and guide the public record. The willingness of government prosecutors to pursue the news

media to reveal sources, even to the point of using grand juries and subpoenas of phone records has disturbed a well established pattern of interactions between the news media and its government sources.

The current systems of classification and security controls, particularly those over Sensitive But Unclassified information, seem designed more to shape news coverage than to protect sensitive information from disclosure from hostile sources. This suggests several consequences.

- The current classification and information security systems tend to discourage rather than facilitate effective information-sharing within the federal government and with state and local government.
- At the same time, these overly broad and excessive classification and SBU control systems prevent -- rather than enhance – effective protection of vital national security information by clouding what truly requires protection.
- If the classification and SBU systems continue to develop draconian tools to control unauthorized disclosures, the news media will be less able to provide the public and Congress to get a regular flow of accurate and balanced information from sources who are careful to avoid compromising the national security. At the same time, these measures will do little to protect truly sensitive national security information from other harmful disclosures.
- Rather than attempting to repair the present system of over-classification, the public, the news media, the Congress, and the intelligence community would benefit more from the specification of rigorous and tight definitions of sources and methods in accord with tear-line processing of intelligence in order to maximize information-sharing while protecting the nation’s secrets.

Exhibit A

Department of Homeland Security Form

DHS Form 11000-6 (08-04)

DEPARTMENT OF HOMELAND SECURITY
NON-DISCLOSURE AGREEMENT

NON-DISCLOSURE AGREEMENT

I, _____, an individual official, employee, consultant, or subcontractor of or to _____ (the Authorized Entity), intending to be legally bound, hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain information, specified below, that is owned by, produced by, or in the possession of the United States Government.

(Signer will acknowledge the category or categories of information that he or she may have access to, and the signer's willingness to comply with the standards for protection by placing his or her initials in front of the applicable category or categories.)

Initials:	**Protected Critical Infrastructure Information (PCII)**

I attest that I am familiar with, and I will comply with all requirements of the PCII program set out in the Critical Infrastructure Information Act of 2002 (CII Act) (Title II, Subtitle B, of the Homeland Security Act of 2002, Public Law 107-296, 196 Stat. 2135, 6 USC 101 et seq.), as amended, the implementing regulations thereto (6 CFR Part 29), as amended, and the applicable PCII Procedures Manual, as amended, and with any such requirements that may be officially communicated to me by the PCII Program Manager or the PCII Program Manager's designee.

Initials:	**Sensitive Security Information (SSI)**

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of SSI information as cited in this Agreement and in accordance with 49 CFR Part 1520, "Protection of Sensitive Security Information," "Policies and Procedures for Safeguarding and Control of SSI," as amended, and any supplementary guidance issued by an authorized official of the Department of Homeland Security.

Initials:	**Other Sensitive but Unclassified (SBU)**

As used in this Agreement, sensitive but unclassified information is an over-arching term that covers any information, not otherwise indicated above, 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 Section 552a of Title 5, as amended, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information categorized by DHS or other government agencies as: For Official Use Only (FOUO); Official Use Only (OUO); Sensitive Homeland Security Information (SHSI); Limited Official Use (LOU); Law Enforcement Sensitive (LES); Safeguarding Information (SGI); Unclassified Controlled Nuclear Information (UCNI); and any other identifier used by other government agencies to categorize information as sensitive but unclassified.

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of the information to which I am granted access as cited in this Agreement and in accordance with the guidance provided to me relative to the specific category of information.

I understand and agree to the following terms and conditions of my access to the information indicated above:

1. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of information to which I have been provided conditional access, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

2. By being granted conditional access to the information indicated above, the United States Government has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement and the laws, regulations, and directives applicable to the specifi c categories of information to which I am granted access.

3. I attest that I understand my responsibilities and that I am familiar with and will comply with the standards for protecting such information that I may have access to in accordance with the terms of this Agreement and the laws, regulations, and/or directives applicable to the specifi c categories of information to which I am granted access. I 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 information under this Agreement.

4. I will not disclose or release any information provided to me pursuant to this Agreement without proper authority or authorization. Should situations arise that warrant the disclosure or release of such information I will do so only under approved circumstances and in accordance with the laws, regulations, or directives applicable to the specific categories of information. I will honor and comply with any and all dissemination restrictions cited or verbally relayed to me by the proper authority.

5. (a) For PCII - (1) Upon the completion of my engagement as an employee, consultant, or subcontractor under the contract, or the completion of my work on the PCII Program, whichever occurs first, I will surrender promptly to the PCII Program Manager or his designee, or to the appropriate PCII officer, PCII of any type whatsoever that is in my possession.
(2) If the Authorized Entity is a United States Government contractor performing services in support of the PCII Program, I will not request, obtain, maintain, or use PCII unless the PCII Program Manager or Program Manager's designee has first made in writing, with respect to the contractor, the certification as provided for in Section 29.8(c) of the implementing regulations to the CII Act, as amended.
(b) For SSI and SBU - I hereby agree that material which I have in my possession and containing information covered by this Agreement, will be handled and safeguarded in a manner that affords sufficient protection to prevent the unauthorized disclosure of or inadvertent access to such information, consistent with the laws, regulations, or directives applicable to the specific categories of information. I agree that I shall return all information to which I have had access or which is in my possession 1) upon demand by an authorized individual; and/or 2) upon the conclusion of my duties, association, or support to DHS; and/or 3) upon the determination that my official duties do not require further access to such information.

6. I hereby agree that I will not alter or remove markings, which indicate a category of information or require specific handling instructions, from any material I may come in contact with, in the case of SSI or SBU, unless such alteration or removal is consistent with the requirements set forth in the laws, regulations, or directives applicable to the specific category of information or, in the case of PCII, unless such alteration or removal is authorized by the PCII Program Manager or the PCII Program Manager's designee. I agree that if I use information from a sensitive document or other medium, I will carry forward any markings or other required restrictions to derivative products, and will protect them in the same matter as the original.

7. I hereby agree that I shall promptly report to the appropriate official, in accordance with the guidance issued for the applicable category of information, any loss, theft, misuse, misplacement, unauthorized disclosure, or other security violation, I have knowledge of and whether or not I am personally involved. I also understand that my anonymity will be kept to the extent possible when reporting security violations.

8. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to the information covered by this Agreement. This may serve as a basis for denying me conditional access to other types of information, to include classified national security information.

9. (a) With respect to SSI and SBU, I hereby assign to the United States Government 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 this Agreement.
(b) With respect to PCII I hereby assign to the entity owning the PCII and the United States Government, all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of PCII not consistent with the terms of this Agreement.

10. This Agreement is made and intended for the benefit of the United States Government and may be enforced by the United States Government or the Authorized Entity. By granting me conditional access to information in this context, the United States Government and, with respect to PCII, the Authorized Entity, may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I understand that if I violate the terms and conditions of this Agreement, I could be subjected to administrative, disciplinary, civil, or criminal action, as appropriate, under the laws, regulations, or directives applicable to the category of information involved and neither the United States Government nor the Authorized Entity have waived any statutory or common law evidentiary privileges or protections that they may assert in any administrative or court proceeding to protect any sensitive information to which I have been given conditional access under the terms of this Agreement.

11. Unless and until I am released in writing by an authorized representative of the Department of Homeland Security (if permissible for the particular category of information), I understand that all conditions and obligations imposed upon me by this Agreement apply during the time that I am granted conditional access, and at all times thereafter.

12. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions shall remain in full force and effect.

13. My execution of this Agreement shall not nullify or affect in any manner any other secrecy or non-disclosure Agreement which I have executed or may execute with the United States Government or any of its departments or agencies.

14. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958, as amended; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 USC 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

15. Signing this Agreement does not bar disclosures to Congress or to an authorized official of an executive agency or the Department of Justice that are essential to reporting a substantial violation of law.

16. I represent and warrant that I have the authority to enter into this Agreement.

17. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me any laws, regulations, or directives referenced in this document so that I may read them at this time, if I so choose.

DEPARTMENT OF HOMELAND SECURITY

NON-DISCLOSURE AGREEMENT

Acknowledgement

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:

I make this Agreement in good faith, without mental reservation or purpose of evasion.

Signature:

WITNESS:

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:

Signature:

This form is not subject to the requirements of P.L. 104-13, “Paperwork Reduction Act of 1995” 44 USC, Chapter 35.