



U.S. Department of Justice

Office of Information and Privacy

---

Telephone: (202) 514-3642

Washington, D.C. 20530

Mr. Steven Aftergood  
Senior Research Analyst  
Federation of American Scientists  
1717 K Street N.W., Suite 209  
Washington D.C. 20036

MAR 29 2005

Re: AG/04-R0517  
MAP:TSW:DM

Dear Mr. Aftergood:

This responds to your Freedom of Information Act request dated February 27, 2004, and received in this Office on March 4, 2004, in which you requested a copy of an interagency memorandum on information sharing dated March 4, 2003. This response is being made on behalf of the Office of the Attorney General.

I apologize for the delay of this response, which was caused by the need to consult with another Department component and other agencies. I have determined the document, consisting of twenty pages, is appropriate for release without excision and a copy is enclosed.

Inasmuch as this constitutes a full grant of your request for processing on behalf of the Office of the Attorney General, I am closing your file in this Office.

Sincerely,

Melanie Ann Pustay  
Deputy Director

Enclosure

MEMORANDUM OF UNDERSTANDING BETWEEN THE INTELLIGENCE  
COMMUNITY, FEDERAL LAW ENFORCEMENT AGENCIES, AND THE DEPARTMENT  
OF HOMELAND SECURITY CONCERNING INFORMATION SHARING

This Agreement provides a framework and guidance to govern information sharing, use, and handling between: the Secretary of Homeland Security, on behalf of the Department of Homeland Security (DHS), including all entities that are, or become, wholly or in part, elements of DHS; the Director of Central Intelligence (DCI), on behalf of all entities that are, or become, wholly or in part, elements of the United States Intelligence Community (IC), other than those that are to become part of DHS; and the Attorney General, on behalf of the Department of Justice (DOJ), including the Federal Bureau of Investigation, and all entities that are, or become, wholly or in part, elements of DOJ, and any other department, agency, or entity having federal law enforcement responsibilities, other than those that are to become part of DHS.

1. Scope of Application. This Agreement shall be binding on all such departments, agencies, and entities on whose behalf the Secretary of Homeland Security, the DCI, and the Attorney General agree herein. This Agreement is intended to mandate minimum requirements and procedures for information sharing, use, and handling, and for coordination and deconfliction of analytic judgments. Departments and agencies are encouraged to develop additional procedures and mechanisms to provide for greater information sharing and coordination than required herein, consistent with the DHS Legislation and other relevant statutory authorities, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, and this Agreement, including, but not limited to:

- (a) the Homeland Security Act of 2002;
- (b) the National Security Act of 1947, as amended;
- (c) the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001;
- (d) the Foreign Intelligence Surveillance Act, as amended;
- (e) Executive Order 12333, as amended, and any subsequent Executive Orders on Intelligence Activities;
- (f) Executive Order 13231, as amended, and any subsequent Executive Orders on Homeland Security;
- (g) Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation, dated September 23, 2002; and
- (h) Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons, dated September 23, 2002.

To the extent that this Agreement provides for more expansive information sharing than other authorities or agreements, with the exception of statutes, or Presidential Directives including, but not limited to, Executive Orders ("Presidential Directives"), the more expansive provisions of this Agreement shall be followed.

2. Definitions. For purposes of this Agreement:

(a) "Analytic conclusion" means the product of analysis of one or more pieces of information in which inferences are drawn from the information being analyzed to arrive at a determination about a fact – such as, for example, a potential threat – that is not explicit or apparent from the face of the original information itself. It does not include, for example, a summary of the factual content of a piece of intelligence information, a report of an interview, or a report or other document that merely collects and summarizes information from multiple sources about the same or related topics, or other types of communication which do not include analytic conclusions as described above.

(b) "Attorney General" means the Attorney General of the United States or the Attorney General's designee, except as otherwise provided herein.

(c) "Classified information" means information that has been determined pursuant to Executive Order No. 12958, or any successor order, Executive Order No. 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure.

(d) "Covered entity" means: any department, agency, bureau, office or other entity that is, or becomes, wholly or in part, an element of the Department of Homeland Security (including the Department itself); any department, agency, bureau, office or other entity that is, or becomes, wholly or in part, an element of the United States Intelligence Community or the Department of Justice; and any other department, agency, or entity having federal law enforcement responsibilities.

(e) "Covered information" means terrorism information, weapons of mass destruction (WMD) information, vulnerabilities information, and other information relevant to the duties of the Department of Homeland Security, as well as analyses based wholly or in part on such covered information.

(f) "Department" or "DHS" shall mean the Department of Homeland Security and any entity that is, or becomes, an element of that Department.

(g) "DHS Legislation" means the Homeland Security Act of 2002 (H.R. 5005, 107th Congress, 2d Session) (November 26, 2002), as it may be amended from time to time.

(h) "DCI" means the Director of Central Intelligence, or, except as otherwise provided herein, the DCI's designee, in his or her capacity as head of the Intelligence Community, and as head of the Central Intelligence Agency.

(i) "Foreign intelligence" has the meaning given to that term in section 3 of the National Security Act of 1947, as amended (50 U.S.C. 401a), as that statutory term may be amended from time to time.

- (j) "Homeland" means the United States as defined in the DHS Legislation.
- (k) "Infrastructure" means the basic systems, assets, facilities, services, and installations needed for the functioning of our society. The term includes, but is not limited to, critical infrastructure, meaning systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on United States national security, economic security, national public health or safety, or any combination of these. Critical infrastructure includes, but is not limited to, agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry and hazardous materials, postal and shipping, and national monuments and icons.
- (l) "Infrastructure information" means all information related to the identification, status, security, criticality, risk assessment, vulnerability to all means of attack, interdependency, and attack consequences (including potential impact on public health or safety, the economy, national security, governance and public confidence) of the infrastructure of the United States.
- (m) "Intelligence Community" has the meaning given it in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)), as it may be amended from time to time.
- (n) "Need-to-know" means a determination made by an authorized holder of classified information, or sensitive law enforcement information, that a prospective recipient requires access to a specific piece, or category of information in order to perform or assist in a lawful and authorized governmental function.
- (o) "Parties" means the signatories to this Agreement and their successors, on behalf of all covered entities they head, supervise or represent.
- (p) "PATRIOT Act" means the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56, 115 Stat. 272, 278-81.
- (q) "Secretary" means the Secretary of Homeland Security or the Secretary's designee, except as otherwise provided herein.
- (r) "Terrorism information" means all information relating to the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, domestic groups or individuals involved in terrorism, to threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations, or to communications between such groups or individuals, and to

information relating to groups or individuals reasonably believed to be assisting or associated with them.

(s) "Vulnerabilities information" means all information relating to the susceptibility -- actual, perceived, or conceptual -- of the United States, including any portion, sector, population, geographic area, or industry, to terrorist attack.

(t) "Weapons of Mass Destruction information" or "WMD information" means terrorism information or vulnerabilities information relating to conventional explosive weapons and non-conventional weapons capable of causing mass casualties and damage, including chemical or biological agents, radioactive or nuclear materials, and the means to deliver them.

3. Policies and Procedures for Information Sharing, Handling and Use. Consistent with the DHS Legislation, and except as otherwise specifically provided in this Agreement, the following agreed-upon policies and procedures shall apply to the provision of covered information by any covered entity to any other covered entity, to the interpretation of all provisions of this Agreement, and to the resolution of all issues related to information sharing, handling and use, and the coordination and deconfliction of operations and analytic conclusions:

(a) *Priority on Preemption, Prevention, and Disruption.* All procedures, guidelines, and mechanisms under this Agreement shall be designed and implemented, and all determinations with regard to sharing information covered by this Agreement shall be made, with the understood, overriding priority of preventing, preempting, and disrupting terrorist threats to our homeland. The parties recognize and agree that, in some cases, this priority shall dictate information sharing even where doing so may affect criminal prosecutions or ongoing law enforcement or intelligence operations. Nonetheless, the covered entities shall act under this Agreement in a manner to protect, to the greatest extent possible, these other significant interests, including the protection of intelligence and sensitive law enforcement sources and methods, other classified information, and sensitive operational and prosecutorial information.

(b) *Reciprocity and Transparency.* All information collected by any covered entity relevant to the missions and responsibilities of any other covered entities should be shared, to the greatest extent possible, between and among all covered entities. Likewise, the parties agree that, to the greatest extent possible, there should be transparency between and among the covered entities with regard to their activities to preempt, prevent, and disrupt terrorist attacks against U.S. persons and interests. Except as otherwise specified in this Agreement, or mandated by relevant Federal statutes or Presidential Directives, procedures and mechanisms for information sharing, use, and handling shall be interpreted and implemented consistently and reciprocally regardless of the role a particular covered entity plays as a provider or recipient of covered information. In other words, for example, international terrorism information collected by the Border Patrol should be shared by DHS with the IC to the same extent foreign intelligence information on terrorism is shared by the IC with DHS.

(c) *Scope of "Covered Information."* Consistent with the priority established in Section 3(a), information relating to terrorism, Weapons of Mass Destruction, vulnerabilities, or other functions of the Department of Homeland Security shall be presumed to be "covered information" under this Agreement. If, after applying this presumption, disagreement remains between covered entities about whether particular information is "covered information," such disagreement shall be resolved pursuant to Section 4(d).

(d) *Effective date of information sharing obligations.* Notwithstanding provisions of this Agreement mandating further agreement on mechanisms, procedures, or other issues, the parties recognize that the obligation to promptly begin the full range of information sharing mandated by the DHS Legislation came into force on January 24, 2003, and that obligations under this Agreement will be in force upon the signature of all parties.

(e) *Sharing Requirements Based on Substance Only.* Consistent with the DHS Legislation and other relevant statutory authorities, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, and this Agreement, the parties agree that this Agreement requires that covered information, including, but not limited to, terrorism information, WMD information, infrastructure, and vulnerabilities information, be provided by any covered entity that collects or analyzes that information to any other covered entity that has a need-to-know that information (or information relating to that subject matter), based on a broad interpretation of the mission of the other covered entity, regardless of:

(i) The type of communication in which the information is incorporated. Covered information must be provided as required in this Agreement regardless of the type of communication in which it is originally reported by the providing agency. The fact that particular covered information may be contained originally in a particular type of communication shall not, under any circumstances, be grounds either to withhold or delay the sharing of any covered information. As illustrative examples only, covered information must be provided by CIA, within the time frames agreed to, whether such information is contained originally in communications referred to as "TDs," "intel cables," "ops cables," or any other type of communication. Likewise, covered information must be provided by the FBI, within the time frames agreed to, whether such information is contained originally in communications referred to as "302s," "ECs," "LHMs," or any other type of communication;

(ii) The manner in which the information is or may be conveyed to the intended agency or individual recipients. Covered entities shall continually endeavor to improve technological means of access to afford maximum flexibility, speed, and volume of information shared, consistent with the strictly necessary protection of intelligence or sensitive law enforcement sources and methods, and with section 3(a) and other relevant provisions of this Agreement.

(f) *Terrorist Threat Integration Center.* The parties agree that, when fully operational, the Terrorist Threat Integration Center (TTIC) shall be the preferred, though not the exclusive, method for sharing covered information at the national level. TTIC information-sharing mechanisms and procedures shall be consistent with the DHS Legislation and other relevant statutory authorities, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, and this Agreement. As soon as practicable, the parties shall determine the extent to which provision of information to one or more covered entities via the TTIC may constitute the only required method for providing such information to such entities, *provided however*, that any decision to share covered information among the parties solely by means of the TTIC shall be memorialized in a separate written agreement executed by the parties, including by designees of the officials signing this Agreement. Analytic conclusions contained in TTIC products shall not be altered by agencies prior to dissemination.

(g) *Policies for Sharing Particular Types of Information With DHS.* Consistent with the DHS Legislation and other relevant statutory authorities, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, and this Agreement, the Secretary shall be provided access to all information necessary for him to carry out the mission of the Department. Except as otherwise directed by the President, the parties agree that the amount of information and depth of detail of information provided to the Secretary, which will vary by the type of information at issue, will be governed by the following policies:

(i) Information Related to Threats of Terrorism Against the United States. As required by the DHS Legislation, DHS shall be provided, without request, all "reports (including information reports containing intelligence which has not been fully evaluated), assessments, and analytical information." The parties understand that, in this category, except upon further request by DHS, and agreement by the originating entity, provided information will not routinely include information, collected through intelligence sources or methods, or sensitive law enforcement sources or methods, which has not been processed in any way to reduce the amount of substantive content or synthesize the material. Thus, for example, a recording of a conversation intercepted under the Foreign Intelligence Surveillance Act (FISA) or an intelligence officer's or FBI agent's hand-written notes of a discussion with a source would not be routinely provided in this category. By contrast, a report forwarding the substance of a FISA-recorded conversation, or an FBI "Electronic Communication" (EC), including the substance of a discussion with a source, even if these include verbatim quotes from the underlying notes, would be provided. ECs containing substantive information, along with "302s," "TDs," "IIRs," and all other similar documents including substantive information, fall into the category of information to be provided. The parties agree, as soon as practicable, to identify and/or put into place necessary and reasonable mechanisms, including, when operational, the TTIC, along with the Joint Terrorism Task Forces (JTTFs), and procedures, to ensure that DHS receives all such information automatically, under the policies

and procedures agreed to in this Agreement, without further request.

(ii) Vulnerabilities Information. As required by the DHS Legislation, DHS shall be provided, without request, all information of any kind concerning "the vulnerability of the infrastructure of the United States, or other vulnerabilities of the United States, to terrorism, whether or not such information has been analyzed." The parties understand that, in this category, without further request by DHS, provided information will routinely include information, collected through intelligence sources or methods, or sensitive law enforcement sources or methods, which has not been processed in any way to reduce the amount of substantive content or synthesize the material. Provided information will include all types of information, without regard to the distinctions drawn by way of example in Section 3(g)(i), except as further agreed to by the parties or their designees. The parties agree, as soon as practicable, to identify and/or put into place necessary and reasonable mechanisms, including, when operational, the TTIC, along with the JTTFs, and procedures, to ensure that DHS receives all such information, under the principles agreed to in this Agreement, without further request.

(iii) Information Relating to Significant and Credible Threats of Terrorism. As required by the DHS Legislation, DHS shall be provided, without request, all information of any kind concerning "significant and credible threats of terrorism against the United States, whether or not such information has been analyzed." The parties understand that, in this category, without further request by DHS, provided information will routinely include information, collected through intelligence sources or methods, or sensitive law enforcement sources or methods, which has not been processed in any way to reduce the amount of substantive content or synthesize the material. Provided information will include all types of information, without regard to the distinctions drawn by way of example in Section 3(g)(i), except as further agreed to by the parties or their designees. The parties agree, as soon as practicable, to identify and/or put into place necessary and reasonable mechanisms, including, when operational, the TTIC, along with the JTTFs, and procedures, to ensure that DHS receives all such information, under the principles agreed to in this Agreement, without further request.

(iv) Other Information Requested by the Secretary. The Secretary shall be provided, upon request, with such other information relating to threats of terrorism against the United States or to other areas of DHS' responsibility, whether or not such information has been analyzed. The parties understand that DHS will be provided information in this category upon request including, if so requested, information which has not been processed in any way to reduce the amount of substantive content or synthesize the material. If so requested, provided information will include all types of information, without regard to the distinctions drawn by way of example in Section 3(g)(i), except as otherwise directed by the President. The parties agree, as soon as practicable, to set up



necessary and reasonable mechanisms, including, when operational, the TTIC, along with the JTTFs, and procedures, to ensure that DHS, when requested, receives all such information, under the principles agreed to in this Agreement.

(h) *Timely Sharing of Information.* Covered information must be provided to those with a need-to-know that information (or information relating to that subject matter), based on a broad interpretation of the mission of the other covered entity, as quickly as possible. Providing all timely and relevant covered information to those who have a need-to-know it in order to assist them in meeting their homeland security-related responsibilities is fundamental to the success of the Department and all other efforts to ensure the security of the homeland from terrorist attack. Delay in providing such information risks frustrating efforts to meet these critical responsibilities and could result in preventable attacks against U.S. persons or interests failing to be preempted, prevented, or disrupted. Accordingly, except as otherwise directed by the President or agreed to by all parties, the parties agree that:

(i) Information that a covered entity reasonably believes relates to a potential terrorism or WMD threat, to the United States homeland, its infrastructure, or to United States persons or interests, shall be provided immediately to other covered entities;

(ii) Other covered information, including, but not limited to, vulnerabilities information, but which a covered entity does not reasonably believe relates to a potential terrorism or WMD threat to the United States homeland, its infrastructure, or to United States persons or interests, shall be provided as expeditiously as possible;

(iii) Under no circumstances may covered information be withheld from a covered entity with a need-to-know that information (or information relating to that subject matter), based on a broad interpretation of the mission of the other covered entity, or may the sharing of such information be delayed beyond the time frames agreed to in this Agreement, except as consistent with the Section 4(d), or other relevant provisions of this Agreement;

(iv) When a question arises as to whether covered information must be provided to the Department or any other covered entity pursuant to this Agreement, the parties will resolve the question pursuant to Section 4(d);

(v) Covered entities agree to use, to the greatest extent possible, the most rapid methods of information sharing, consistent with the strictly necessary protection of intelligence or sensitive law enforcement sources and methods, and with Section 3(a) and other relevant provisions of this Agreement; and

(vi) Consistent with Section 3, and other relevant provisions of this Agreement, the parties agree that they shall work diligently to ensure that all covered entities receive the same information within the same time frame,

provided that the information is relevant to the mission of the covered entities. Further, the parties agree to make reasonable efforts to provide covered information in a format useful to the intended recipient(s).

(i) *Redaction of Intelligence or Sensitive Law Enforcement Source or Method Identifying Information and the Use of Tailored Products.*

(i) Redaction. The parties agree that, consistent with Section 3(a) and other relevant provisions of this Agreement, covered entities originating covered information to be shared may exclude or mask strictly intelligence or sensitive law enforcement source or method identifying information, *provided that* the substance of the covered information may be understood equally well without the redacted information. For information covered by Section 3(g)(ii) and (iii) and, if so requested by the Secretary, by Section 3(g)(iv), redactions may be made only to the extent strictly necessary to remove information that clearly identifies, or would reasonably permit ready identification of, intelligence or sensitive law enforcement sources or methods that are particularly susceptible to countermeasures that would nullify or measurably reduce their effectiveness. The parties further agree that, consistent with Section 3(a) and other relevant provisions of this Agreement, and consistent with the DHS Legislation, the parties may exclude or mask the source of any voluntarily submitted infrastructure or vulnerabilities information, *provided that* the substance of the information may be understood equally well without the redacted information.

(ii) Use of Tailored Products. As an alternative to redaction of original communications, covered entities may create tailored products for transmission of information to DHS or, to the extent practicable, other covered entities, so long as such products are consistent with Section 3(i)(i):

(iii) In no event may a covered entity's choice to exercise either of these options for transmitting information covered by Section 3(h)(i) to DHS result in a delay of sharing covered information beyond the time frame contemplated in that section. If delay is unavoidable as a result of a covered entity's preference for transmission by specifically tailored products, a redacted version of the original communication at issue shall be provided immediately, without waiting for the production of a tailored product, and with only such redactions as are consistent with Section 3(i)(i).

(iv) In any case where a covered entity chooses to exclude or mask information, that entity shall indicate this exclusion or masking to DHS and, to the extent practicable, other covered entities, including, if necessary, directly and exclusively to the Secretary (or head of another covered entity, if applicable), the fact that information was excluded or masked and the reasons for doing so. Such indication of exclusion or masking shall occur at the same time as provision of the remaining information from the same communication or, in the rare instance in which a covered entity determines, consistent with the provisions of this

Agreement, to withhold in its entirety a communication containing covered information, such indication shall occur immediately.

(v) The parties agree that the provisions of this section shall not apply to established source protection procedures utilized by CIA's Directorate of Operations, or equivalent procedures developed and used by other covered entities, *provided that* such procedures do not result in the failure to provide DHS with substantive information as required under the DHS Legislation and this Agreement, and that the Secretary may personally request revisions in such procedures if he determines that they restrict DHS' access to information in a way that jeopardizes DHS' mission. For information described in Section 3(i)(i), such procedures shall be revised, as soon as is practicable, and without request from the Secretary, to ensure that those procedures only remove such intelligence that clearly identifies, or would reasonably permit ready identification of, intelligence or sensitive law enforcement sources or methods that are particularly susceptible to countermeasures that would nullify or measurably reduce their effectiveness.

(j) *Requests for Additional Information.* In addition to the participation of DHS in the "requirements" processes, as discussed further herein, the DHS Legislation provides for DHS to request additional or follow-up information upon receipt of individual items of information. As soon as practicable, the parties shall agree to mechanisms and procedures, including the TTIC, JTTFs, and, if appropriate, focal points, for DHS to make, and covered entities to respond to, such requests. These mechanisms and procedures shall be designed to facilitate the greatest amount of additional information sharing consistent with strictly necessary protection of intelligence or sensitive law enforcement sources and methods, with Section 3(a) and other relevant provisions of this Agreement, and with the timeliest possible responses to requests for additional information.

(k) *Information Use Restrictions.* In general, parties shall disclose covered information free of any originator controls or information use restrictions. Several categories of covered information that must be disclosed to covered entities pursuant to the DHS Legislation, this Agreement, and other authorities, remain subject to special labeling, handling, storage, use and access auditing requirements imposed by statute or, to the extent consistent with the DHS Legislation, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, and this Agreement, pursuant to applicable regulations. The scope and duration of such restrictions, including caveats restricting use of the disclosed information to a particular level or element of a covered entity, will be tailored to address the particular situation or subject matter involved. When imposed, use restrictions shall be no more restrictive than strictly necessary to accomplish the desired effect.

(l) *Secondary Information Sharing.* To the extent consistent with this Agreement, covered entities may share information provided by other covered entities with additional covered entities. Such secondary sharing shall be carried out, to the greatest extent possible, in a manner that permits the originating agency to know to

whom the information has been provided. The parties shall agree, as soon as is practicable, upon recommendations, if any, for changes to Executive Order 12958, Director of Central Intelligence Directive 6/6 (and complementary or successor directives dealing with Originator Controls, the so-called "third agency rule," and other policies or procedures governing the sharing of received information with additional recipients) in order to comply with the DHS Legislation, and to carry out the President's announced policies for protecting against terrorist threats to the homeland, and the provisions of this Agreement.

(m) *Other Obligations to Share Information.* A covered entity's voluntary or obligatory provision of covered information to another covered entity does not in itself discharge or diminish any other obligation the providing entity may have to provide that information, or any part of it, to any other department, agency or other public or private organization or individual under any statute, Presidential Directive, or other agreement. Although all covered entities will attempt to identify and call attention to information relevant to the mission of other covered entities, the responsibility to share information relevant to the mission or responsibilities of any covered entity in addition to DHS remains the responsibility of the originator or initial federal recipient of the information and does not shift to DHS by virtue of DHS' receipt of the information. The parties agree, however, that, to the greatest extent possible, other sharing obligations shall be harmonized and coordinated with those covered by this Agreement, including the agreed preference for using the TTIC and JTTFs as information-sharing mechanisms, in order to reduce duplication, facilitate deconfliction, and increase efficiency.

(n) *PATRIOT Act Information.* Law enforcement-related information related to DHS mission, permitted or required to be provided to intelligence agencies under the PATRIOT Act and its implementing guidelines shall also be considered covered information under this Agreement and shall, therefore, be provided to the Department and other covered entities, in accordance with the DHS Legislation and other relevant statutory provisions, and this Agreement.

(o) *Other Intelligence Information.* Nothing in this Agreement shall be read to restrict the access of the Secretary or his designee to information the Secretary ordinarily would receive as a member of the Intelligence Community, including national security and foreign intelligence information.

(p) *Information Sharing Mechanisms.* As soon as practicable, the parties shall agree upon specific mechanisms, consistent with Section 3 and other relevant provisions of this Agreement, for how different types of covered information will be shared, including technical and administrative arrangements, and, as appropriate, designation of focal points, to maximize the effectiveness and coordination for providing covered information. Subsequent arrangements for information sharing may be reached upon the approval of the parties or their designees. The parties shall work to develop, as part of this process, effective mechanisms for covered entities to identify covered information held by them and to ensure, to the greatest degree feasible, the provision of such information, without specific request, to other covered entities. The parties further agree

that, notwithstanding their agreement to develop further mechanisms and procedures for information sharing, covered entities shall promptly build on mechanisms and procedures already in place to identify and provide to DHS covered information that is generated or received by them in the course of carrying out their missions.

(q) *Methods of Providing Information.* The parties recognize and agree that there are many possible methods for "providing" information, including, but not limited to, hand-delivery, oral briefings, transmission by secure data-link, and affording routine and unrestricted access to computerized databases, including the ability to transfer such information to a recipient entity as necessary, and by full and complete co-location of analysts or other personnel and full integration of, and access to, information, as well as, for example, ensuring that the Secretary receives all daily threat briefing materials (including threat matrices and overnight reports). The parties further agree that requirements to "provide" information under this Agreement may be satisfied, depending on the type of information at issue, by the use of a single mechanism, such as via the TTIC, consistent with section 3(f) of this Agreement, or a combination of mechanisms already in place and/or created under this Agreement. The parties shall agree, as part of the development of these mechanisms and procedures, as to which method, or combination of methods, of providing information will be sufficient for particular types or categories of information.

(r) *Responsible Officials for Information Sharing.* Until such time as modified by the parties, the responsible officials for information sharing under this Agreement are as follows:

(i) For the Secretary of Homeland Security, the Undersecretary for Information Analysis and Infrastructure Protection, or another individual designated by the Secretary to act in this capacity;

(ii) For the Attorney General, Executive Assistant Director for Counterterrorism and Counterintelligence; and

(iii) For the Director of Central Intelligence, the Associate Director of Central Intelligence for Homeland Security.

(s) *Provision of Covered Information to the DHS Directorate of Information Analysis and Infrastructure Protection.* Until further agreement by the parties, or their designees, all covered information provided, including information provided, under current procedures to existing elements transferred to DHS, e.g., the United States Coast Guard and the U.S. Customs Service, shall also be separately provided to the Directorate of Information Analysis and Infrastructure Protection, including, if agreed by the Secretary, via the TTIC. The Undersecretary for Information Analysis and Infrastructure Protection, or another individual designated by the Secretary to act in this capacity, shall work with entities not within the Directorate to ensure effective coordination of information.

(t) *Classified Information.* The head of each covered entity shall put procedures in place to ensure that each individual recipient of classified information has, and maintains, appropriate security clearances, training, and need-to-know to receive classified information at the level at which the recipient will receive such information. Individuals shall be designated at each covered entity at several levels of seniority to receive classified information judged by the originating agency to be sufficiently sensitive to require limited distribution. In rare cases, the parties expect that extremely sensitive information may be provided only to the Secretary or, as appropriate, the head of another covered entity. The head of each covered entity also shall ensure that all mechanisms and procedures for receiving, storing, and handling classified information meet established legal and regulatory standards. The policies and procedures governing access to covered information under this Agreement, including such information that is classified, shall apply without regard to whether that information is made available in written, oral, or electronic form, or to the means or mechanism by which it is communicated to the recipient.

(u) *Thresholds.* In order to ensure that the Department is provided with all information necessary to carry out its responsibilities, but is not inundated with unmanageable volumes of information below thresholds reasonable to perform its mission, as soon as practicable, the Secretary shall advise the other parties, individually or collectively, as to establishing additional thresholds for information sharing, consistent with the DHS Legislation. For example, the Secretary may determine that low-level information concerning purely indigenous foreign terrorist groups with no apparent capability to mount operations against the United States is not relevant to DHS' mission. Such further agreement shall be consistent with the DHS Legislation and other relevant statutory authorities, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, and this Agreement. At any time following such initial agreement, the parties may agree to additional information sharing, or to more or less restrictive thresholds, as the volume of information involved and the needs of DHS become clearer, so long as such agreements are consistent with the DHS Legislation and this Agreement. Such agreements may be made by designees of the parties.

(v) *Privacy.* All information sharing pursuant to this Agreement shall be consistent with applicable privacy laws.

#### 4. Coordination, Deconfliction, and Dispute Resolution.

(a) *Coordination and Deconfliction Policy.* Consistent with the President's direction that our highest priority is the protection of the American people from potentially devastating terrorist attacks, covered entities shall take all necessary measures to ensure that terrorist threats to our homeland are addressed cooperatively, efficiently, and with the understood overriding purpose of preventing, preempting, and disrupting those threats. To that end, the parties agree that no homeland security-related prevention, preemption, or disruption activity of any covered entity shall be presumed to be the best option in any given case, or otherwise deemed of higher precedence, importance, or

priority than any other such activity. The covered entities shall work together, to the greatest extent possible, to achieve, in each case, the maximum preventative, preemptive, and disruptive effect on potential threats, including coordinating simultaneous and complementary activities of multiple covered entities when appropriate. Because the failure to coordinate operational activities to preempt, prevent, and disrupt terrorist threats can create confusion, inefficiency and, in extreme cases, dangerous situations resulting from conflicting operational activities, the parties agree to coordinate operational activities to the greatest possible extent. Specifically, each party shall take all reasonable steps to ensure coordination and deconfliction of homeland security-related law enforcement, intelligence or national security-related activities of covered entities under that party's authority with such activities of other covered entities.

(b) *Analytic Conclusions and Supporting Information.* Terrorism and other homeland-security related analytic efforts of all covered entities must be informed by the most comprehensive, accurate, and timely information available, regardless of its nature and source, including, but not limited to, terrorism, WMD, vulnerabilities, and other pertinent information available to any covered entity. Analytic conclusions relating to terrorist or WMD threats to the homeland, or other issues within the responsibility of DHS, including information updating and amplifying previous conclusions, must be shared with all covered entities as soon as they are produced. Preemptive, preventative, and disruptive actions by all covered entities must be informed to the greatest extent possible by all available information and by all analytic conclusions, including competing conclusions, of all entities with relevant analytic responsibilities. At the same time, the Federal government must, to the greatest extent possible, speak with one voice to state and local officials, private industry, and the public, in order to prevent confusion, mixed signals, and, potentially, dangerous operational conflicts. In furtherance of these goals, the parties agree as follows:

(i) The parties shall ensure that covered entities disseminate their terrorism or other homeland security-related analytic products without delay to other covered entities that have related interests and responsibilities;

(ii) Except as otherwise provided in Sections 4(b)(iii) or (iv), no analytic conclusions, as defined in Section 2(a) of this Agreement, of any covered entity shall be disseminated to state, local, or private sector officials, or to the public, without the prior approval of the Secretary of Homeland Security, his designee, or in accordance with approval mechanisms, potentially including the TTIC or the JTTFs, established by the Secretary after the date of this Agreement.

(iii) Analytic conclusions may be provided directly to such officials or to the public where the head of a covered entity or his or her designee reasonably determines that exigent circumstances exist such that providing an analytic conclusion prior to required approval is necessary to prevent, preempt, or disrupt an imminent threat of death or serious bodily injury or significant damage to U.S. infrastructure or other interests. In the event an analytic conclusion is disseminated pursuant to the exigent circumstances exception in this paragraph,

the Secretary and other covered entities shall be notified immediately of the dissemination.

(iv) Analytic conclusions may be shared with federal, state, and local law enforcement officials without the prior approval of the Secretary of Homeland Security, *provided, however*, that it is the intention of the parties that DHS be provided with the earliest possible advance notice of the potential of such communications and, where possible, DHS will be included in the development of the communications through the DHS liaisons at FBI Headquarters. The Secretary of Homeland Security, or his designee (including a DHS representative to a JTTF if designated by the Secretary to do so), must approve further dissemination of such analytic conclusions to other non-law enforcement state and local officials or to the public.

(v) Nothing in this Agreement shall prevent covered entities from coordinating on analytic conclusions with, or seeking the views of, other Federal Government entities in evaluating terrorism or other homeland-security-related information.

(c) *Establishment of Mechanisms for Operational Coordination and Deconfliction.* As soon as practicable, the parties shall agree upon specific mechanisms, including technical, administrative, and, as appropriate, designation of focal points, to maximize the effectiveness of operational coordination and deconfliction. These will cover both overseas and domestic operations related to homeland security. Subsequent agreements for operational coordination and deconfliction may be reached upon the approval of the parties or their designees.

(d) *Information Sharing Dispute Resolution.* Consistent with the DHS Legislation and other relevant statutory authorities, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, the obligation to protect intelligence or sensitive law enforcement sources and methods from unauthorized disclosure, and with Section 3(a), and other relevant sections of this Agreement, issues concerning the application of the terms of this Agreement in any specific context with respect to whether particular covered information should be provided to the Department or to any other covered entity shall be handled under the following procedures:

(i) A holder of particular covered information at issue, whether within or outside the entity originating that information, shall refer the matter by the most expeditious means to the head of the entity originating the information (or that official's designee) for expeditious review.

(ii) The reviewing official shall, without exception, render a definitive decision on the request within 24 hours of receiving the referral and, in light of the access provisions in the DHS Legislation, shall resolve any doubt in favor of



providing the requested information.

(iii) If the originating agency's reviewing official declines to provide the covered information requested, that official shall, within the 24 hours allotted for response, provide the Department or other covered entity with --

- (A) the fact that the specific information is being withheld;
- (B) a succinct and specific statement of the reasons for the withholding; and
- (C) as much of the information requested as the head of the originating agency (or that official's designee) reasonably concludes can be provided given the President's announced policies for protecting against terrorist threats to the homeland, the DHS Legislation and other relevant statutory authorities, and relevant Presidential Directives.

(iv) If, at that point, a compromise is not reached expeditiously, the dispute will be resolved either by the Secretary, Attorney General, and DCI by mutual decision or through referral to the Assistant to the President for National Security Affairs and Assistant to the President for Homeland Security Affairs, or their designees, for resolution. Notwithstanding any other provision of this Agreement, the Attorney General, Secretary, or DCI, or their deputies may, whenever any of them deems it necessary or advisable (particularly when a fundamental matter of policy is implicated or time is of the essence), intervene to raise and resolve any issue of access to covered information by mutual decision or through the National Security Council and/or Homeland Security Council system.

(e) *NSPD-8*. Nothing in this Agreement in any way affects the responsibilities and authorities for coordination of United States counter-terrorism activities established in National Security Presidential Directive (NSPD) 8.

5. Protection of Intelligence and Sensitive Law Enforcement Sources and Methods. The parties intend that all provisions of this Agreement be interpreted consistently with the DCI's statutory responsibility to protect intelligence sources and methods from unauthorized disclosure and with similar responsibilities of the Attorney General and the Secretary to protect sensitive law enforcement sources and methods, with the DHS Legislation and other relevant statutory authorities, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, and with Section 3(a), and other relevant provisions of this Agreement. Consistent with this agreed-upon interpretation:

(a) The DCI shall carry out his responsibilities for the protection of intelligence sources and methods, and the Secretary and Attorney General shall carry out analogous responsibilities for sensitive law enforcement sources and methods, in a manner, and through mechanisms, that ensure that all covered information is made available promptly to the Department, and to other covered entities with a need-to-know and proper security clearances and handling procedures in place, subject only to such handling and use restrictions as are strictly and unavoidably necessary to protect

intelligence and sensitive law enforcement sources and methods from unauthorized disclosure.

(i) The DCI shall ensure that the substance of all covered information relevant to the responsibilities of all covered entities is provided to those entities in a form suited to their effective use of that information, consistent with the DCI's obligation to protect intelligence sources and methods from unauthorized disclosure and Section 3(a) of this Agreement. The Secretary and the Attorney General shall similarly ensure that the substance of covered information is provided in a suitable form.

(ii) The DCI shall ensure that dissemination of classified reporting based, wholly or in part, on covered information is accompanied by dissemination of as much of that reporting and covered information as is possible at an unclassified (which may, when necessary, be marked "Sensitive-but-Unclassified" or "SBU") or reduced classification level, in order to ensure the broadest possible availability and use of covered information by those with a need-to-know that information (or information relating to that subject matter), based on a broad interpretation of the mission of the other covered entity. The Secretary and the Attorney General shall similarly ensure that dissemination is done in a manner that ensures the broadest possible availability.

(b) Information may be redacted or put into a tailored product to the extent consistent with Section 3(i) of this Agreement.

(c) Nothing in this section relieves any member of the Intelligence Community that originates covered information from its obligation to provide that information to DHS and other covered entities, as appropriate, in a form consistent with this Agreement, the DHS Legislation, and other relevant statutes and authorities regarding the protection of sources and methods.

6. "Sanitization" and Modification of Classification Levels for Further Sharing by DHS.

(a) Consistent with the President's announced policies, our national priorities, including this section, Section 3(a), and other relevant provisions of this Agreement, the DHS Legislation and other relevant statutes and Presidential Directives, covered entities that originate covered information that is classified shall retain the authority to determine whether that information, or any portions thereof, must remain classified in the interest of national security.

(i) Covered entities shall ensure that covered information that is classified or otherwise subject to restricted dissemination, but which reasonably appears likely to require onward passage to state, local, or private sector officials, the public, or other law enforcement officials for use in a criminal investigation, reaches DHS promptly with accompanying high-content "tear lines" suitable for onward passage at an unclassified level. Until this can be achieved

simultaneously to the transmission of covered information, the development of such tearlines shall not delay the provision of covered information.

(ii) The parties shall ensure, to the greatest extent possible, that covered entities utilize agreed-upon standardized formatting for preparation of tear-line material for passage to state, local, or private sector officials, including state and local law enforcement officials for use in a law enforcement investigation, or to the public, with the goal of providing necessary substantive information, but not enabling recipients to determine the originator, within the Federal government, of the information.

(b) DHS may, on its own initiative or at the request of a homeland security official to whom covered information is disseminated, ask that the originating agency declassify or reduce the classification level attached to that information in order to permit dissemination to additional officials who have a need-to-know the information, to promote ease of handling by those authorized to review it, to permit its incorporation into a document that is unclassified or classified at a lower level, or for other purposes consistent with the need promptly to provide homeland security officials with all relevant covered information that they have a need-to-know in the conduct of their official duties. Whenever it receives such a request, the originating agency shall respond to DHS, within 24 hours (or such longer period as is agreed to by all parties), unless compelling circumstances exist to require a longer response time. Such response will either --

(i) agree to declassify or reduce the classification level of the covered information in question as requested; or

(ii) provide an alternative formulation responsive to the requester's need for additional information sharing, but without declassifying or reducing the classification of the original document or covered information where that cannot be done consistent with assuring the national security.

(c) Where the need by DHS for further dissemination of classified information received from other covered entities, including through declassification or the preparation of unclassified tear-lines, is urgent because that information contains or may contain terrorist threat indications critical to the ability of homeland security officials to prevent, preempt, or disrupt a possible terrorist attack, that information may be passed directly to the entity or official that has a need-to-know that information, *provided that* the covered entity passing the information first notifies the originating agency and takes steps reasonable under the exigent circumstances to protect whatever classified information is not essential to initiating the urgent homeland security assurance measures that may be required.

(d) The parties agree to develop together, as soon as practicable, mechanisms and procedures, including through the use of detailees and assignees to the TTIC and JTTFs, as appropriate, to carry out the provisions of Section 6. The parties agree to work

together to ensure that the administrative, financial, and personnel burdens of this section are shared to the greatest extent possible among covered entities.

7. Detail or Assignment of Personnel. To facilitate the information sharing, coordination, and deconfliction policies covered in this Agreement, covered entities shall detail, and/or assign, to the greatest extent possible, including to the TTIC and/or JTTFs, personnel who have the authority either to make classification review and redaction decisions themselves, or, consistent with the time frames established in this Agreement, to refer those decisions to the appropriate officials at the originating agency for prompt action.

8. DHS Participation in Requirements Processes. As soon as practicable, the parties shall modify existing mechanisms and processes for prioritization of terrorism, WMD and other relevant foreign intelligence collection (including within the United States) and requirements processes to ensure that DHS has meaningful participation at each stage and level of each such mechanism or process, including through participation in the TTIC. The parties also shall work together to provide recommendations as to whether, and how, processes or mechanisms for purely "domestic" terrorism (e.g., concerning the capabilities, plans and intentions of exclusively domestic white supremacist or militia groups), and other relevant intelligence collection should be created or, alternatively, how to ensure meaningful participation by DHS in the prioritization for gathering such information. This section does not refer to operational activities.

9. Databases. The parties agree to establish procedures and mechanisms to provide DHS, and, as appropriate and practicable, other covered entities, with access to databases containing covered information. To this end, the parties shall establish a working group within 30 days of the date of this Agreement. Developed procedures and mechanisms, including through the use of the TTIC and/or JTTFs, should be consistent with the DHS Legislation and other relevant statutory authorities, Presidential Directives, the President's announced policies for protecting against terrorist threats to the homeland, and the appropriate needs for access by DHS to appropriate databases, as well as with the protection of intelligence or sensitive law enforcement sources and methods, and with Section 3(a) and other provisions of this Agreement. Such procedures and mechanisms should facilitate, to the greatest possible extent: ease and speed of information exchange; differentiated access, to allow individuals with different levels of security clearance and need-to-know to have different levels of access to databases; and compatibility with other databases of covered entities.

10. Statement of Intent Concerning Information Technology. It is the intent of the parties to build and modernize all relevant databases and other information technology systems in order to maximize compatibility with other systems with which they must interact. Such procedures and mechanisms also must comply with existing statutory and Presidential Directives, including with regard to the protection of classified information and applicable privacy protections.

11. Handling and Storage. The parties shall ensure that covered entities within their jurisdiction observe the established handling and storage standards appropriate to the classification and access restrictions indicated on covered information they receive, use, and

disseminate, subject only to the provisions of this Agreement pertaining to exigent circumstances.

12. Information collected and shared by foreign governments. This Agreement contemplates a separate Memorandum of Understanding, consistent with this Agreement, being agreed to by the parties, that addresses concerns related to information collected and shared by foreign governments.

13. Implementation.

(a) Each of the parties shall implement their responsibilities under this Agreement as to the covered entities under their jurisdiction through such binding regulations, orders, directives, and guidance as necessary or prudent from time to time.

(b) Any authority or duty assigned herein to the Attorney General, the Secretary, or the DCI, may be delegated to one or more subordinate officials at the discretion of the official to whom the authority or duty is assigned, except as otherwise provided in this Agreement. Each such delegation shall be promptly communicated to all other parties.

14. No Private Rights Created. These procedures are not intended to and do not create any rights, privileges, or benefits, substantive or procedural, enforceable by any individual or organization against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

15. Counterpart Signatures. This Agreement may be signed in counterparts, each of which shall be considered to be an original.

\_\_\_\_\_  
Attorney General

3-4-03  
Date

\_\_\_\_\_  
Director of Central Intelligence

\_\_\_\_\_  
Date

\_\_\_\_\_  
Secretary of Homeland Security

Feb. 28, 2003  
Date