Guideline 4 – Facilitate Information Sharing Between Executive Departments and Agencies and Foreign Partners

Introduction

Mandate and Process

In a "Memorandum for the Heads of Executive Departments and Agencies" dated December 16, 2005, the President directed that the Secretary of State, in coordination with the Secretaries of Defense, the Treasury, Commerce, and Homeland Security, the Attorney General, and the Director of National Intelligence (DNI) "review existing authorities and submit to the President for approval, through the APHS-CT [Assistant to the President for Homeland Security and Counterterrorism] and the APNSA [Assistant to the President for National Security Affairs], recommendations for appropriate legislative, administrative, and policy changes to facilitate the sharing of terrorism information with foreign governments and allies, except for those activities conducted pursuant to sections 102A(k), 104A(f), and 119(f)(1)(E) of the National Security Act of 1947."

In anticipation of this Presidential directive, the Department of State established the Foreign Government Information Sharing Working Group in late 2005. The Working Group met over the course of the next five months. In view of Executive Order 13388 and section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (PL 108-458) (IRTPA), and as agreed with the Program Manager for the Information Sharing Environment (PM-ISE), this Working Group Report is being submitted through the Information Sharing Council (ISC).

The Nature and Scope of Terrorism Information Sharing with Foreign Partners

Given the Working Group's mandate, this Report assumes as its general context that terrorism information sharing is generally desirable and focuses primarily on how to facilitate information sharing within the relevant context while noting a number of the risks associated with information sharing between foreign partners and entities within and outside the U.S. Government.

For purposes of this Report, the term "foreign governments" will be used as a general term referring to foreign governments and their sub-components, such as individual ministries or foreign State and local authorities. While the Report focuses in particular on foreign governments, however, the same conclusions and recommendations are generally applicable to other foreign information sharing partners. Such foreign partners include, for example, regional inter-governmental organizations such as the European Union (EU), international organizations composed of governments such as the

United Nations (UN) and the International Criminal Police Organization (INTERPOL), certain other entities with recognized comparable international status such as the International Committee of the Red Cross (ICRC), and even certain foreign private entities such as port operators, foreign airlines, and other logistics providers.

Information sharing with foreign partners that is relevant for counterterrorism purposes includes classified and also sensitive diplomatic, military, law enforcement, and homeland security information that is directly related to terrorists and terrorism; it also may include such information as is necessary for screening purposes and information that may be linked to terrorism at some future time: for example, general visa information and information regarding lost and stolen passports, weapons of mass destruction, suspect financial transactions, and serious criminal offenses committed by individuals who are not known to be terrorists. The term "terrorism information" is defined in section 1016(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-408), as referring generally to information concerning persons who are known or suspected to be, or have links to, terrorists, as well as information concerning actual or potential terrorist activities and threats. The term "secondary information," on the other hand, will be used to refer to other information (lawfully collected for specific authorized purposes) that may be relevant for specific counterterrorism purposes, such as lost and stolen passport information that may be used for screening purposes, or information regarding persons or facilities that subsequently are linked to specific terrorist threats. In this Report, however, the term "terrorism information sharing" may also be used as a more general term to refer to information sharing for counterterrorism purposes.

In what follows, the variety of information provided by foreign governments and other foreign partners will be referred to generally, for the sake of simplicity, as "foreign government information," except where otherwise noted or where the context clearly dictates otherwise.

Foreign government information sharing arrangements will vary in nature. There are numerous treaties and other formal international agreements that either directly concern or may be relevant to sharing information for counterterrorism purposes. In addition to legally binding international agreements there are also Memoranda of Understanding between governments that are not legally binding but are relatively detailed arrangements that support information sharing. In addition to government-to-government agreements, particular government ministries or departments may also have "counterpart agreements" of a more or less formal nature. When the foreign partner is a foreign private entity, in addition to any agreement with that entity, an agreement or understanding with the relevant foreign government may also be required.

Increasingly, international agreements are being negotiated for specific homeland security and counterterrorism purposes to support the war on terrorism. The Department of Homeland Security (DHS) led negotiations with the European Union in 2004 on airline passenger name record (PNR) data used in border security counterterrorism screening. A program on exchange of lost and stolen passport information also began recently between the United States and Australia; this has expanded to include New Zealand. Discussions are also underway under the auspices of the Asian-Pacific Economic Cooperation (APEC) on arrangements to facilitate the exchange of lost and stolen passport data among APEC economies. Pursuant to Homeland Security Presidential Directive-6 (HSPD-6), the Department of State is leading an interagency initiative to negotiate international agreements on sharing terrorist lookout information. In addition, the Department of Homeland Security has nascent efforts underway to promote exchanges of biometric and associated biographical information with selected foreign governments.

In this Report, the term "agreement" is used to refer to the various forms of agreements and arrangements for which there is a governing written procedure, whether or not legally binding. There are also informal information sharing relationships at the interpersonal level, typically among counterpart government officials and depending on personal knowledge and trust; such relationships are not reflected in any written agreement. Such informal information sharing relationships are particularly important in the law enforcement context, but such informal sharing can also be important in the diplomatic, defense, homeland security, and other contexts.

For analytic purposes, the Working Group separately considered the problems and issues with respect to the provision of information by foreign partners, on the one hand and, on the other hand, with respect to the sharing of information by the United States. As noted repeatedly during the Working Group discussions, however, the concept of "reciprocity," which is fundamental to international relations generally, is also a governing norm in information sharing relationships, be they formal international agreements or informal, interpersonal relations. In the international context, information sharing can never be regarded as a "one-way street." Whatever we ask for and expect from foreign governments, they will likely ask for and expect from us. Conversely, what foreign governments ask from us, they should also be prepared to give.

I. Obtaining Information from Foreign Governments

Foreign Government Conditions for Information Sharing: Maintaining Confidentiality

Much of the information shared in the terrorism context is either classified information or is sensitive for other reasons, e.g. privacy, homeland security, or law enforcement information. Therefore a condition for terrorism information sharing is that the information will be protected from unauthorized public disclosure unless permission is granted by the originating government for its release. (Issues associated with other kinds of restrictions on dissemination and use are addressed in the next section.) In addition, for information provided "off the record" or informally by individual sources, it can be equally if not more important to protect not only the information but also the source.

The United States and foreign governments will therefore include appropriate security assurances and protections for the protection of classified information and sensitive information in any international agreements, consistent with their respective laws and regulations. The ability of the United States to protect foreign government information under domestic law depends on the application of the relevant rules for classification of information pursuant to Executive Order 12958, as amended; the requirements for mandatory release of information pursuant to the Freedom of Information Act (FOIA), the Privacy Act of 1974, or court order; and for protection or privilege as recognized in various statutes, court rules of procedure, and evidentiary privileges for various specific types of information.

It is vital to be able to share relevant information within the U.S. Government and with other domestic and foreign partners for counterterrorism purposes. It is important therefore to minimize wherever possible any restrictions on handling and safeguarding that impede sharing, particularly when the restrictions are not necessary to meet foreign government requirements.

Much of the terrorism information provided by foreign governments will be classified pursuant to Executive Order 12958, as amended by Executive Order 13292 ("the Executive Order"). Under the Executive Order, foreign government information will be regarded as U.S. classified information when it is received or generated under a treaty or international agreement that so provides, or when a decision is made by a U.S. original classification authority that it meets the standards for classification, e.g., that its unauthorized disclosure reasonably could be expected to cause the requisite degree of damage to the national security of the United States. As specified in section 1.1 of the Order, this decision benefits from a presumption that the unauthorized disclosure of information provided in confidence by a foreign government or international organization causes damage to the national security.

When foreign government information is classified pursuant to the Executive Order, the ability to share information can significantly depend on the applicable requirements for safeguarding and access. The normal rules governing protection of U.S. classified information ("Confidential," "Secret," and "Top Secret" information) typically require, for example, segregation of information in separate electronic systems or classified areas and access is generally limited to those with security clearances.

In some cases, the foreign government may in fact want the full panoply of U.S. restrictions to apply, but in other cases they may be willing to accept more flexible handling. Some foreign governments and international organizations, for example, have a classification category of "restricted" information which is similar to U.S. "For Official Use Only" (FOUO) or "Sensitive But Unclassified" (SBU). In these cases, classification even as "Confidential" may restrict the sharing of information much more than is really required. In other cases, the foreign government may be willing to agree to more flexible handling than their own classification regimes would normally require. Foreign governments and international organizations may also provide information to the U.S. Government "in confidence" that is not classified under their systems, but still require that the information be protected from disclosure to the public. In such cases, the U.S. may have to classify it in order to provide adequate protection under U.S. law.

Under Executive Order 12958 and Information Security Oversight Office (ISOO) Directive No. 1 access and handling rules can be modified in appropriate circumstances to permit more flexible handling and access rules. Possible modified handling regimes can include, for example, disseminating information over encrypted unclassified systems (or even unencrypted) rather than requiring it to be segregated on a classified systems, or permission to share with other government officials who don't have security clearances but do have a "need to know." Use of modified handling regimes whenever possible consistent with foreign government requirements can therefore facilitate terrorism information sharing.

It is obviously easiest to share foreign government information within the U.S. Government and with domestic partners when the foreign government information can be adequately protected without classifying it at all. However, the ability of the United States to protect unclassified information depends on a multiplicity of statutes, privileges, and exemptions. These typically are narrower and more specific, focusing on one type of information or even one specific agency. The problems and confusions created by the multiplicity of U.S. statutes, rules, and regulations on the handling and safeguarding of SBU or Controlled Unclassified Information (CUI) and how they are applied in various governmental agencies can make it difficult to adequately protect foreign government information. A single type of information from a single source may be treated in different ways by different agencies. This potential diversity of treatment

is particularly problematic when information is sought to be pooled in a single Information Sharing Environment (ISE).

The multiplicity of foreign government rules and systems for classification and protection of their own information is also an issue. There are some 188 countries with which the United States has diplomatic relations, each of which has its own separate regime, in addition to the various international organizations such as the United Nations and NATO that have formalized classification regimes. These various regimes range from relatively simple and rudimentary systems to fairly elaborate sets of rules that may include such details as technical requirements for database storage and encryption. Some agencies – most notably the Department of Defense – have considerable expertise regarding foreign marking and handling regimes. The DNI Controlled Access Program Coordination Office (CAPCO) provides a single source of information on marking requirements that can be shared with the community at large provided that they have access to classified networks. Many U.S. Government organizations, however, may not have access to the classified systems necessary to access this database. This can create considerable confusion and complications in the handling of foreign government and international organization information—including the electronic handling of such information in an ISE.

Conclusions and Recommendations:

The Working Group concluded that improvements can be made in the area of protecting foreign government information from unauthorized public disclosure. At present foreign government information may in some cases be subjected to greater restrictions on handling and dissemination than are actually required to meet foreign government expectations and requirements. The complexity and diversity of the U.S. legal rules governing unclassified information may also be an impediment, and may lead to the same type of information from the same source having to be handled in different ways by different U.S. agencies. The multiplicity of foreign government classification regimes and requirements may also be an impediment that could be overcome with awareness training and a database that is accessible to the community at large.

Recommendations:

1. There should be a review under ISOO auspices of ISOO Directive No. 1, to determine what could be accomplished to encourage more flexible handling and dissemination of foreign government information where appropriate. ISOO advised the Working Group that it has already formed an interagency working group to undertake this review and update. It was noted that this effort will be coordinated with the Classification Management Working Group.

2. The Foreign Government Information Sharing Working Group should develop model or illustrative U.S. texts on information sharing and protection that can be used in international agreements pertaining to terrorism information sharing in order to facilitate agreement on a level of protection that would not unnecessarily impede redissemination for counterterrorism purposes. Such model or illustrative texts could also establish or encourage a "tear line" approach to maximize the distribution of information shared under the agreement.

3. Statutory language may be necessary in order to provide a greater level of protection for foreign government information in the ISE. After work on Presidential Guideline 3 is completed, further consideration should be given to whether additional statutory protection for foreign government information is feasible and desirable, either in general or as specifically related to terrorism and the ISE. While statutory protection offers a relatively straightforward way to provide protection to foreign government nonpublic information, the feasibility, advantages and disadvantages, and precise form of such legislation would require further consideration. Options might include, for example, (a) legislation protecting foreign government information generally (e.g., like 10 USC § 130c, which generally authorizes the Department of Defense and certain others to withhold foreign government information provided in confidence from public disclosure), (b) legislation protecting foreign government information specifically in the context of terrorism information sharing, or (c) legislation that would authorize agencies to afford protections pursuant to specific types of information sharing agreements. The ability of Federal agencies to protect foreign government information from public release under the FOIA under current law would need to be considered as well. Consideration of possible legislation should also take into consideration the views and conclusions of other working groups, especially the SBU Working Group, as it might be desirable to consider legislation focusing on information in the ISE more generally, not limited to foreign government information.

4. A central, electronically accessible repository of information on foreign government and international organization marking and handling regimes should be developed so that U.S. agencies and domestic partners can more readily understand the safeguarding and handling rules for different kinds of foreign government information, when the U.S. has undertaken to follow these rules. Most simply, this can consist of links to existing information, e.g., as maintained by the Department of State, Department of Defense, or CAPCO. A more elaborate option would be a web portal where foreign governments

themselves could upload their relevant information. Such a repository can also be part of a more general electronic resource on foreign government information.

5. Appropriate common standards or protocols for electronic handling of foreign government information within the ISE should be developed in order to ensure that any necessary foreign government requirements are respected. This would include the implications of such requirements for the inclusion of foreign government information in the ISE. For example, will an Information Sharing Environment have the capacity to implement the diversity of foreign government regimes? Or should there simply be some uniform marker or markers to flag some or all non-public foreign government information (e.g., that does not conform to a standardized regime or regimes) and to direct users where necessary to an appropriate agency contact? As part of this inquiry, the nature and implications of any specific foreign government technological or information technology (IT) security requirements for handling electronic information should also be further explored.

6. Departments and agencies should give consideration to the feasibility of multilateral efforts to encourage standardization of technological and substantive marking and handling standards. While it would be undesirable to seek a binding international agreement on standards, since this would likely require the United States as well as other countries to change their current standards, efforts taking the form of guidelines or "best practices" can be useful. Any initiative in this area should be carried out in a forum, such as the G-8, where the participants are experts in the precise subject matter. Any such efforts must also take account of the different categories of relevant information, e.g., law enforcement and border security information as well as defense information.

Foreign Government Conditions for Information Sharing: Other Restrictions on Dissemination and Use

In addition to the basic requirement that information provided in confidence not be publicly disclosed except as authorized, foreign governments may seek to impose other, more stringent restrictions on the dissemination or use of information those governments provide to the United States. It may be necessary, as a practical matter, to be willing to accept some limitations as a condition of receiving information from foreign governments. However, some restrictions are unacceptable, such that the United States would forgo receiving the information or entering into an information sharing agreement, rather than agree to the restrictions.

Many existing agreements already contain such restrictions. Many existing Mutual Legal Assistance Treaties, for example, provide that no information or evidence obtained

pursuant to the treaty will be used or disclosed "for any purposes other than for the proceedings stated in the request without the prior consent of the Requested Party." Numerous other agreements similarly provide that information exchanged pursuant to the agreement should be used for only the purposes specified in the agreement.

Restrictions on dissemination and use of information provided by foreign governments have also been an issue in the context of current efforts to negotiate new agreements on terrorism information sharing. The countries of the European Union are perhaps the most significant example. All EU Member States are signatories to the European Convention on Human Rights, in which Article 8 provides the right to respect a person's private life and correspondence. The European Court of Human Rights has given this article broad interpretation. Many Member States have the right to privacy in their constitutions, and all have Data Protection Authorities, which monitor data protection and data privacy in their states. All EU Member States are also bound by Directive 95/46/EC on the Protection of Personal Data. The directive allows processing of personal data if certain conditions are met: the data subject is informed and consents, it is necessary to enter/perform a contract, to protect the subject's vital interests, or to perform a task in the public interest. The data subject has the right to access the data and demand rectification/deletion of inaccurate data, or data not being processed in accordance with data protection rules. Directive 95 also prohibits transferring EU data to non-EU countries determined to have inadequate data protection frameworks. This Directive, however, defers to member states the regulation of personal data in the law enforcement context, with the result that national rules vary considerably. The European Commission currently is considering a draft Framework Decision, expected to be adopted in 2007, which would harmonize practice among the member states in the law enforcement area generally along the lines of Directive 95. It currently is unclear to what extent the Framework Decision would regulate information-sharing with third countries, and, if so, how restrictively, but it is likely to entail scrutiny of the adequacy of their national data protection regimes.

As discussed below in connection with sharing of U.S. person information, it is not only the foreign partners but also the United States that will want to include such restrictions in information sharing agreements, not only to protect confidential and other non-public information but also to protect U.S. persons and U.S. person information. Since provisions in international agreements are reciprocal in nature, any provisions necessary to protect U.S. persons and information will also permit foreign governments to impose restrictions on the information they provide.

The nature and extent of the restrictions that a foreign government will want to impose will likely vary depending on the context. The EU and foreign governments as well are particularly concerned that information provided regarding "innocent" persons is

strictly protected, e.g., databases regarding larger pools of persons for screening purposes, particularly with respect to their own nationals. This concern extends not only to whether the information will be shared at all, but also to how the information, if shared, will be disseminated and protected. Foreign governments will likely want to limit the use that may be made of such information. For example, foreign governments have repeatedly said, in different contexts, that they do not want information regarding their nationals to be used as a basis for inclusion on the "no fly" list.

If, on the other hand, there is reason to suspect an individual of terrorism or criminal wrongdoing, there is likely to be lesser concern regarding information sharing per se. However, there may still be significant concerns if the information is made public, as this may compromise other equities, such as law enforcement investigations or intelligence sources and methods. For the same reasons, foreign governments may want to restrict the permissible uses of the information in order to avoid any use that will alert the individual in question that they are under suspicion.

Foreign government restrictions on the dissemination and use of information present a number of difficult issues. One is simply keeping track of these various restrictions. A further complication in this regard is that information may be obtained from multiple sources. Information obtained from country X may be subject to restrictions, but the same information may be obtained from Country Y without restriction. It then becomes necessary not only to know the source of specific pieces of information, but also to be able to cross-check whether the same information is also available from another source, and to defend a disclosure, if necessary, to Country X.

A second issue concerns the acceptability of foreign government restrictions, given the overall need and mandate to share terrorism information. It is important to bear in mind that, as noted in the introduction, not all information provided by foreign governments in the context of terrorism information sharing is necessarily "terrorism information" as defined in IRTPA. As a legal matter, not all limitations on the *use* of information that foreign governments provide are necessarily inconsistent with Executive Order 13388. The Order requires that terrorism information be disseminated to Federal agencies, consistent with agency responsibilities, Attorney General guidance, and applicable law. It does not, however, necessarily preclude foreign governments imposing certain restrictions on the use of such information, e.g., that certain information not be used for "no fly" purposes or that in some cases no action be taken so as not to alert a suspect to law enforcement interest or to protect sources and methods. Thus, as a legal matter the Executive Order is consistent with the kind of approach that has been discussed and it therefore is not necessary to recommend any amendment in order to facilitate information-sharing with foreign partners. The acceptability of such restrictions in any given case, however, would have to be judged as a policy matter,

bearing in mind that the United States itself would want to impose some use restrictions in relation to U.S. person information.

Conclusions and Recommendations:

- The Working Group reached the following general conclusions regarding the acceptability of foreign government restrictions on dissemination and use of information:

  - Not all use limitations are inconsistent with Executive Order 13388. Thus, as a legal matter the Executive Order is consistent with the kinds of use restrictions that are generally important to foreign governments and it therefore is not necessary to recommend any amendment in order to facilitate information-sharing with foreign partners. The acceptability of such restrictions in any given case would have to be judged as a policy matter, bearing in mind that the United States itself would want to impose some use restrictions in relation to U.S. person information provided to foreign governments. In general, the key is to ensure that information can be disseminated and used for critical counterterrorism purposes, including threat analysis and dealing with specific threat situations.

  - Secondary information (e.g., regarding persons who are not suspected of terrorism and other information that is not relevant to terrorism but may later become relevant) may be segregated and more highly restricted, until such time as there is a triggering circumstance that establishes relevance.

  - Even with respect to information concerning persons suspected of involvement in terrorism it may be possible to consider accepting certain use limitations on a case-by-case basis, where national security considerations permit. For example, in some cases the United States as well as other countries may cooperate to investigate and resolve certain "hits" without alerting a suspect to the existence of derogatory information or the fact that he is under investigation.

Recommendations:

1. In designing the ISE, it should be assumed that, as a consequence of restrictions imposed by foreign governments on dissemination or use, some categories of information will not be directly incorporated within or immediately accessible through the ISE, but rather will be kept in separate, segregated databases until such time as the information becomes relevant to a permissible "use." The relevance determination will not and cannot be made electronically and automatically, but will require a human interface to make the requisite judgment.

2. It will also be necessary as part of the ISE to create a means to identify within the ISE not only what is foreign government information but also which government provided it and what restrictions it is subject to, and to accommodate the wide variety of foreign government restrictions on handling, dissemination, and use. This should take into account insofar as relevant the conclusions and recommendations resulting from the SBU Working Group as well as the relevant rules regarding the treatment of foreign government information pursuant to Executive Order 12958, as amended.

3. The Foreign Government Information Sharing Working Group should also develop model or illustrative texts that address the question of restrictions on dissemination and use for inclusion in international agreements.

4. Agencies involved in negotiating international agreements providing for information sharing must take into consideration the possible overlap among and conflict between the various provisions of different agreements with different countries. It would be a problem, for example, if the United States agreed with Country A that it would provide "all" information in a given area, while at the same time agreeing with Country B that it would not provide Country B information to Country A.

5. As an aid to identifying the above and other relevant issues, the Foreign Government Information Sharing Working Group should also develop a checklist of issues that need to be taken into account in negotiating international agreements.

II. Sharing U.S. Information with Foreign Governments

Sharing U.S. Person Information

Sharing information regarding U.S. citizens and permanent residents ("U.S. person information"), particularly if they are not suspected of being involved in terrorism or other crimes, is a sensitive area raising policy as well as legal concerns. The Privacy Act is particularly significant from a legal point of view, as it contains a number of protections for information concerning U.S. citizens and lawful permanent residents. These protections include a general prohibition on the disclosure of any information concerning an individual from a "system of records" (as defined by the Act) without the consent of the person to whom the record pertains, unless one of the Act's exceptions applies (see 5 USC §552a(b)). An electronic database or other set of records constitutes a "system of records" under the Privacy Act if information from the database is retrieved by the name or other personal identifier of a U.S. person (see 5 USC § 552a(a)(5)). (With respect to certain foreign intelligence and counterintelligence information, however, see section 203(d) of the USA Patriot Act, Public Law 107-56; 50 USC § 403-5d, and 50 USC § 401a(2) and (a)(5). This Report does not address the special rules and requirements specifically concerning the sharing of intelligence information.)

The Terrorist Screening Center (TSC) has identified the following specific concerns regarding the sharing of terrorist watchlist information, which are relevant also to sharing information in other contexts. Any decision to share U.S. person information should therefore bear these risks in mind, and appropriate controls and safeguards should be implemented wherever possible to mitigate these risks:

- U.S. Government terrorist watchlist information is not static; people are added to and removed from the watchlist every day. Unless appropriate controls are put in place, foreign governments could use old and invalid watchlist data against U.S. citizens who have since been cleared of involvement with terrorism and removed from the watchlist.

- U.S. Government terrorist watchlist information only provides other governments with limited biographic information (e.g., the "No-Fly" list contains only names and dates of birth), which is not always sufficient to avoid mis-identifying innocent persons as the person affiliated with terrorism. Access to other identifying data about the watchlist subject, which is held in the Terrorist Screening Data Base and other U.S. Government databases, is often necessary to avoid misidentifications; therefore, any sharing of watchlist information should also include a process to resolve whether the U.S. person encountered by the foreign government is actually the watchlist subject.

- Other countries' anti-terrorism laws might not provide an acceptable level of due process protections for U.S. persons. Sharing information with such countries poses the risk that U.S. Government information could be used to subject a U.S. person to treatment that the U.S. Government considers to be a violation of civil rights or simply unfair (e.g., detention without demonstrable cause, denial of access to legal counsel). Once a U.S. person is in the hands of a foreign legal system, the U.S. Government may have limited or no ability to influence their treatment or consequences.

- Without U.S. Government permission, foreign governments could further distribute U.S. person information to other countries (potentially including countries that the U.S. Government might never agree to share with directly), thereby exacerbating the problems listed above.

Given the concerns and risks involved, there has been reluctance to share U.S. person information with foreign governments in the HSPD-6 process. Foreign governments are often also reluctant to share screening information on their own nationals with the U.S. Government. At the same time, however, sharing U.S. person information with foreign governments may be necessary and appropriate in some circumstances. Such sharing may be important, for example, so that the foreign government will reciprocally share information on its own persons, so that the foreign government could develop further information of interest to us (e.g., encounter information) or to further common interests in prevention and prosecution. It was noted that the United States currently shares U.S. person information with certain foreign airlines and foreign governments in the "no fly" context, as the "no fly" list does not separately identify U.S. persons.

The initial step in sharing that presents the fewest risks is not to share identifying information in the first instance. This is exemplified by the sharing of lost and stolen passport information, where it is only the passport number and other non-personal information that is shared in the first instance. Another option is to have real-time querying against a watchlist database, to determine simply if there is a "hit". Work is also being done on techniques that can query for "hits" against watchlists while preserving the anonymity of individuals.

These approaches not only have the advantage of limiting dissemination of personal information, but also help to ensure that information is up to date. Providing for real-time contact between the United States and a foreign government at the moment of screening may also help to guard against foreign governments taking unanticipated or inappropriate actions based on information provided. However, in any case the question must be confronted: "Are we prepared to share follow-up data if there is a match?" The answer must be yes (provided there are sufficient safeguards for any personal

identifying information) in at least a sufficient number of cases for the arrangement to be of interest to a foreign government.

A positive "hit" is not generally useful unless there is a means to follow-up by sharing further information regarding the nature of and basis for the "hit." At a minimum, it is necessary to verify whether the individual of concern to one government is the same individual as appears in the other government's watchlist. In addition, typically there will be a desire to know the nature of the derogatory information involved. Many foreign governments are not interested in receiving our watchlist (which consists solely of identifying information) unless they also receive access to the back-up data. In part this is because the United States sets a relatively low threshold for watchlisting individuals, erring on the side of including rather than excluding individuals who may present a threat. Accordingly, without access to the backup information the foreign government cannot assess whether any particular action should be taken with respect to any particular individual.

Another aspect that warrants consideration is the subset of data that might be shared. In general, it appears that foreign governments are interested in a narrower subset of information, with a higher threshold for including any given individual. Consideration could also be given to agreeing with foreign governments on a standardized set of criteria to define subsets of information that might be shared for certain purposes. On the other hand, inclusion of more data can make it easier to screen hits.

In the case of certain subsets of information and information sharing contexts, the balance of risks and benefits weighed more strongly in favor of sharing. While one might be concerned about sharing U.S. person information for general screening purposes, the balance weighs more strongly in favor of sharing when there are specific grounds to believe that individuals are connected with terrorist organizations or terrorist activity, particularly in the context of cooperative arrangements for law enforcement, security, or other investigations. Even more weight would be given to sharing if information indicates an imminent hazard, in which case the information would be shared as appropriate even in the absence of any established information sharing arrangements.

Conclusions and Recommendations:

- The Working Group concluded that, in general, the question of sharing U.S. person information is the reverse side of the question of accepting foreign government restrictions on information that they provide. Given the governing norm of reciprocity, in developing information sharing relationships with foreign governments that contemplate sharing of information on individual persons, U.S. Government agencies need to be sensitive to the potential impact on U.S. persons

and the legal requirements of the Privacy Act. Therefore, agreements and arrangements will have to ensure protection of individual person information in a manner that is acceptable to both parties.

- With respect to specific approaches for ensuring appropriate privacy protection, the Working Group did not endorse the adoption of a more formalized system of "judging" countries such as is in effect for the EU. Rather, the preferred approach is to incorporate the necessary protections in governing agreements. While this still requires a threshold judgment that the foreign government, or the particular agency of the foreign government that is involved, will properly respect and implement the agreement, this is a more flexible approach that enables information sharing with a broader range of countries.

- Another useful approach is to establish a system whereby each party can only query another party's database, instead of providing data on all suspect individuals. This can be coupled with limitations on who can have access to the information and for what purpose. This approach may not be feasible in many countries, however, since few countries have the kind of sophisticated, centralized database that is required. Many, if not most, countries are in the same situation as the United States was prior to the creation of TSC, with multiple, separate, decentralized databases. In some cases, the necessary level of information technology may also be lacking.

- Another approach is to limit the subset of information that is shared to meet common agreed criteria, as a basis for specific agreed actions. For example, the U.S. may elect to only share U.S. person data where a certain threshold of evidence or information has been met, such as the issuance of a warrant.

- These different approaches are not mutually exclusive, and one or more of them could be used in any given case. In any case, a human interface is required to determine what information can be shared in a given case.

- Greater standardization or harmonization of international approaches could be useful, but efforts to develop precise standards or binding international agreements on a multilateral basis would likely not result in texts that would be acceptable to the United States or the foreign governments. Efforts to develop "best practices" and "protocols," on the other hand, could be useful. It was noted for example that the G-8 is developing a "Best Practices" paper on how to deal with persons who are found to be using lost or stolen passports. In addition, it is important to continue to follow developments within the EU.

Recommendations:

1. The conclusions of the Working Group need to be taken into account in the design of the ISE, and in particular the limitations on foreign government access to the ISE information and the need for a 24/7 human interface to make decisions regarding information sharing.

2. The Foreign Government Information Sharing Working Group, with appropriate participation of privacy officers and legal counsel, should develop model or illustrative provisions or checklists dealing with the privacy and related concerns involved in sharing information regarding individual persons in terrorism information sharing agreements. These can, as appropriate, draw from the Fair Information Practices (FIP), which serve as the basis for the U.S. Privacy Act and have long-standing international acceptance, e.g., the 1980 Guidelines in Protection of Privacy and Transborder Flows of Personal Data developed by the Organization for Economic Cooperation and Development (OECD Guidelines) and the 2004 APEC Privacy Framework. (The Privacy Act itself does not as a legal matter dictate the precise type and nature of protections that foreign governments would have to adhere to when information is shared with them pursuant to one of the exceptions to the general prohibition on disclosure. There are, however, relevant Privacy Act requirements that must be complied with, such as the requirement that when information has been passed to a foreign government and is later corrected, that correction must also be provided to the foreign governments that received the original information.)

3. All relevant agencies should ensure that when developing international agreements that involve sharing information on individual persons, the potential impact on U.S. persons is considered as a requirement of the authorization and negotiation process.

4. All relevant agencies should review their Privacy Act routine uses, Privacy Act notices and published systems of records descriptions to ensure that all relevant elements recognize and provide for sharing with foreign governments, as broadly defined in the Introduction to this Report.

5. Relevant law and guidance regarding information privacy rights must be reviewed to determine whether amendment or elaboration would be necessary to permit protection and sharing of U.S. person information.

6. The Foreign Government Information Sharing Working Group, with appropriate participation by privacy officers and legal counsel, should develop recommended texts for Privacy Act routine uses, Privacy Act notices, and

published records systems descriptions to permit appropriate sharing with foreign governments and other foreign partners for counterterrorism purposes. This should include, for example, a model routine use to permit necessary sharing with foreign governments, covering not only "terrorism information" but also "secondary information."

7. Relevant lead agencies working with multilateral fora, in coordination with the Program Manager and ISC and other relevant agencies, should encourage where appropriate multilateral efforts to develop "best practices" in appropriate contexts, including checklists and protocols on what to do if there is a "hit."

Sharing U.S. Classified Information

In many cases sharing U.S. classified information with foreign governments occurs in a relatively formal context. For example, the Department of Defense presently has 64 General Security Agreements with foreign governments that describe the agreed security requirements each government will use for the protection of classified military information provided to either party, as well as directives and instructions pertaining to the disclosure of classified military information to foreign governments and international organizations, and an International Security Programs directorate within the Office of the Under Secretary of Defense for Policy responsible for providing policy oversight on all matters relating to the disclosure of classified military information to foreign governments and international organizations. Disclosure authority has been delegated within the Department of Defense to Foreign Disclosure Officers to facilitate decisions on disclosure to foreign governments and international organizations in support of lawful and authorized U.S. Government purposes. The Intelligence Community (IC) similarly has a relatively formal structure in place. In other contexts, such as diplomacy and law enforcement, as well as sharing with allies in ongoing military operations, the context for sharing may be more fluid and ad hoc, depending on relationship and specific circumstances, and governed by more informal or implicit rules, although formal treaties such as mutual legal assistance treaties and police cooperation agreements or arrangements are also relevant with many countries. The context may also vary in that disclosure of information may be done orally, visually, or in documentary form.

Disclosure decisions may in some cases require informed and sophisticated judgments regarding the foreign government in question and the net impact on U.S. interests. In some contexts, such as diplomacy, disclosure decisions need to take into account such factors as the internal dynamics of the foreign government and the trustworthiness or specific agendas of the ministry or official who is receiving the information. Account may also have to be taken of actual or possible future political changes in foreign

governments that may affect the reliability of individual officers, departments, or entire governments as sharing governments.

Another possible consideration is the extent to which the information provided may subsequently be redisseminated beyond the original recipient, to others in the foreign government. In current practice, sharing typically occurs within a specific more limited community, such as the diplomatic community, IC, or law enforcement community. There is a mutual expectation that the information will be shared only with its intended recipients under specific explicit or implicit guidelines.

Another consideration in information sharing with foreign governments is the question of reciprocity or leverage, i.e., what does the United States get in return? In some cases, e.g., in case of apprehending criminals or dealing with imminent threat, sharing serves compelling mutual interests in apprehending criminals, preventing terrorist acts, and saving lives. In other cases, however, a foreign government may seek access to U.S. information while not being willing to give information in return; sharing in such case might depend on reciprocity. One criterion that must be satisfied when wishing to disclose U.S. information is that the disclosure will result in benefits to the United States at least equivalent to the value of the information disclosed.

As a consequence of the above and other factors, the decision whether, when, and with whom to share specific U.S. classified information may require a more nuanced judgment that takes into consideration not only the substance of the information but the political context, i.e., the impact of sharing with a specific individual in a specific foreign government on the achievement of U.S. objectives. While it is necessary in the terrorism information sharing area to move beyond informal rules and relationships to more institutionalized arrangements, this has to be done in a way that continues to maximize the positive impact on achieving U.S. objectives and does not have unintended consequences whereby foreign governments use the information in ways that are not anticipated or desired. Given the exigencies of sharing, however, particularly in operational contexts, the decision on approval to share must often be made quickly and on demand.

Conclusions and Recommendations:

- The Working Group concluded that the key area to facilitating the sharing of U.S. classified information related to terrorism is to institutionalize the ability to make disclosure decisions that are consistent with governing law and policy and U.S. national interests on a timely basis.

Recommendations:

1. Agencies should have systems of foreign disclosure officers or comparable systems in order to make and or expedite sharing decisions. In developing such systems, it would be useful to look at the Department of Defense and IC systems as an educational model.

2. Agencies should provide the necessary programs and information to support their disclosure officers: e.g., training on sharing with foreign governments, interagency contact persons who can provide necessary information, and web-based information resources.

3. Agencies should develop or review agency-specific written disclosure procedures on the release of classified information to foreign governments, including declassification where appropriate, in the terrorism information sharing context.

Sharing U.S. SBU/CUI Information

Much of what has been said above regarding sharing of classified information is applicable to sharing of U.S. Government SBU/CUI information as well. The picture is further complicated, however, by the fact that there are many different types of such information, subject to different rules. Sharing of visa information, for example, is subject to different rules than sharing of law enforcement information or sharing of information protected by the Privacy Act. Under current practice, these complications may have been somewhat mitigated by the fact that sharing often occurs between counterpart agencies – e.g., military to military, or law enforcement to law enforcement. It is not so much a problem, for example, to share information that is restricted to law enforcement purposes if you are sharing with another law enforcement agency. More institutionalized government-to-government arrangements for terrorism information sharing, however, are likely to exacerbate this problem. The situation is comparable to that of sharing with State, local, and tribal authorities, where the lack of clear and uniform rules governing SBU/CUI is a significant complicating factor. At the same time, however, it is important that overall efforts to harmonize and institutionalize terrorism information sharing rules not have the unintended consequence of disrupting existing informal, inter-personal information sharing relationships. As noted above, this is particularly prevalent in the law enforcement context but important as well in the diplomatic, military, and other contexts where U.S. government officials have established relationships with counterpart foreign officials.

Conclusions and Recommendations:

- The Working Group concluded that, while there is a need to simplify and expand permissible sharing of SBU information with foreign governments, the issues in

this regard are not unique to foreign governments but rather largely derive from the nature of the various agency regimes for handling this type of information. The work undertaken pursuant to Presidential Guideline 3 therefore should address this problem. One area, however, that is specific to foreign governments is the nature and extent of each agency's relevant statutory authorities.

Recommendations:

1. Work under Guideline 3 should take into account that the existing various SBU/CUI markings and requirements create confusion and difficulty for foreign partners and for U.S. agency decisions on when and to what extent terrorism information can be shared with foreign partners.

2. Agency heads should review their relevant authorities governing sharing of SBU/CUI information to make sure that they permit sharing relevant information with all varieties of foreign partners for counterterrorism purposes.

Handling of U.S. Information by Foreign Governments

Assessing a foreign government's willingness and ability to provide appropriate protections to U.S. information, once it is shared, requires an understanding of the foreign government's system and an assessment of its reliability as a sharing partner. Like the United States government, foreign governments may be required to disclose information under some circumstances by their domestic laws. A foreign government might have inadequate facilities to provide adequate protection, or they might in some case lack the political will to do so. It may not always be easy to determine whether a foreign government is or is not complying with undertakings regarding protection, nor are there many tools to enforce compliance, apart from refusing to provide information in the future.

In addition to protection, a number of other issues in relation to foreign government handling of U.S. information deserve mention. First, it must be borne in mind that the relevant "culture" that surrounds information sharing may be very different in any given foreign country. Foreign governments may also have other priorities that are in the domestic context more significant than terrorism, and will look at information sharing in that light. Even where the foreign government shares U.S. views and objectives with respect to counterterrorism, the concept of sharing may not be as well-developed, even within the government itself. Even in the United States, great strides have been made only in the past few years, since the September 11 attacks. Foreign government technology may also be a limitation. Particularly in less developed countries, the government may have the will but not the resources to participate in information sharing arrangements.

Conclusions and Recommendations:

- The Working Group concluded that it would facilitate terrorism information sharing if agencies had more information regarding the willingness and ability of foreign governments to ensure that U.S. information receives necessary protections.

Recommendations:

1. Agencies should develop and the ISE should include mechanisms to make information regarding foreign government protection of U.S. information more widely available. A number of agencies conduct security surveys to determine the capability of a foreign government to protect U.S. information provided to them. The Department of Defense in particular has an extensive program in place. The results of these surveys could be made more widely available in connection with the ISE. Consideration should also be given to whether existing survey programs could be expanded to greater coverage. Consideration should also be given to including other relevant information, such as agency experience with particular governments, departments, or officials. In developing such resources, it must be noted that the willingness and ability to protect information may vary not only among countries, but as between various subcomponents of foreign governments and even as between different foreign government officials. The back up resources mentioned above for disclosure officers (agency contacts, web portals, training) should also be designed to assist agencies in assessing the reliability of foreign governments, agencies, and individuals as sharing partners.

2. In developing a checklist and model or illustrative texts for international agreements, the Foreign Government Information Sharing Working Group should also address the possible inclusion of audit procedures in agreements.

3. Assistance should be given to foreign partners where needed to help them develop necessary capacities to protect, store, and share information. This would include, for example, basic information technology, communications, and safeguarding infrastructure, the development of centralized databases, and necessary training.