United States General Accounting Office

GAO

Report to Congressional Requesters

April 2003

INFORMATION TECHNOLOGY

Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing

GAO

Accountability ★ Integrity ★ Reliability

GAO

Accountability•Integrity•Reliability

Highlights

Highlights of GAO-03-322, a report to Congressional Requesters

April 2003

INFORMATION TECHNOLOGY

Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing

Why GAO Did This Study

Terrorist and criminal watch list systems—sometimes referred to as watchout, lookout, target, or tip-off systems—are important tools in controlling and protecting our nation's borders. The events of September 11, 2001, and other incidents since then, have highlighted the need to share these watch lists. In light of the importance of border security, GAO was asked to identify federal databases and systems that contain watch lists, the agencies that maintain and use them in protecting our nation's borders, the kind of data they contain, whether federal agencies are sharing information from these lists with each other and with state and local governments and private organizations, the structural characteristics of those lists that are automated, and whether opportunities exist to consolidate these watch lists.

What GAO Recommends

GAO recommends that the Secretary of DHS, in collaboration with the heads of the other departments and agencies that have and use watch lists, lead an effort to consolidate and standardize the federal government's watch list structures and policies. DHS and other departments involved in this study generally agreed with GAO's findings and recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-03-322.

To view the full report, including the scope and methodology, click on the link above. For more information, contact Randolph C. Hite at 202-512-3439 or hiter@gao.gov.

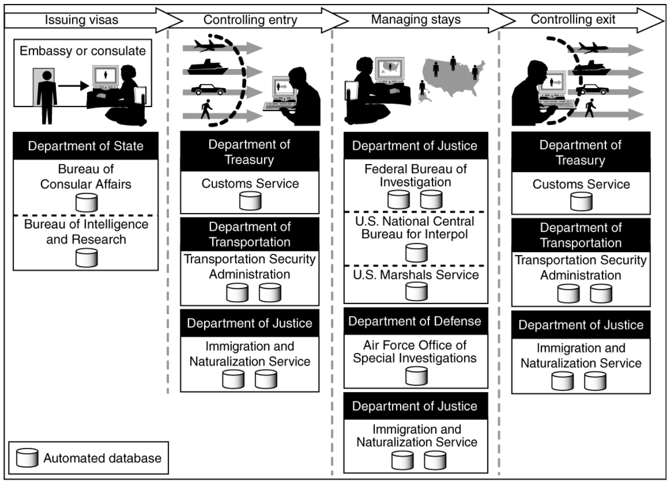
What GAO Found

Generally, the federal government's approach to using watch lists in performing its border security mission is decentralized and nonstandard, largely because these lists were developed in response to individual agencies' unique missions, including their respective legal, cultural, and systems environments. Specifically, as shown in the figure below, nine federal agencies—which prior to the creation of the Department of Homeland Security (DHS) spanned the Departments of Defense, Justice, State, Transportation, and the Treasury—develop and maintain 12 watch lists.

These lists include overlapping but not identical sets of data, and different policies and procedures govern whether and how these data are shared with others. As a general rule, this sharing is more likely to occur among federal agencies than between federal agencies and either state and local government agencies or private entities. Further, the extent to which such sharing is accomplished electronically is constrained by fundamental differences in the watch lists' systems architecture (that is, the hardware, software, network, and data characteristics of the systems).

Two agencies identified opportunities to standardize and consolidate these lists, which GAO believes would improve information sharing. The President's homeland security strategy further recognizes the need to address the proliferation of these lists. While the Office of Homeland Security was reportedly pursuing consolidation as part of an effort to develop a border and transportation security blueprint, referred to as an enterprise architecture, the DHS Chief Information Officer told us that the department had recently taken responsibility for the blueprint. However, we were not provided enough information to evaluate these efforts.

Simplified Diagram of Border Security Process and the Departments and Agencies That Use Watch Lists


Issuing visas
Controlling entry
Managing stays
Controlling exit
Embassy or consulate
Department of State
Bureau of Consular Affairs
Bureau of Intelligence and Research
Department of Treasury
Customs Service
Department of Transportation
Transportation Security Administration
Department of Justice
Immigration and Naturalization Service
Department of Justice
Federal Bureau of Investigation
U.S. National Central Bureau for Interpol
U.S. Marshals Service
Department of Defense
Air Force Office of Special Investigations
Department of Justice
Immigration and Naturalization Service
Department of Treasury
Customs Service
Department of Transportation
Transportation Security Administration
Department of Justice
Immigration and Naturalization Service
Automated database

Sources: GAO (data), Nova Development Corp. (images).

Note: The Transportation Security Administration, Customs, and Immigration and Naturalization Service and their associated databases appear multiple times because watch lists that are used in more than one phase of the process are shown in each phase.

Contents

Letter

Appendixes

Tables

Figures

Abbreviations

DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
INS	Immigration and Naturalization Service
TSA	Transportation Security Administration

G A O
Accountability ★ Integrity ★ Reliability

United States General Accounting Office
Washington, D.C. 20548

April 15, 2003

The Honorable Charles E. Grassley
Chairman
Committee on Finance
United States Senate

The Honorable Carl Levin
Select Committee on Intelligence
United States Senate

Terrorist and criminal watch list systems—sometimes referred to as watchout, lookout, target, or tip-off systems—are important tools in controlling and protecting our nation's borders. The events of September 11, 2001, and other incidents since then, have reinforced their importance and highlighted the need to share and use these lists. Because watch lists are important tools in border security, you requested that we identify

- federal databases and systems that contain watch lists, the agencies that maintain and use these watch lists in protecting our nation's borders, and the kinds of data these watch lists contain;
- whether federal agencies' sharing of watch list data is governed by policies and procedures;
- whether watch lists are (1) being exchanged among federal agencies and between federal agencies and state, local, and private organizations, and (2) supported by common system architectures (system hardware, software, and data characteristics); and
- whether opportunities exist for consolidating watch lists.

To address these objectives, using a questionnaire, we surveyed nine agencies that perform border security functions and that, according to our research, either develop or use watch lists. We did not independently verify agencies' responses. Details of our objectives, scope, and methodology are discussed in appendix I.

Results in Brief

Generally, the federal government's approach to developing and using terrorist and criminal watch lists in performing its border security mission is diffuse and nonstandard, largely because these lists were developed and have evolved in response to individual agencies' unique mission needs and the agencies' respective legal, cultural, and technological environments. More specifically, nine federal agencies[1]—which spanned the Departments of Defense, Justice, State, Transportation, and the Treasury—have developed and maintain 12 watch lists. These lists contain a wide variety of data; most contain biographical data, such as name and date of birth, and a few contain biometric[2] data, such as fingerprints. Beyond the nine agencies that have developed and maintain these watch lists, about 50 other federal agencies and many state and local government entities have access to one or more of these lists.

Nonstandardization also extends to the policies and procedures governing whether and how agencies share watch lists. Specifically, two of the nine federal agencies do not have such policies and procedures, and the remaining seven have differing ones. For example, one of the agencies' policies included guidance on sharing with other federal agencies as well as state and local governments, but another addressed sharing only with federal agencies. As a general rule, the federal agencies that have watch lists share the lists among themselves. However, half of these agencies share their respective lists with state and local agencies, and one-fourth share them with private entities. The extent to which such sharing is accomplished electronically is constrained by fundamental differences in watch list system architectures (that is, the hardware, software, network, and data characteristics of the systems).

The number and variability of federal watch lists, combined with the commonality of purpose of these lists, point to opportunities to consolidate and standardize them. Appropriately exploiting these opportunities offers certain advantages—such as faster access, reduced duplication, and increased consistency—which can reduce costs and improve data reliability. Some of the agencies that have developed and maintain watch lists acknowledged these opportunities, as does the President's homeland

[1] The nine agencies are the State Department's Bureau of Intelligence and Research and Bureau of Consular Affairs; the Justice Department's Federal Bureau of Investigation, Immigration and Naturalization Service, U.S. Marshals Service, and U.S. National Central Bureau for Interpol; the Department of Defense's Air Force Office of Special Investigations; the Transportation Department's Transportation Security Administration; and the Treasury Department's U.S. Customs Service. Of these, the Immigration and Naturalization Service, the Transportation Security Administration, and the U.S. Customs Service are being incorporated into the new Department of Homeland Security.

[2] Biometrics are records of physical identification marks, such as fingerprints and iris scans.

security strategy. To this end, Office of Homeland Security officials stated in public forums during the course of our review that watch list consolidation activities were under way as part of efforts to develop a set of integrated blueprints—commonly called an enterprise architecture[3]—for the new Department of Homeland Security (DHS). According to DHS's Chief Information Officer, responsibility for the consolidation effort has been transferred to DHS.

To strengthen our nation's homeland security capability, we are recommending that the Secretary of DHS take a series of steps aimed at ensuring that watch lists are appropriately and effectively standardized, consolidated, and shared. In commenting on a draft of this report, DHS—as well as other departments that develop and maintain watch lists and that commented on the draft—generally agreed with our findings and recommendations. Their comments are summarized and evaluated in the Agency Comments and Our Evaluation section of this report.

Background

The President's national strategy for homeland security and the Homeland Security Act of 2002[4] provide for securing our national borders against terrorists. Terrorist and criminal watch lists are important tools for accomplishing this end.

Simply stated, watch lists can be viewed as automated databases that are supported by certain analytical capabilities. To understand the current state of watch lists, and the possibilities for improving them, it is useful to view them within the context of such information technology management disciplines as database management and enterprise architecture management.

[3] An enterprise architecture can be viewed as a blueprint that describes an entity's operational and technical environments. The blueprint includes descriptive models of the entity's current and future business and technical environments, along with a roadmap for transitioning from the current to the future environment.

[4] P.L. 107-296.

Overview of the President's Homeland Security Strategy and the Homeland Security Act

Since the September 11th terrorist attacks, homeland security—including securing our nation's borders—has become a critical issue. To mobilize and organize our nation to secure the homeland from attack, the administration issued, in July 2002, a federal strategy for homeland security.[5] Subsequently, the Congress passed and the President signed the Homeland Security Act, which established DHS in January 2003. Among other things, the strategy provides for performance of six mission areas, each aligned with a strategic objective, and identifies major initiatives associated with these mission areas. One of the mission areas is border and transportation security.[6]

For the border and transportation security mission area, the strategy and the act specify several objectives, including ensuring the integrity of our borders and preventing the entry of unwanted persons into our country. To accomplish this, the strategy provides for, among other things, reform of immigration services, large-scale modernization of border crossings, and consolidation of federal watch lists.[7] It also acknowledges that accomplishing these goals will require overhauling the border security process. This will be no small task, given that the United States shares a 5,525 mile border with Canada and a 1,989 mile border with Mexico and has 95,000 miles of shoreline. Moreover, each year, more than 500 million people legally enter our country, 330 million of them noncitizens. More than 85 percent enter via land borders, often as daily commuters.

Overview of the Border Security Process

Our nation's current border security process for controlling the entry and exit of individuals consists of four primary functions: (1) issuing visas, (2) controlling entries, (3) managing stays, and (4) controlling exits. The federal agencies involved in these functions include the Department of State's Bureau of Consular Affairs and its Bureau of Intelligence and Research, as well as the Justice Department's Immigration and Naturalization Service (INS), the Treasury Department's U.S. Customs

[5] Office of Homeland Security, *National Strategy for Homeland Security* (July 2002).

[6] The other critical mission areas are intelligence and warning, domestic counterterrorism, protecting critical infrastructure, defending against catastrophic terrorism, and emergency preparedness and response.

[7] The strategy assigned the Federal Bureau of Investigation the responsibility for standardizing and consolidating watch lists. However, according to the bureau, this responsibility was subsequently assumed by the Office of Homeland Security.

Service (Customs), and the Transportation Department’s Transportation Security Administration (TSA).[8]

The process begins at the State Department’s overseas consular posts, where consular officers are to adjudicate visa applications for foreign nationals who wish to enter the United States. In doing so, consular officials review visa applications, and sometimes interview applicants, prior to issuing a visa. One objective of this adjudication process is to bar from entry any foreign national who is known or suspected to have engaged in terrorist activity, is likely to engage in such activity, or is a member or supporter of a known terrorist organization.[9]

Foreign nationals (and any other persons attempting to enter the United States, such as U.S. citizens) are to be screened for admission into the United States by INS or Customs inspectors. Generally, this consists of questioning the person and reviewing entry documents. Since October 2002, males aged 16 or over from certain countries (for example, Iran, Iraq, Syria, and the Sudan) are also required to provide their name and U.S. address and to be photographed and fingerprinted. [10] In addition, airline officials use information provided by TSA to screen individuals attempting to travel by air. As discussed in the next section, requirements for checking a person against a watch list differ somewhat, depending upon whether the person arrives at a land-, air-, or seaport.

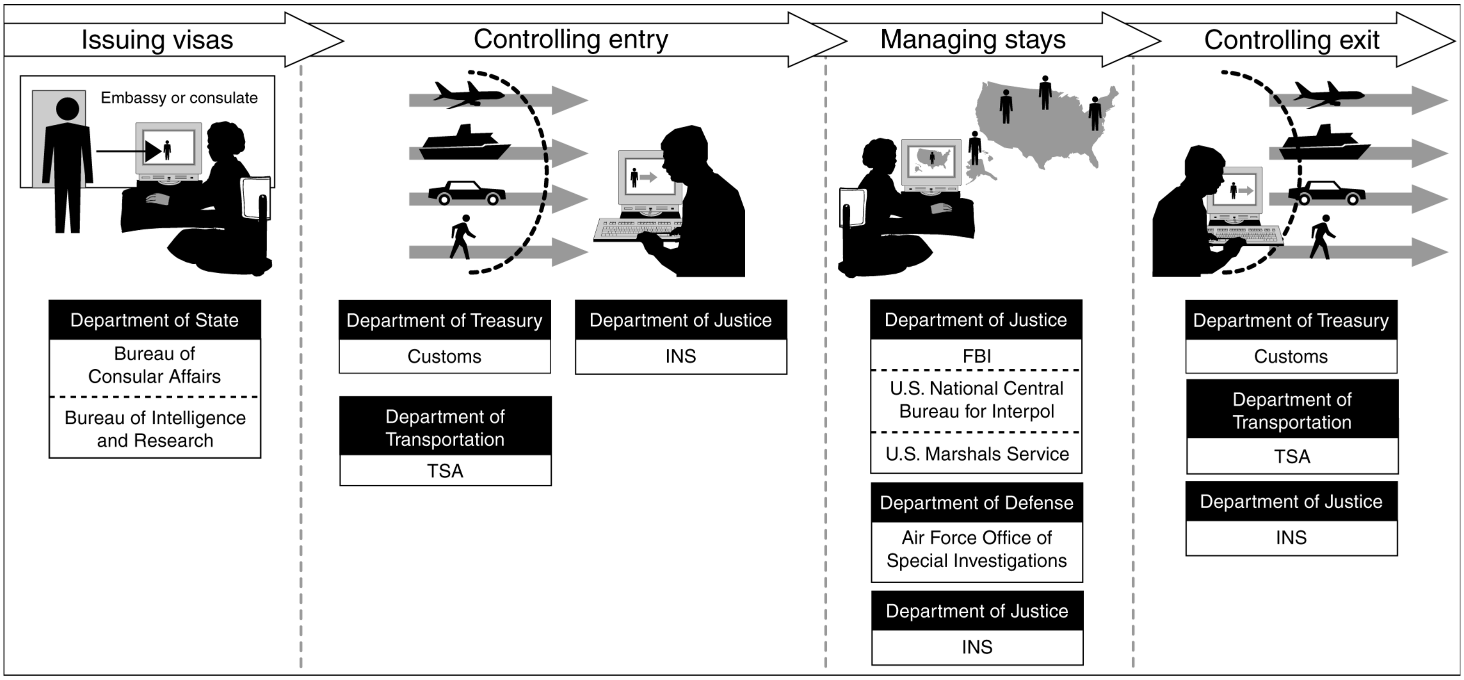
After foreign nationals are successfully screened and admitted, they are not actively monitored unless they are suspected of illegal activity and come under the scrutiny of a law enforcement agency, such as the Department of Justice’s Federal Bureau of Investigation (FBI). Also, when foreign nationals depart the country, they are not screened unless they are males aged 16 years or over from certain countries referenced above, or are leaving by air. According to TSA, all passengers on departing flights are screened prior to boarding the plane. Figure 1 is a simplified overview of the border entry/exit process.

[8] Of these agencies, INS, Customs, and TSA have been incorporated into DHS.

[9] U.S. General Accounting Office, *Border Security: Visa Process Should Be Strengthened as an Antiterrorism Tool*, GAO-03-132NI (Washington, D.C.: October 2002).

[10] The requirement to screen these individuals is part of the Justice Department’s implementation of the National Security Entry-Exit Registration System. According to Justice, it implemented the first phase of the system in October 2002.

Figure 1: Simplified Overview of the Border Security Process and the Departments and Agencies Involved



Sources: GAO (data), Nova Development Corp. (images).

Note: Customs and TSA appear twice in this figure because they support both entry and exit control. INS appears three times because it supports entry control, stay management, and exit control.

The Role of Watch Lists in the Border Security Process

Watch lists are important tools that are used by federal agencies to help secure our nation's borders. These lists share a common purpose—to provide decisionmakers with information about individuals who are known or suspected terrorists and criminals, so that these individuals can either be prevented from entering the country, apprehended while in the country, or apprehended as they attempt to exit the country. As shown in figure 2, which builds on figure 1 by adding watch list icons and associating them with the agencies that maintain the respective lists, watch lists collectively support nine federal agencies in performing the four primary functions in the border security process. Specifically:

- When a person applies for a visa to enter the United States, State Department consular officials are to check that person against one or more watch lists before granting a visa.

- When a person attempts to enter the United States by air or sea, INS or Customs officials are required to check that person against watch lists before the person is allowed to enter the country. In addition, when a person attempts to enter the United States by air, INS or Custom officials check him or her against watch lists provided by TSA prior to allowing him or her to board the plane. Persons arriving at land borders may be checked, but there is no requirement to do so. The exception, as previously discussed, is for males aged 16 or over from certain countries, who are required to be checked.[11]

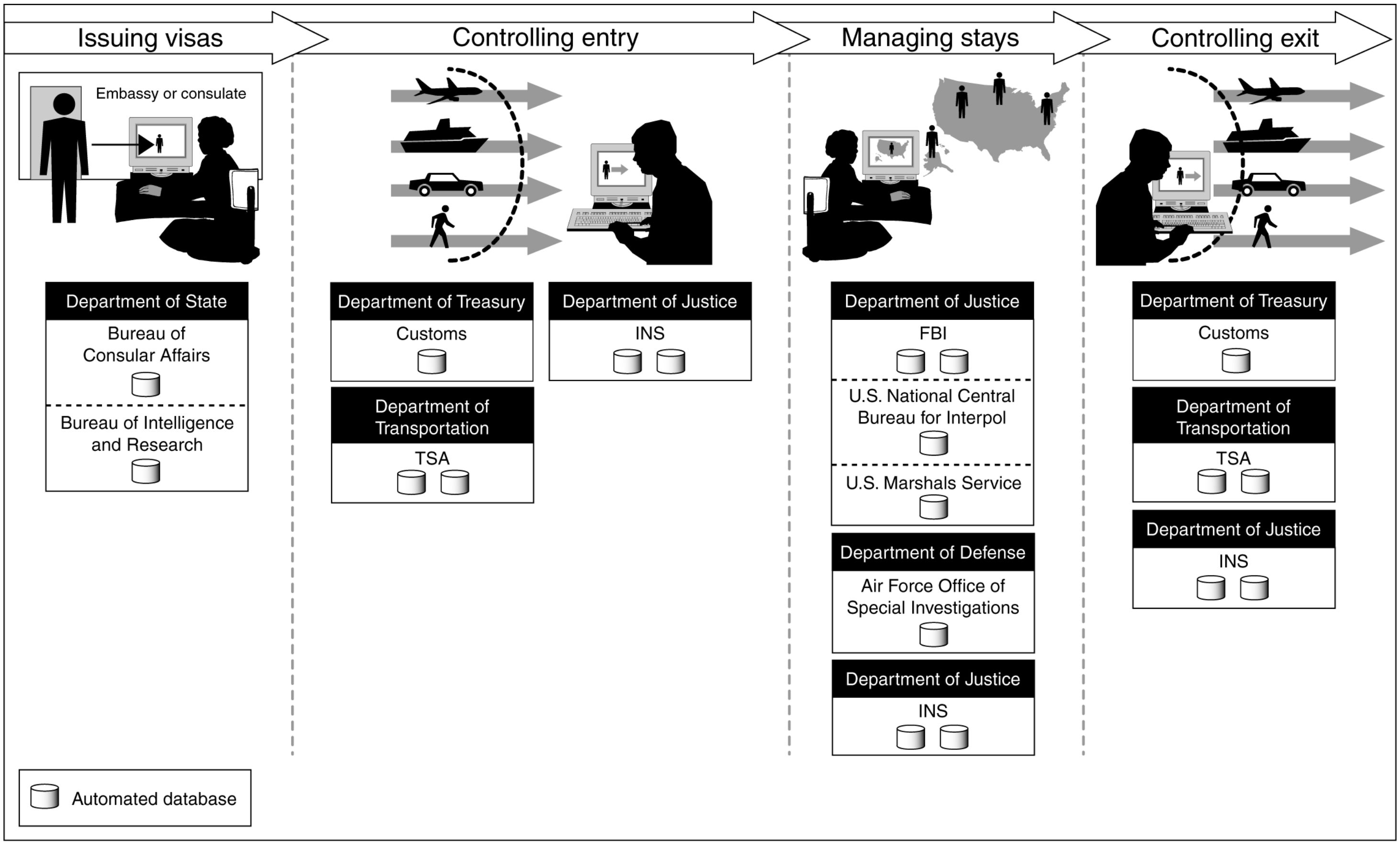
- Once a watch list identifies a person as a known or suspected terrorist, INS, Customs, or airline officials are to contact the appropriate law enforcement or intelligence organization (for example, the FBI), and a decision will be made regarding the person's entry and the agency's monitoring of the person while he or she is in the country.

- When a person exits the country by plane, airline officials are to check that person against watch lists.

In performing these roles, the agencies use information from multiple watch lists. For example, U.S. National Central Bureau for Interpol officials told us that they provide information to the agencies involved in entry control, exit control, and stay management.

[11] Inspectors are also required to check all entering vehicles' license plates against watch lists.

Figure 2: Simplified Diagram of the Border Security Process and the Departments and Agencies That Use Watch Lists



Sources: GAO (data), Nova Development Corp. (images).

Note: Customs and TSA, along with their associated lists, appear twice in this figure because they support both entry and exit control. INS appears three times because its lists support entry control, stay management, and exit control.

President's Strategy Recognizes Problems with Watch Lists and Proposes Improvements

In addition to highlighting the importance of watch lists for border security, the President's national strategy cites problems with these lists, including limited sharing. According to the July 2002 strategy, in the aftermath of the September 11th attacks it became clear that vital watch list information stored in numerous and disparate federal databases as not available to the right people at the right time. In particular, federal agencies that maintained information about terrorists and other criminals had not consistently shared it. The strategy attributed these sharing limitations to legal, cultural, and technical barriers that resulted in the watch lists being developed in different ways, for different purposes, and in isolation from one another.

To address these limitations, the strategy calls for integrating and reducing variations in watch lists and overcoming barriers to sharing the lists. It also calls for developing an enterprise architecture for border security and transportation (see next section for a description of an enterprise architecture).[12] More specifically, the strategy provides for developing a consolidated watch list that would bring together the information on known or suspected terrorists contained in federal agencies' respective lists.[13]

Enterprise Architecture: A Brief Description

If properly developed, enterprise architectures provide clear and comprehensive pictures of an entity, whether it is an organization (for example, a federal department, agency, or bureau) or a functional or mission area that cuts across more than one organization (for example, grant management, homeland security, or border and transportation security). These architectures are recognized as essential tools for effectively and efficiently engineering business operations and the systems and databases needed to support these operations.

More specifically, enterprise architectures are systematically derived and captured blueprints or descriptions—in useful models, diagrams, and narrative—of the mode of operation for a given enterprise. This mode of operation is described in both (1) logical terms, such as interrelated business processes and business rules, information needs and flows, data models, work locations, and users, and (2) technical terms, such as hardware, software, data, communications, and security attributes and performance standards. They provide these perspectives both for the enterprise's current, or "as is," environment and for its target, or "to be,"

[12] The President's strategy assigned the responsibility for developing an enterprise architecture to the Critical Infrastructure Assurance Office, which was part of the Commerce Department but is now being incorporated into the new Department of Homeland Security. However, according to the Critical Infrastructure Assurance Office, this responsibility for developing homeland security enterprise architectures was subsequently assumed by the Office of Homeland Security.

[13] The President's strategy assigned the FBI the responsibility for standardizing and consolidating watch lists. However, according to the FBI, this responsibility has been transferred to the Office of Homeland Security.

environment, as well as a transition plan for moving from the “as is” to the “to be” environment.

Using enterprise architectures is a basic tenet of effective IT management, embodied in federal guidance and commercial best practices.[14] When developed and used properly, these architectures define both business operations and the technology that supports these operations in a way that optimizes interdependencies and interrelationships. They provide a common frame of reference to guide and constrain decisions about the content of information asset investments in a way that can ensure that the right information is available to those who need it, when they need it.

Options for Enterprise Database Structures

As discussed in the previous section, enterprise architectures facilitate delivery of the right information to the right people at the right time. To this end, these architectures include data models, or logical representations of data types and their relationships, which are used to engineer physical data “stores,” or repositories. When engineered properly, these data stores are structured in a way that effectively and efficiently supports both shared and unique enterprise applications, functions, and operations. The structure of these data stores, whether they are paper records or automated databases, can take many forms, employing varying degrees of centralization and standardization. Associated with the structures being employed are opportunities and limitations to effective and efficient information exchange and use.

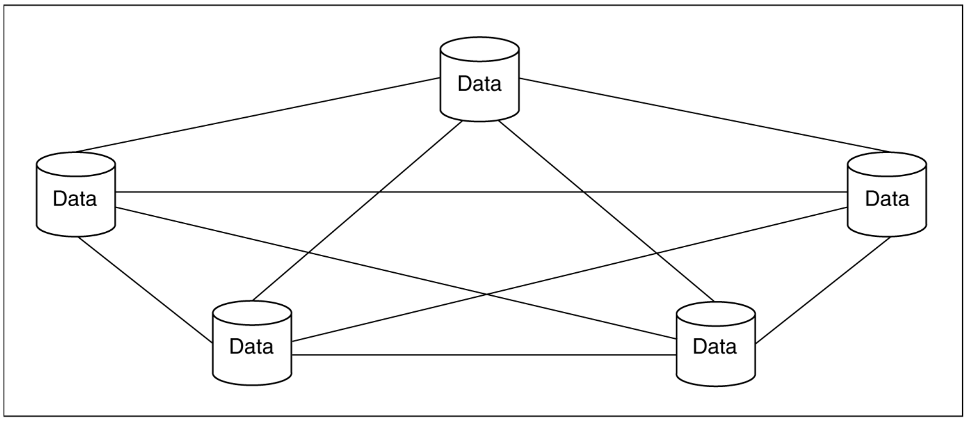
Generally, these structures can be viewed along a continuum. At one extreme, databases can be nonstandard, both in terms of metadata[15] and the technologies that manage the data, and they can be decentralized, meaning that they were built in isolation from one another to support isolated or separate, “stovepiped” applications, functions, and operations. In this case, integrating the databases to permit information exchange

[14] For example, see Office of Management and Budget, *Management of Federal Information Resources*, Circular No. A-130 (Washington, D.C.: November 2000) and U.S. General Accounting Office, *Executive Guide: Improving Mission Performance through Strategic Information Management and Technology: Learning from Leading Organizations*, GAO/AIMD-94-115 (Washington, D.C.: May 1994).

[15] In short, metadata are “data about data.” That is, they are definitional data that describe the context, quality, condition, or characteristics of the specific data elements in a set of data or a database.

requires the development of unique, and potentially complex and costly, point-to-point interfaces (hardware and software) that translate the data or bridge incompatibilities in the technology. Further, the sheer number of databases involved can exponentially increase the number of relationships, and thus interfaces, that have to be built and maintained. Structuring databases in this way can quickly evolve into an overly complex, unnecessarily inefficient, and potentially ineffective way to support mission operations. (See fig. 3 for a simplified diagram conceptually depicting this approach to structuring databases.)

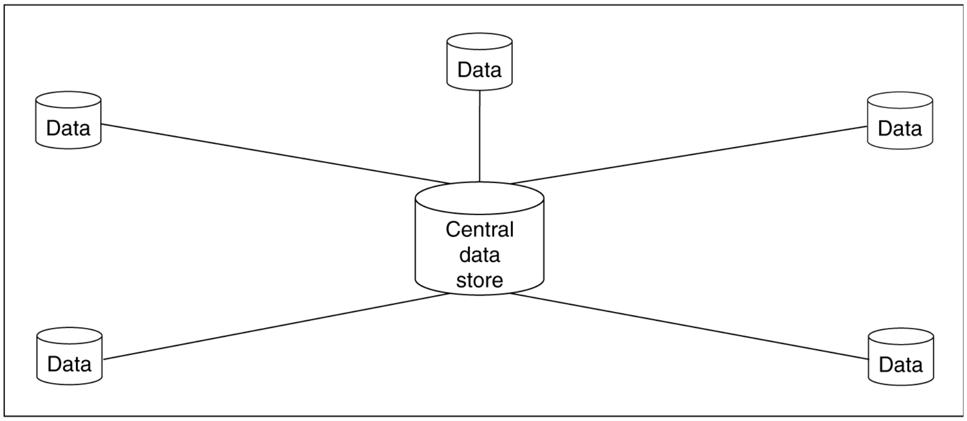
Figure 3: Simplified Diagram of the Complexity Associated with Connecting Decentralized Databases



Source: GAO.

At the other extreme, databases can be structured to recognize that various enterprise applications, functions, and operations have a need for the same data or sets of data, even though they may need to use them in different ways to support different mission applications, functions, and operations. If engineered properly, these database structures allow for greater use of standards, in terms of both data definitions and technology, and are more centralized, although the option exists to create subsidiary databases—known as data warehouses and data marts—to permit more uniquely configured and decentralized data sources to support specific and unique mission needs. Further, since the core data in these subsidiary databases are received from a corporate database(s), the need for interfaces to translate data or connect incompatible technologies is greatly reduced. Structuring databases in this way can minimize complexity and maximize efficiency and mission effectiveness. (See fig. 4 for a simplified diagram conceptually depicting this approach to structuring databases.)

Figure 4: Simplified Diagram of Central Data Store with Subsidiary Databases



Source: GAO.

Federal Agencies Maintain Numerous Watch Lists, Containing Varying Types of Data, Used by Many Organizations

Terrorist watch lists are developed, maintained, or used by federal, state, and local government entities, as well as by private-sector entities, to secure our nation's borders. Twelve such lists are currently maintained by federal agencies. These lists contain various types of data, from biographical data—such as a person's name and date of birth—to biometric data—such as fingerprints.

Twelve Federal Watch Lists Are Maintained by Nine Agencies

Nine federal agencies, which prior to the establishment of DHS spanned five different cabinet-level departments, currently maintain 12 terrorist and criminal watch lists. These lists are also used by at least 50 federal, state, and local agencies. The above-mentioned departments are the Departments of State, Treasury, Transportation, Justice, and Defense. Table 1 shows the departments, the associated nine agencies that maintain watch lists, and the 12 watch lists.

Table 1: Departments, Agencies, and Their Watch Lists

Department	Agency/Department subcomponent	Watch list
State	Bureau of Consular Affairs	Consular Lookout and Support
	Bureau of Intelligence and Research	TIPOFF
Treasury	Customs	Interagency Border Inspection[a]
Transportation	TSA	No-Fly
		Selectee
Justice	INS	National Automated Immigration Lookout
		Automated Biometric (fingerprint) Identification System[b]
	U.S. Marshals Service	Warrant Information
	FBI	Violent Gang and Terrorist Organization File[c]
		Integrated Automated Fingerprint Identification
	U.S. National Central Bureau for Interpol[d]	Interpol Terrorism Watch List
Defense	Air Force (Office of Special Investigations)	Top Ten Fugitive

Source: GAO.

[a] Interagency Border Inspection operates as a part of Customs' Treasury Enforcement Communications System, commonly referred to as TECS.

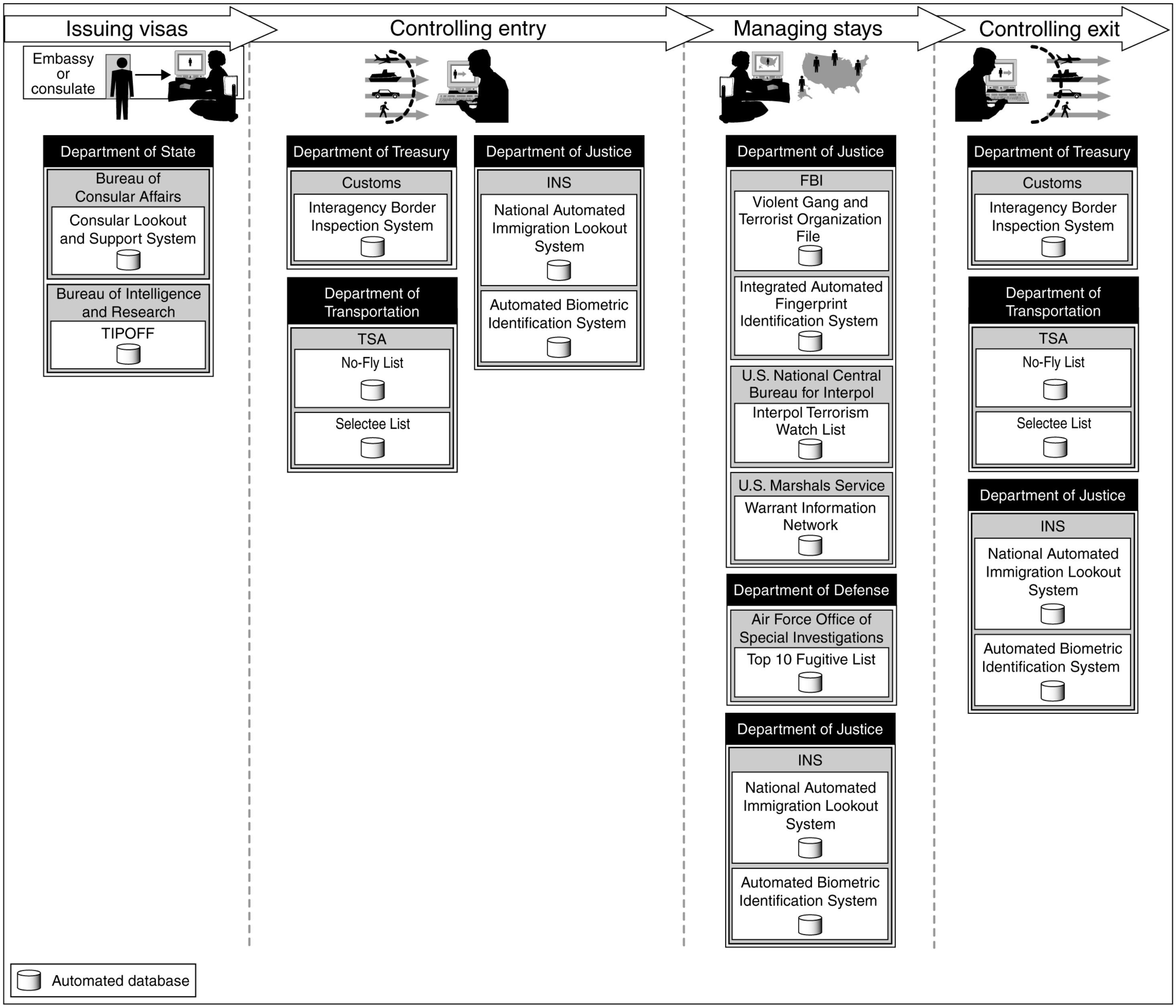
[b] INS is in the process of integrating this system with the FBI's Integrated Automated Fingerprint Identification System.

[c] This list is part of the FBI's National Crime Information Center.

[d] Interpol (International Police Organization) is an intergovernmental organization made up of 181 member countries for the purpose of ensuring cooperation among the world's law enforcement entities. It is headquartered in Lyon, France. The U.S. National Central Bureau for Interpol, within the Justice Department, serves as the U.S. member of Interpol and facilitates dissemination of Interpol watch list information to federal, state, and local agencies.

The 12 watch lists support the federal agencies involved in the border security process. Figure 5, which builds on figure 2, provides a graphical representation identifying the name of each of the lists and relating them to the agencies that maintain the lists and are involved in performing the four border security functions: issuing visas, controlling entries, managing stays, and controlling exits.

Figure 5: Simplified Diagram of the Border Security Process, Departments and Agencies Involved, and Watch Lists Used


Issuing visas
Controlling entry
Managing stays
Controlling exit
Embassy or consulate
Department of State
Bureau of Consular Affairs
Consular Lookout and Support System
Bureau of Intelligence and Research
TIPOFF
Department of Treasury
Customs
Interagency Border Inspection System
Department of Transportation
TSA
No-Fly List
Selectee List
Department of Justice
INS
National Automated Immigration Lookout System
Automated Biometric Identification System
Department of Justice
FBI
Violent Gang and Terrorist Organization File
Integrated Automated Fingerprint Identification System
U.S. National Central Bureau for Interpol
Interpol Terrorism Watch List
U.S. Marshals Service
Warrant Information Network
Department of Defense
Air Force Office of Special Investigations
Top 10 Fugitive List
Department of Justice
INS
National Automated Immigration Lookout System
Automated Biometric Identification System
Department of Treasury
Customs
Interagency Border Inspection System
Department of Transportation
TSA
No-Fly List
Selectee List
Department of Justice
INS
National Automated Immigration Lookout System
Automated Biometric Identification System
Automated database

Sources: GAO (data), Nova Development Corp. (images).

Notes: Customs and TSA, along with their associated lists, appear twice in this figure because they support both entry and exit control. INS appears three times because its systems support entry control, stay management, and exit control.

INS also uses the Interagency Border Inspection System to control entry and exit as well as to monitor stays.

Watch Lists Contain Different Types of Data

The 12 watch lists do not all contain the same types of data, although some types are included in all of the lists. At the same time, some types of data are included in only a few of the lists. More specifically, all of the lists include the name and date of birth; 11 include other biographical information (for example, passport number and any known aliases); 9 include criminal history (for example, warrants and arrests); 8 include biometric data (for example, fingerprints); 3 include immigration data (for example, visa type, travel dates, departure country, destination country, country visited, arrival dates, departure dates, and purpose of travel); and 2 include financial data (for example, large currency transactions). Figure 6 shows the data types that are included in each watch list.

Figure 6: Types of Data Included in Watch Lists

Data type	Consular Lookout and Support	TIPOFF	Interagency Border Inspection	No-Fly	Selectee	National Automated Immigration Lookout	Warrant Information	Automated Biometric (fingerprint) Identification	Violent Gang and Terrorist Organization File	Integrated Automated Fingerprint Identification	Interpol Terrorism Watch List	Top Ten Fugitive
Biographic items												
Name	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Aliases	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	
Nationality/citizenship	▨	▨	▨	▨	▨	▨	▨	▨		▨	▨	▨
Birth date	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Passport number	▨	▨	▨	▨	▨	▨	▨		▨	▨	▨	
Country issuing passport	▨	▨	▨	▨	▨	▨	▨				▨	
Address		▨	▨	▨	▨		▨	▨			▨	▨
Criminal history												
Warrants	▨	▨				▨	▨	▨	▨		▨	▨
Arrests	▨	▨				▨	▨	▨		▨	▨	
Biometric items												
Photographs		▨	▨				▨	▨	▨	▨	▨	
Ten print fingerprints		▨	▨					▨		▨	▨	
Facial		▨					▨				▨	▨
Two print fingerprints			▨					▨				
Iris												
Hand												
Immigration												
Visa type		▨	▨									
Travel dates		▨	▨									
Departure country			▨									
Destination country			▨									
Countries visited											▨	
Arrival date			▨									
Departure date			▨									
Travel purpose		▨										
Financial												
Large currency transactions		▨	▨									
Credit card requests												

Source: GAO.

Note: Shaded cells indicate data included in watch lists.

Watch List Sharing Is Governed by Varying Policies and Procedures

Effective sharing of information from watch lists and of other types of data among multiple agencies can be facilitated by agencies' development and use of well-coordinated and aligned policies and procedures that define the rules governing this sharing. One effective way to implement such policies and procedures is to prepare and execute written watch list exchange agreements or memorandums of understanding. These agreements would specify answers to such questions as what data are to be shared with whom, and how and when they are to be shared.

Not all of the nine agencies have policies and procedures governing the sharing of watch lists. In particular, two of the agencies reported that they did not have any policies and procedures on watch list sharing. In addition, of the seven that reported having such policies and procedures, one did not require any written agreements. Further, the policies and procedures of the seven have varied. For example, one agency's policies included guidance on sharing with other federal agencies as well as with state and local governments, but another's addressed sharing only with other federal agencies. In addition, each agency had different policies and procedures on memorandums of understanding, ranging from one agency's not specifying any requirements to others' specifying in detail that such agreements should include how, when, and where data would be shared with other parties.

The variation in policies and procedures governing the sharing of information from watch lists can be attributed to the fact that each agency has developed its own policies and procedures in response to its own specific needs. In addition, the agencies reported that they received no direction from the Office of Homeland Security identifying the needs of the government as a whole in this area. As a result, federal agencies do not have a consistent and uniform approach to sharing watch list information.

Federal Agency Watch List Data Sharing and Supporting System Architectures Vary

The President's homeland security strategy and recent legislation call for increased sharing of watch lists, not only among federal agencies, but also among federal, state, and local government entities and between government and private-sector organizations. Currently, sharing of watch list data is occurring, but the extent to which it occurs varies, depending on the entities involved. Further, these sharing activities are not supported by systems with common architectures. This is because agencies have developed their respective watch lists, and have managed their use, in isolation from each other, and in recognition of each agency's unique legal, cultural, and technological environments. The result is inconsistent and limited sharing.

Watch List Sharing Varies

According to the President's homeland security strategy, watch list data sharing has to occur horizontally among federal agencies as well as vertically among federal, state, and local governments in order for the country to effectively combat terrorism. In addition, recent federal homeland security legislation, including the Homeland Security Act,[16] USA PATRIOT ACT of 2001,[17] and the Enhanced Border Security and Visa Entry Reform Act of 2002[18] require, among other things, increased sharing of homeland security information both among federal agencies and across all levels of government.

The degree to which watch list data are being shared is not consistent with the President's strategy and recent legislative direction on increased data sharing. Specifically, while federal agencies report that they are generally sharing watch list data with each other, they also report that sharing with organizations outside of the federal government is limited. That is, five of the nine agencies reported that they shared data from their lists with state and local agencies, and three reported that they shared data with private industry. Figure 7 visually summarizes the extent to which federal agencies share watch list data with each level of government (federal, state, and local) and with the private sector.

[16] P.L. 107-296, section 202.

[17] P.L. 107-56.

[18] P.L. 107-173.

Figure 7: Extent of Agency Sharing of Watch List Data with Other Federal Agencies and with State, Local, and Private Organizations

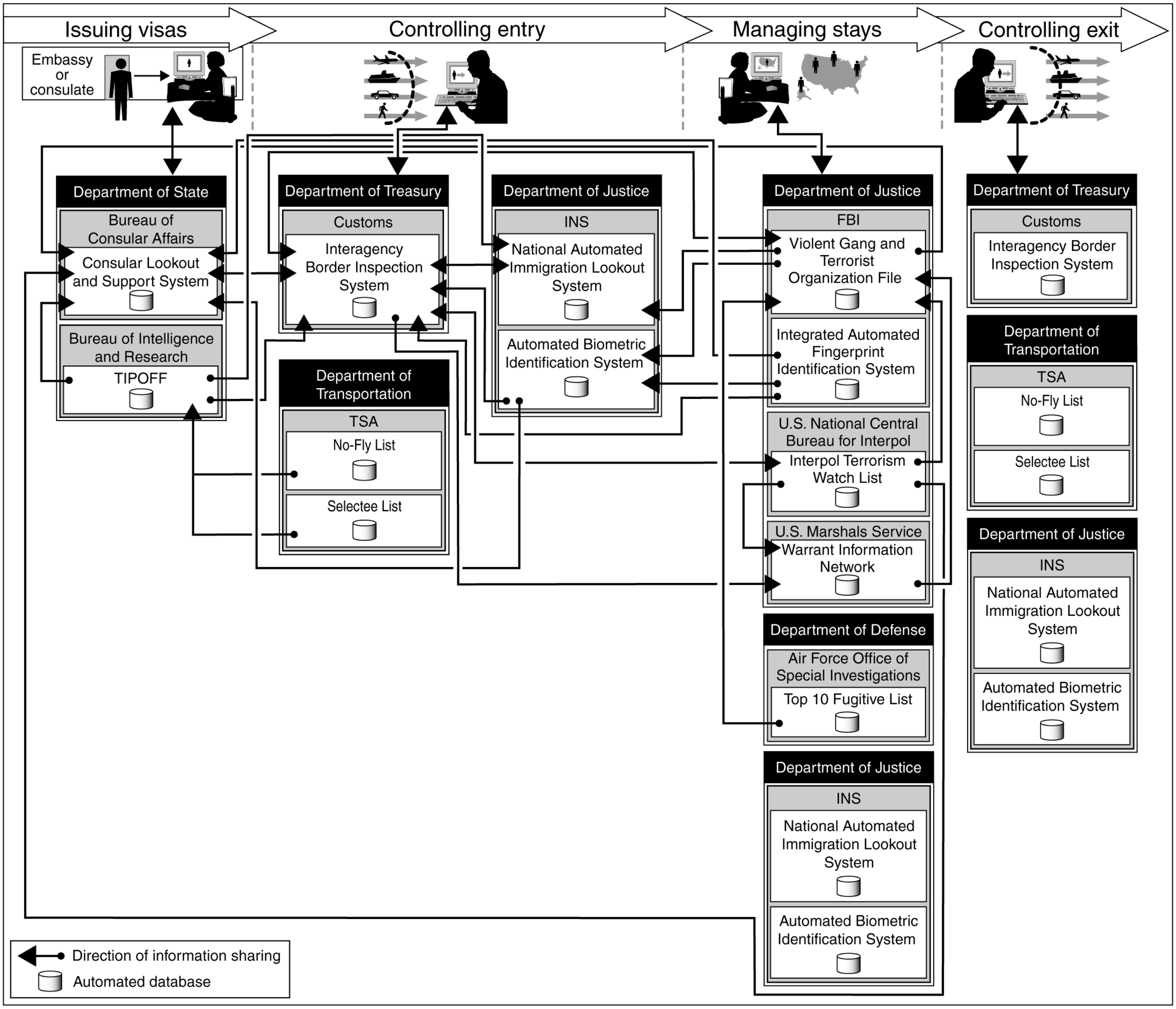
Watch list name (agency that maintains list)	Other federal agencies	State agencies	Local agencies	Private entities
Consular Lookout and Support (Bureau of Consular Affairs)	░	□	□	□
TIPOFF (Bureau of Intelligence and Research)	▓	□	□	□
Interagency Border and Inspection (Customs)	░	□	□	□
No-Fly (TSA)	░	░	░	░
Selectee (TSA)	░	░	░	░
National Automated Immigration Lookout (INS)	░	░	░	□
Warrant Information (U.S. Marshals Service)	░	░	░	░
Automated Biometric Identification (INS)	▓	□	□	□
Violent Gang and Terrorist Organization File (FBI)	▓	▓	▓	□
Integrated Automated Fingerprint Identification (FBI)	▓	▓	▓	□
Interpol Terrorism Watch List (U.S. National Central Bureau for Interpol)	▓	▓	▓	□
Top Ten Fugitive (Air Force)	▓	□	□	□

□ Shares no data
░ Shares some data
▓ Shares all data

Source: GAO.

As noted above, federal agencies are sharing either all or some of their watch list data with each other. However, this sharing is the result of each agency's having developed and implemented its own interfaces with other federal agencies' watch lists. The consequence is the kind of overly complex, unnecessarily inefficient, and potentially ineffective network that is associated with unstructured and nonstandard database environments. In particular, this environment consists of nine agencies—with 12 watch lists—that collectively maintain at least 17 interfaces; one agency's watch list alone has at least 4 interfaces. A simplified representation of the number of watch list interfaces and the complexity of the watch list environment is provided in figure 8.

Figure 8: Simplified Overview of the Border Security Process, Departments and Agencies Involved, Watch Lists Used, and Sharing among Watch Lists


Issuing visas
Controlling entry
Managing stays
Controlling exit
Embassy or consulate
Department of State
Bureau of Consular Affairs
Consular Lookout and Support System
Bureau of Intelligence and Research
TIPOFF
Department of Treasury
Customs
Interagency Border Inspection System
Department of Transportation
TSA
No-Fly List
Selectee List
Department of Justice
INS
National Automated Immigration Lookout System
Automated Biometric Identification System
Department of Justice
FBI
Violent Gang and Terrorist Organization File
Integrated Automated Fingerprint Identification System
U.S. National Central Bureau for Interpol
Interpol Terrorism Watch List
U.S. Marshals Service
Warrant Information Network
Department of Defense
Air Force Office of Special Investigations
Top 10 Fugitive List
Department of Justice
INS
National Automated Immigration Lookout System
Automated Biometric Identification System
Department of Treasury
Customs
Interagency Border Inspection System
Department of Transportation
TSA
No-Fly List
Selectee List
Department of Justice
INS
National Automated Immigration Lookout System
Automated Biometric Identification System
Direction of information sharing
Automated database

Sources: GAO (data), Nova Development Corp. (images).

Note: Several watch lists are used in more than one phase of the border security process. For example, Customs uses the Interagency Border Inspection System for controlling entry and for controlling exits. In such cases, we showed the watch list interfaces under only one phase.

A key reason for the varying extent of watch list sharing is the cultural differences among the government agencies and private-sector organizations involved in securing U.S. borders. According to the President's strategy, cultural differences often prevent agencies from exchanging or integrating information. We also recently reported that differences in agencies' cultures has been and remains one of the principal impediments to integrating and sharing information from watch lists and other information. [19]

Historically, legal requirements have also been impediments to sharing, but recent legislation has begun addressing this barrier. Specifically, the President's strategy and our past work[20] have reported on legal requirements, such as security, privacy, and other civil liberty protections, that restrict effective information sharing. To address this problem, Congress has recently passed legislation that has significantly changed the legal framework for information sharing, which, when fully implemented, should diminish the effect of existing legal barriers. In particular, Congress has enacted legislation providing for agencies to have increased access to other agencies' information and directing more data sharing among agencies. For example, section 701 of the USA PATRIOT ACT[21] broadened the goals of regional law enforcement's information sharing to cover terrorist activities. The Enhanced Border Security and Visa Entry Reform Act[22] expanded law enforcement and intelligence information sharing about aliens seeking to enter or stay in the United States. Most recently, the Homeland Security Act[23] provides the newly created DHS with wide access to information held by federal agencies relating to "threats of terrorism" against the United States. Section 891 expresses the "sense of Congress" that "Federal, state, and local entities should share homeland security

[19] GAO-02-1122T.

[20] For example, see U.S. General Accounting Office, *National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy*, GAO-02-811T (Washington, D.C.: June 2002).

[21] P. L. 107-56.

[22] P. L. 107-173.

[23] P. L. 107-296.

information to the maximum extent practicable." Further, section 892 of the Act requires the President to prescribe and implement procedures for the sharing of "homeland security information" among federal agencies and with state and local agencies, and section 895 requires the sharing of grand jury information.

Watch List Sharing Is Not Supported by a Common Architecture

The President's homeland security strategy stresses the importance of information sharing and identifies, among other things, the lack of a common systems architecture—and the resultant incompatible watch list systems and data—as an impediment to systems' interoperating effectively and efficiently. To address this impediment, the strategy proposes developing a "system of systems" that would allow greater information sharing across federal agencies as well as among federal agencies, state and local governments, private industry, and citizens.

In order for systems to work more effectively and efficiently, each system's key components have to meet certain criteria. In particular, their operating systems[24] and applications [25] have to conform to certain standards that are in the public domain, their databases have to be built according to explicitly defined and documented data schemas and data models, and their networks have to be connected. More specifically, critical system components would have to adhere to common standards, such as open systems standards, to ensure that different systems interoperate.[26] One source for open system standards is the International Organization for Standardization.[27] Also, these systems' data would have to have common—or at least mutually understood—data definitions so that data could, at a minimum, be received and processed, and potentially aggregated and

[24] An operating system is the program that manages all the other programs (called applications) in a computer.

[25] An application is a program that is designed to perform a specific function for the user or another program.

[26] Open system standards are standards, such as the ISO Open Systems Interconnection model that, when followed, result in a computer system that can incorporate all devices that use the same communications facilities and protocols, regardless of make or model.

[27] The International Organization for Standardization is an international association of member countries, each of which is represented by its leading standard-setting organization—for example, ANSI (American National Standards Institute) for the United States.

analyzed. Such data definitions are usually captured in a data dictionary.[28] Further, these systems would have to be connected to each other via a telecommunications network or networks. When system components and data do not meet such standards, additional measures have to be employed, such as acquiring or building and maintaining unique system interfaces (hardware and software) or using manual workarounds. These measures introduce additional costs and reduce efficiency and effectiveness.

The 12 automated watch list systems do not meet all of these criteria (see table 2). For example, they use three different types of operating systems, each of which stores data and files differently. Overcoming these differences requires the use of software utilities to bridge the differences between systems. Without such utilities, for example, a Windows-based system cannot read data from a diskette formatted by a UNIX-based system.

[28] A data dictionary is a collection of descriptions of the data objects or items in a data model, including a descriptive name; relationships to other data items, structures, and types (text or image or binary value); possible predefined values; and a text description. Such dictionaries are used for the benefit of programmers and others who need to refer to them in developing or operating and maintaining systems.

Table 2: Selected Architectural Characteristics of the 12 Watch List Systems

Watch list database	Is the operating system compatible with all other watch list operating systems?	Are the software applications compliant with open system standards?	Is the data dictionary available and shared?	Is the system connected to an external network?
Consular Lookout and Support System	No	No	Yes	Yes
TIPOFF	No	No	Yes	No
Interagency Border Inspection System	No	No	Yes	No
National Automated Immigration Lookout System	No	No	No	No
Warrant Information Network	No	No	Yes	Yes
Automated Biometric Identification System	No	No	No	No
Violent Gang and Terrorist Organization File[a]	No	No	Yes	Yes
Integrated Automated Fingerprint Identification System[a]	No	Yes	Yes	Yes
Top Ten Fugitive List	No	Yes	No	Yes
Interpol Terrorism Watch List	No	Yes	Unknown[b]	No
No-Fly List	No	No	No	No
Selectee List	No	No	No	No

Source: GAO.

[a] System is connected to a network, but databases are not accessible directly from the network.

[b] Officials from the U.S. National Central Bureau for Interpol stated that they did not know to what extent Interpol headquarters shares its data dictionary with others.

Also, nine of the systems do not have software applications that comply with open system standards. In these cases, agencies may have had to invest time and resources in designing, developing, and maintaining unique interfaces[29] so that the systems can exchange data.

Further, five of the systems' databases do not have a data dictionary, and of the remaining seven systems that do have data dictionaries, at least one is not sharing its dictionary with other agencies. Without both the existence and sharing of these data dictionaries, meaningful understanding of data received from another agency could require an added investment of time and resources to interpret and understand what the received data mean. Moreover, aggregation and analysis of the data received with the data from other watch lists may require still further investment of time and resources to restructure and reformat the data in a common way.

Last, seven of the systems are not connected to a network outside of their agencies or departments. Our experience has shown that without network connectivity, watch list data sharing among agencies can occur only through manual intervention. According to several of these agencies, the manual workarounds are labor-intensive and time-consuming, and they limit the timeliness of the data provided. For example, data from the TIPOFF system are shared directly with the National Automated Immigration Lookout System through a regular update on diskette. Those data are then transferred from the National Automated Immigration Lookout System to the Interagency Border Inspection System.

The President' s strategy attributes these differences to the agencies' building their own systems to meet agency-specific mission needs, goals, and policies, without knowledge of the information needs and policies of the government as a whole. As noted and depicted in figure 6, this approach has resulted in an overly complex, unnecessarily inefficient, and potentially ineffective federal watch list sharing environment.

Opportunities Exist for Consolidating Watch Lists and Improving Information Sharing

As addressed in the preceding sections of this report, federal watch lists share a common purpose and support the border security mission. Nevertheless, the federal government has developed, maintains, and—along with state and local governments and private entities—uses 12 separate watch lists, some of which contain the same types of data. However, this proliferation of systems, combined with the varying policies

[29] An interface is the point at which a connection is made between two elements, such as systems, so that they can work with one another.

and procedures that govern the sharing of each, as well as the architectural differences among the automated lists, create strong arguments for list consolidation. The advantages of doing so include faster access, reduced duplication, and increased consistency, which can reduce costs and improve data reliability.

Most of the agencies that have developed and maintain watch lists did not identify consolidation opportunities. Of the nine federal agencies that operate and maintain watch lists, seven reported that the current state and configuration of federal watch lists meet their mission needs, and that they are satisfied with the level of watch list sharing. However, two agencies supported efforts to consolidate these lists. The State Department's Bureau of Consular Affairs and the Justice Department's U.S. Marshals Service agreed that some degree of watch list consolidation would be beneficial and would improve information sharing. Both cited as advantages of consolidation the saving of staff time and financial resources by limiting the number of labor-intensive and time-consuming data transfers, and one also cited the reduction in duplication of data that could be realized by decreasing the number of agencies that maintain lists.

The President's strategy also recognizes that watch list consolidation opportunities exist and need to be exploited. More specifically, the strategy states that the events of September 11th raised concerns regarding the effectiveness of having multiple watch lists and the lack of integration and sharing among them. To address these problems, the strategy calls for integrating the numerous and disparate systems that support watch lists as a way to reduce the variations in watch lists and remove barriers to sharing them.

To implement the strategy, Office of Homeland Security officials have stated in public settings that they were developing an enterprise architecture for border and transportation security, which is one of the six key mission areas of the newly created DHS.[30] They also reported the following initial projects under this architecture effort: (1) developing a consolidated watch list that brings together information on known or suspected terrorists in the federal agencies' watch lists, and

[30] The President's July 2002 homeland security strategy assigns responsibility to the Critical Infrastructure Assurance Office (in the Commerce Department) for developing the enterprise architecture for data sharing and to the FBI for consolidating watch lists. Officials at these two agencies told us that their respective responsibilities were subsequently assumed by the Office of Homeland Security.

(2) establishing common metadata or data definitions for electronic watch lists and other information that is relevant to homeland security. However, the Office of Homeland Security did not respond to our inquiries about this effort, and thus we could not determine the substance, status, and schedule of any watch list consolidation activities. Since then, the DHS Chief Information Officer told us that DHS has assumed responsibility for these efforts.

Conclusions

Our nation's success in achieving its homeland security mission depends in large part on its ability to get the right information to the right people at the right time. Terrorist and criminal watch lists make up one category of such information. To date, the federal watch list environment has been characterized by a proliferation of systems, among which information sharing is occurring in some cases but not in others. This is inconsistent with the most recent congressional and presidential direction. Our experience has shown that even when sharing is occurring, costly and overly complex measures have had to be taken to facilitate it. Cultural and technological barriers stand in the way of a more integrated, normalized set of watch lists, and agencies' legal authorities and individuals' civil liberties are also relevant considerations. To improve on the current situation, central leadership—spanning not only the many federal agencies engaged in maintaining and using watch lists, but also the state and local government and the private-sector list users—is crucial to introducing an appropriate level of watch list standardization and consolidation while still enforcing relevant laws and allowing agencies to (1) operate appropriately within their unique mission environments and (2) fulfill their unique mission needs. Currently, the degree to which such leadership is occurring, and the substance and status of consolidation and standardization efforts under way, are unclear. In our view, it is imperative that Congress be kept fully informed of the nature and progress of such efforts.

Recommendations for Executive Action

To promote better integration and sharing of watch lists, we recommend that DHS's Secretary, in collaboration with the heads of the departments and agencies that have and use watch lists, lead an effort to consolidate and standardize the federal government's watch list structures and policies. To determine and implement the appropriate level of watch list consolidation and standardization, we further recommend that this collaborative effort include

1. updating the watch list information provided in this report, as needed, and using this information to develop an architectural understanding of our nation's current or "as is" watch list environment;

2. defining the requirements of our nation's target or "to be" watch list architectural environment, including requirements that address any agency-unique needs that can be justified, such as national security issues and civil liberty protections;

3. basing the target architecture on achievement of the mission goals and objectives contained in the President's homeland security strategy and on congressional direction, as well as on opportunities to leverage state and local government and private-sector information sources;

4. developing a near-term strategy for implementing the target architecture that provides for the integration of existing watch lists, as well as a longer-term strategy that provides for migrating to a more consolidated and standardized set of watch lists;

5. ensuring that these strategies provide for defining and adopting more standard policies and procedures for watch list sharing and addressing any legal issues affecting, and cultural barriers to, greater watch list sharing; and

6. developing and implementing the strategies within the context of the ongoing enterprise architecture efforts of each of the collaborating departments and agencies.

In addition, we recommend that the Secretary report to Congress by September 30, 2003, and every 6 months thereafter, on the status and progress of these efforts, as well as on any legislative action needed to accomplish them.

Agency Comments And Our Evaluation

In commenting on a draft this report, three of the six departments provided either written (Justice and State) or oral (DHS) comments. The remaining three departments (Defense, Transportation, and Treasury) said that they had reviewed the draft but had no comments. The Office of Homeland Security was also provided with a draft but said that it would not comment. The departments that provided comments generally agreed with our findings and recommendations. They also (1) provided technical comments, which we have incorporated as appropriate in the report, and

(2) offered department-unique comments, which are summarized and evaluated below.

In his oral comments, DHS's Chief Information Officer stated that the department now has responsibility for watch list consolidation. Additionally, the Chief Information Officer generally described DHS's plans for watch list consolidation and agreed that our recommendations were consistent with the steps he described. In light of DHS's assumption of responsibility for watch list consolidation, we have modified our recommendations to direct them to the DHS Secretary.

In its written comments, Justice stated that, in addition to cultural differences, there are other reasons why agencies do not share watch list information, such as national security and civil liberty requirements, and that these requirements complicate the consolidation of watch list information. Justice also stated that, while it agrees that there is a need to establish a common watch list architecture to facilitate sharing, this need should not impede short-term efforts to improve sharing. We agree with Justice's first point, which is why our recommendations provide for ensuring that all relevant requirements, which would include pertinent national security and civil liberty protections, are taken into consideration in developing our nation's watch list architectural environment. To make this more explicit, we have modified our recommendations to specifically recognize national security and civil liberty requirements. We also agree with Justice's second point, and thus our recommendations also provide for pursuing short-term, cost-effective initiatives to improve watch list sharing while the architecture is being developed. (Justice's comments are reprinted in app. II.)

In its written comments, State said that our report makes a number of valuable points concerning the benefits of watch list consolidation, enterprise architecture, and information sharing. However, State also said that our report (1) attributed watch list differences solely to varying agency cultures, (2) seemed to advocate a "one size fits all approach," and (3) often makes the assumption that software and systems architecture differences necessarily obstruct information sharing. With respect to State's first point, our report states clearly that watch list differences are attributable not only to varying cultural environments, but also to each agency's unique mission needs and its legal and technical environments as well. Concerning State's second point, our report does not advocate a "one size fits all" solution. Rather, our recommendation explicitly calls for DHS to lead a governmentwide effort to, among other things, determine the appropriate degree of watch list consolidation and standardization needed and to consider in this effort the differences in agencies' missions and needs. Regarding State's last point, our report does not state or assume that differences in software and system architecture categorically obstruct or preclude information sharing. Instead, we state that those differences requiring additional measures—such as building and maintaining unique system interfaces or using manual workarounds—introduce additional costs and reduce efficiency and effectiveness. (State's comments are reprinted in app. III.)

As agreed with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 15 days from the date on the report. At that time, we will send copies of the report to other congressional committees. We will also send copies to the Directors of the Offices of Homeland Security and Management and Budget, and the Secretaries of the Departments of Defense, Homeland Security, Justice, State, Transportation, and the Treasury. Copies will also be made available at our Web site at www.gao.gov.

Should you or your offices have questions on matters discussed in this report, please contact me at (202) 512-3439. I can also be reached by E-mail at hiter@gao.gov. An additional GAO contact and staff acknowledgments are listed in appendix V.

Randolph C. Hite

Randolph C. Hite
Director, Information Technology Architecture
and Systems Issues

Objectives, Scope, and Methodology

Our objectives were to identify (1) federal databases and systems that contain watch lists, the agencies that maintain and use these watch lists in protecting our nation's borders, and the kinds of data these watch lists contain; (2) whether federal agencies' sharing of watch list data is governed by policies and procedures; (3) whether watch lists are (a) being exchanged among federal agencies and between federal agencies and state, local, and private organizations and (b) supported by common system architectures (system hardware, software, and data characteristics); and (4) whether opportunities exist for consolidating watch lists.

The scope of our work was based on the federal government's agency structure before the formation of the Department of Homeland Security. We focused on the agencies that use or maintain watch lists in performing border security functions. We identified these departments and agencies through discussions with federal government officials knowledgeable about the U.S. border security mission area.

The specific departments and agencies included in our scope were:

- Department of Justice
    - Federal Bureau of Investigation
    - Immigration and Naturalization Service
    - U.S. Marshals Service
    - U.S. National Central Bureau for Interpol
- Department of State
    - Bureau of Consular Affairs
    - Bureau of Intelligence and Research
- Department of the Treasury
    - U.S. Customs Service
- Department of Defense
    - Air Force Office of Special Investigations

- Department of Transportation
  - Transportation Security Administration.

To address our objectives, we surveyed each of the agencies cited above, using a data collection instrument. To develop this instrument, we reviewed, among other things, past GAO and other reports on watch lists and on the border security process, along with relevant guidance on such topics as systems interoperability, enterprise architecture management, database management, and information sharing. We used this research to develop a series of questions designed to obtain and aggregate information necessary to answer our objectives. We then incorporated these questions into the questionnaire (see app. IV for a copy of the questionnaire). We pretested the questionnaire at two federal agencies, made adjustments based on the pretest, and then transmitted it to the agencies cited above on July 29, 2002. Responses from agencies were received from August 2002 through October 2002. We did not independently verify agency responses. However, we did contact agency officials when necessary to clarify their responses.

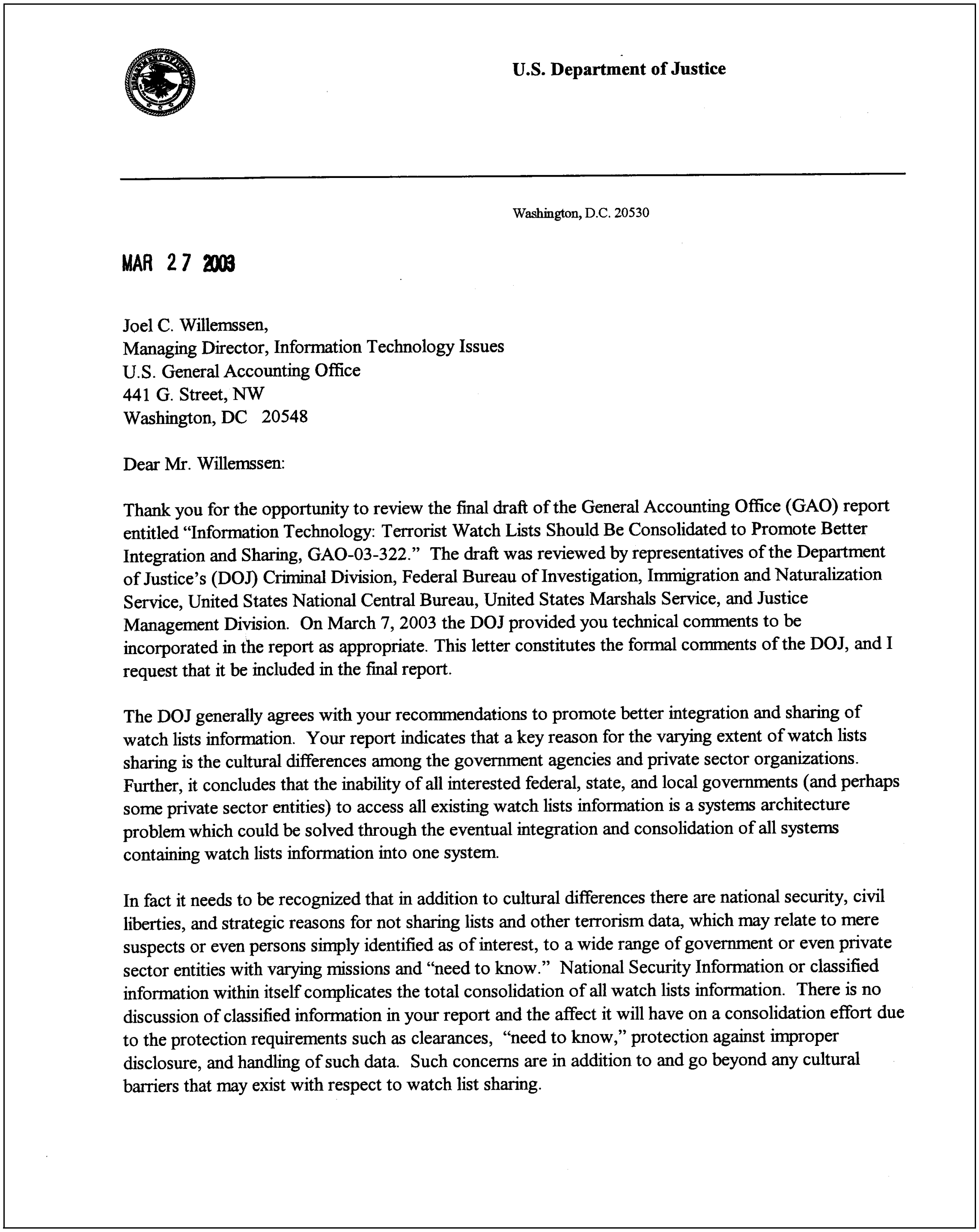
Next, we compiled the agencies' responses to determine the number of watch lists being used, confirm the universe of agencies that have lists, and determine the number of organizations that use the lists and the kinds of data the lists contain. We also analyzed the agencies' policies and procedures governing watch list sharing. In addition, we reviewed the survey responses to determine the degree of sharing among federal, state, local, and private-sector entities, and we compared the extent of sharing with the sharing goals contained in the President's homeland security strategy and the Homeland Security Act of 2002. Moreover, we aggregated the agencies' descriptions of their watch list systems architectures and analyzed them to identify similarities and differences. We also analyzed the architectural components of the watch list systems and compared them with the standards required for systems to interoperate and share data efficiently and effectively. Finally, we analyzed the agencies' responses on watch list consolidation, to identify whether there were opportunities for consolidating watch lists and, if so, what the benefits were of doing so.

Additionally, we reviewed the President's homeland security strategy, homeland security legislation and agency budget requests, and other public documents to identify federal government efforts related to maintaining and sharing watch lists. We also attended conferences and other public events at which Office of Homeland Security officials spoke on homeland security enterprise architecture and watch list standardization and consolidation efforts. We attempted to meet with Office of Homeland Security officials, but they declined to meet with us. As a result, we submitted written questions to the Office of Homeland Security, but received no response.

We conducted our work at the headquarters of the nine federal agencies identified above, in and around the Washington, D.C., metropolitan area, from July 2002 through March 2003, in accordance with generally accepted government auditing standards.

Appendix II

Comments from the Department of Justice



U.S. Department of Justice

Washington, D.C. 20530

MAR 27 2003

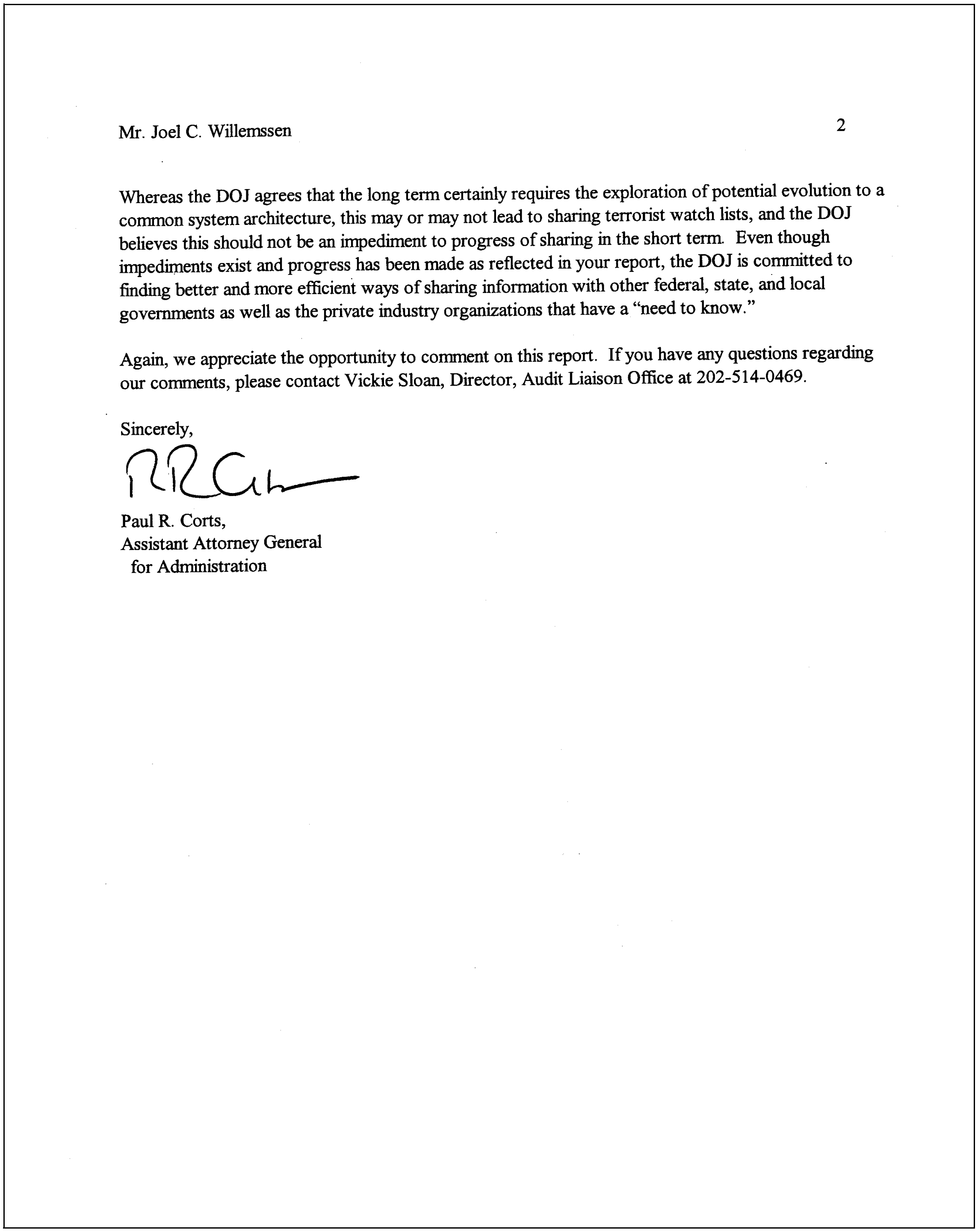
Joel C. Willemssen,
Managing Director, Information Technology Issues
U.S. General Accounting Office
441 G. Street, NW
Washington, DC 20548

Dear Mr. Willemssen:

Thank you for the opportunity to review the final draft of the General Accounting Office (GAO) report entitled “Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing, GAO-03-322.” The draft was reviewed by representatives of the Department of Justice’s (DOJ) Criminal Division, Federal Bureau of Investigation, Immigration and Naturalization Service, United States National Central Bureau, United States Marshals Service, and Justice Management Division. On March 7, 2003 the DOJ provided you technical comments to be incorporated in the report as appropriate. This letter constitutes the formal comments of the DOJ, and I request that it be included in the final report.

The DOJ generally agrees with your recommendations to promote better integration and sharing of watch lists information. Your report indicates that a key reason for the varying extent of watch lists sharing is the cultural differences among the government agencies and private sector organizations. Further, it concludes that the inability of all interested federal, state, and local governments (and perhaps some private sector entities) to access all existing watch lists information is a systems architecture problem which could be solved through the eventual integration and consolidation of all systems containing watch lists information into one system.

In fact it needs to be recognized that in addition to cultural differences there are national security, civil liberties, and strategic reasons for not sharing lists and other terrorism data, which may relate to mere suspects or even persons simply identified as of interest, to a wide range of government or even private sector entities with varying missions and “need to know.” National Security Information or classified information within itself complicates the total consolidation of all watch lists information. There is no discussion of classified information in your report and the affect it will have on a consolidation effort due to the protection requirements such as clearances, “need to know,” protection against improper disclosure, and handling of such data. Such concerns are in addition to and go beyond any cultural barriers that may exist with respect to watch list sharing.



Mr. Joel C. Willemssen 2

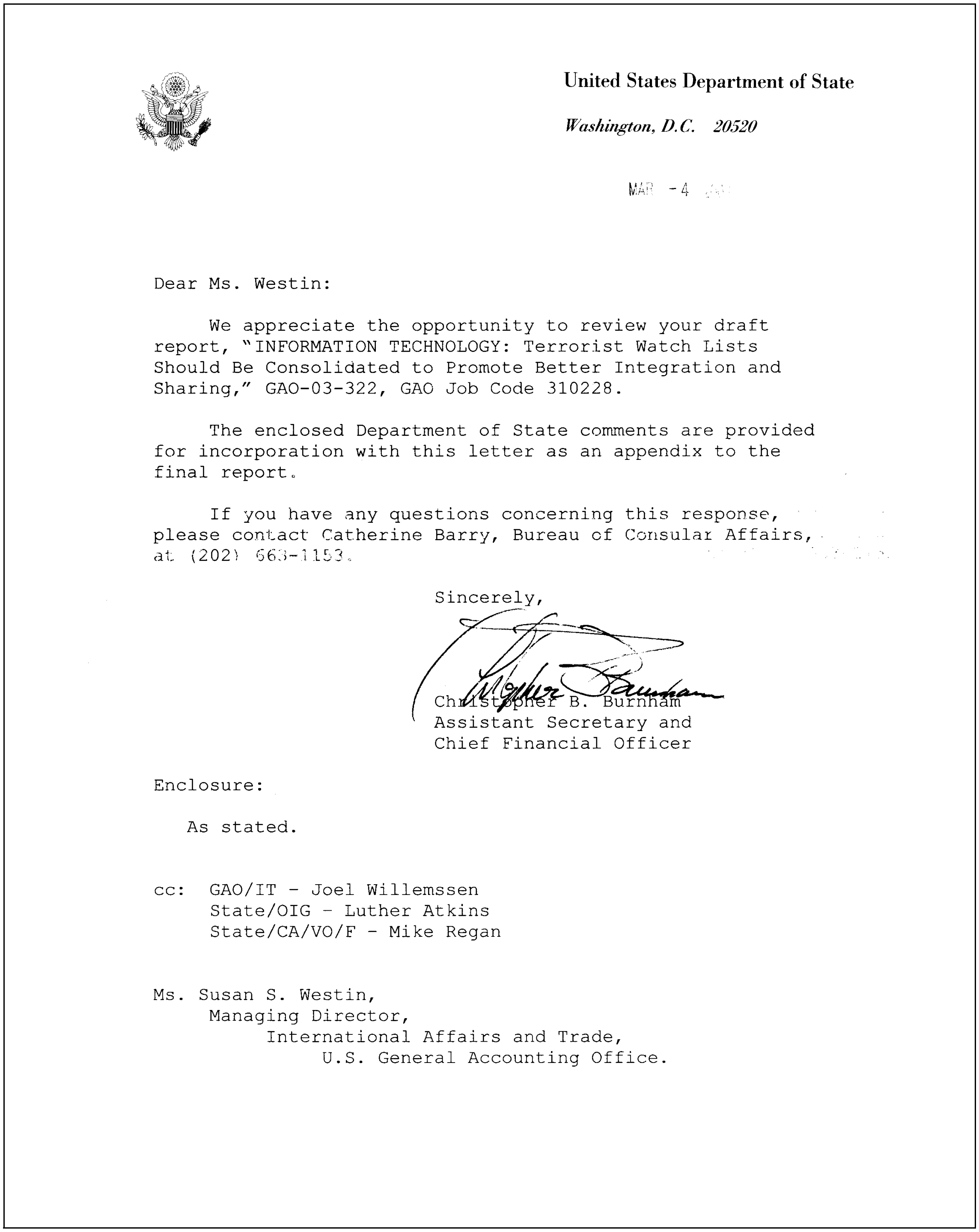
Whereas the DOJ agrees that the long term certainly requires the exploration of potential evolution to a common system architecture, this may or may not lead to sharing terrorist watch lists, and the DOJ believes this should not be an impediment to progress of sharing in the short term. Even though impediments exist and progress has been made as reflected in your report, the DOJ is committed to finding better and more efficient ways of sharing information with other federal, state, and local governments as well as the private industry organizations that have a "need to know."

Again, we appreciate the opportunity to comment on this report. If you have any questions regarding our comments, please contact Vickie Sloan, Director, Audit Liaison Office at 202-514-0469.

Sincerely,

Paul R. Corts,
Assistant Attorney General
for Administration

Comments from the Department of State



United States Department of State

Washington, D.C. 20520

MAR -4 [illegible]

Dear Ms. Westin:

We appreciate the opportunity to review your draft report, "INFORMATION TECHNOLOGY: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing," GAO-03-322, GAO Job Code 310228.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

If you have any questions concerning this response, please contact Catherine Barry, Bureau of Consular Affairs, at (202) 663-1153.

Sincerely,

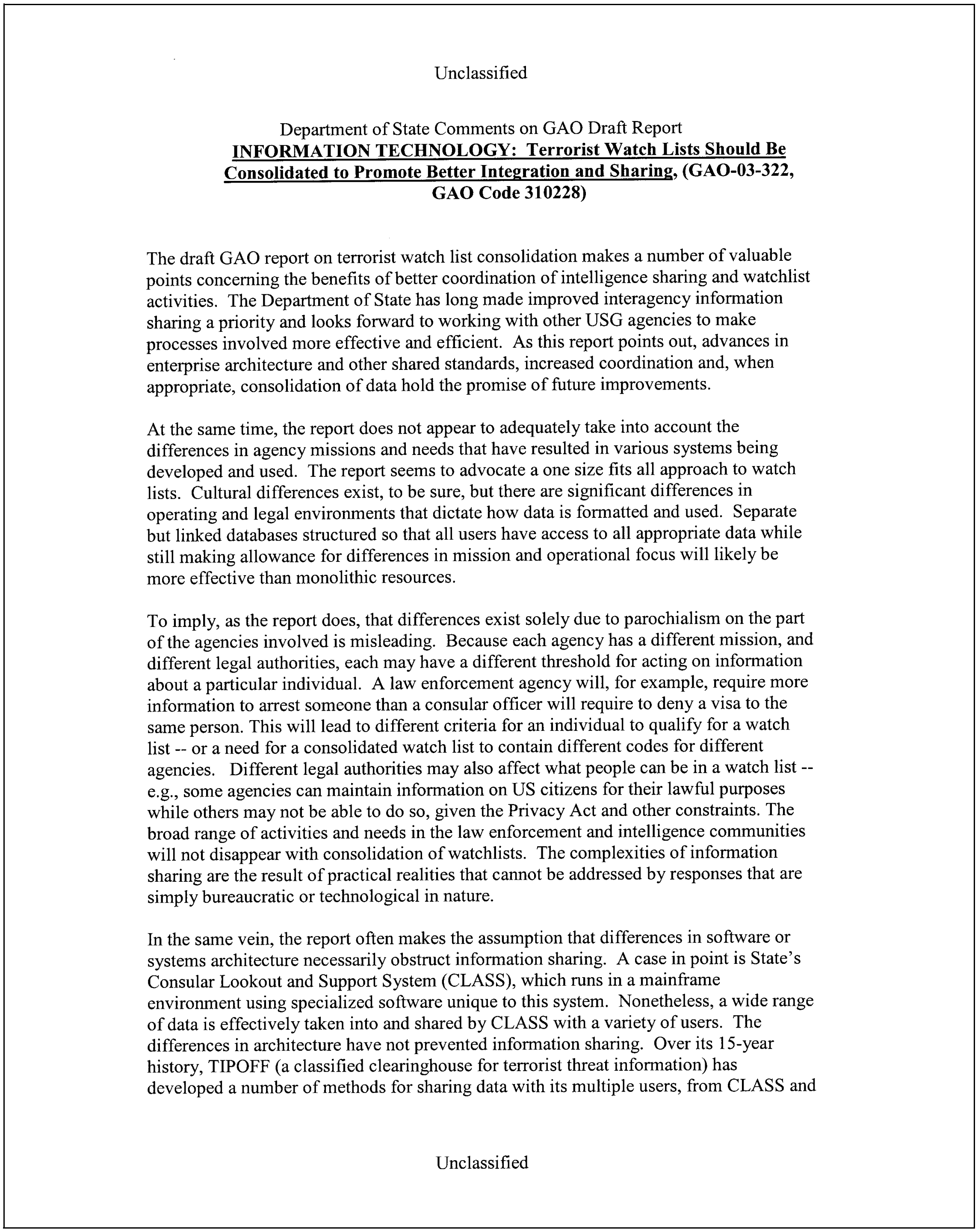
Christopher B. Burnham
Assistant Secretary and
Chief Financial Officer

Enclosure:

As stated.

cc: GAO/IT - Joel Willemssen
State/OIG - Luther Atkins
State/CA/VO/F - Mike Regan

Ms. Susan S. Westin,
Managing Director,
International Affairs and Trade,
U.S. General Accounting Office.



Unclassified

Department of State Comments on GAO Draft Report
INFORMATION TECHNOLOGY: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing, (GAO-03-322, GAO Code 310228)

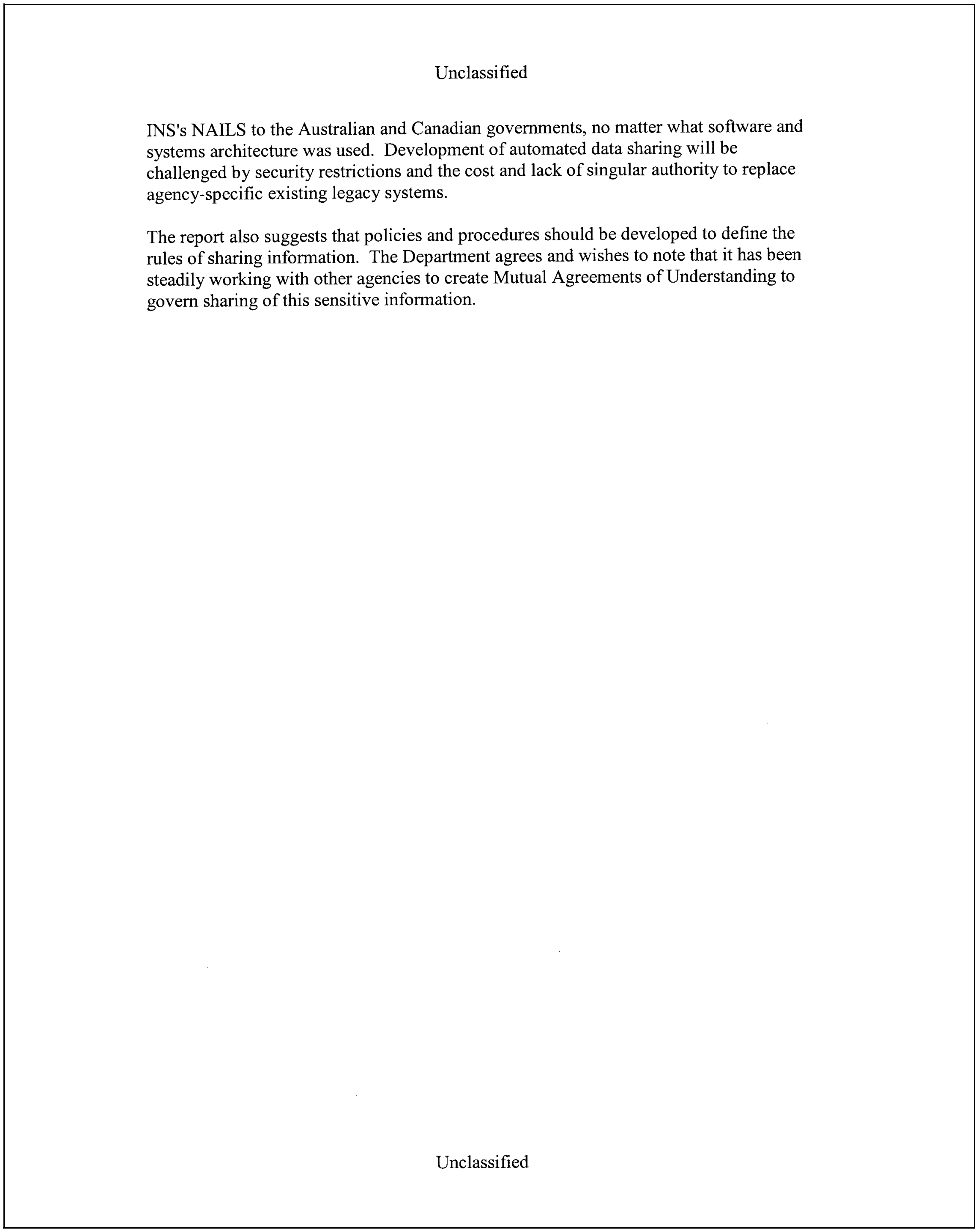
The draft GAO report on terrorist watch list consolidation makes a number of valuable points concerning the benefits of better coordination of intelligence sharing and watchlist activities. The Department of State has long made improved interagency information sharing a priority and looks forward to working with other USG agencies to make processes involved more effective and efficient. As this report points out, advances in enterprise architecture and other shared standards, increased coordination and, when appropriate, consolidation of data hold the promise of future improvements.

At the same time, the report does not appear to adequately take into account the differences in agency missions and needs that have resulted in various systems being developed and used. The report seems to advocate a one size fits all approach to watch lists. Cultural differences exist, to be sure, but there are significant differences in operating and legal environments that dictate how data is formatted and used. Separate but linked databases structured so that all users have access to all appropriate data while still making allowance for differences in mission and operational focus will likely be more effective than monolithic resources.

To imply, as the report does, that differences exist solely due to parochialism on the part of the agencies involved is misleading. Because each agency has a different mission, and different legal authorities, each may have a different threshold for acting on information about a particular individual. A law enforcement agency will, for example, require more information to arrest someone than a consular officer will require to deny a visa to the same person. This will lead to different criteria for an individual to qualify for a watch list -- or a need for a consolidated watch list to contain different codes for different agencies. Different legal authorities may also affect what people can be in a watch list -- e.g., some agencies can maintain information on US citizens for their lawful purposes while others may not be able to do so, given the Privacy Act and other constraints. The broad range of activities and needs in the law enforcement and intelligence communities will not disappear with consolidation of watchlists. The complexities of information sharing are the result of practical realities that cannot be addressed by responses that are simply bureaucratic or technological in nature.

In the same vein, the report often makes the assumption that differences in software or systems architecture necessarily obstruct information sharing. A case in point is State's Consular Lookout and Support System (CLASS), which runs in a mainframe environment using specialized software unique to this system. Nonetheless, a wide range of data is effectively taken into and shared by CLASS with a variety of users. The differences in architecture have not prevented information sharing. Over its 15-year history, TIPOFF (a classified clearinghouse for terrorist threat information) has developed a number of methods for sharing data with its multiple users, from CLASS and

Unclassified

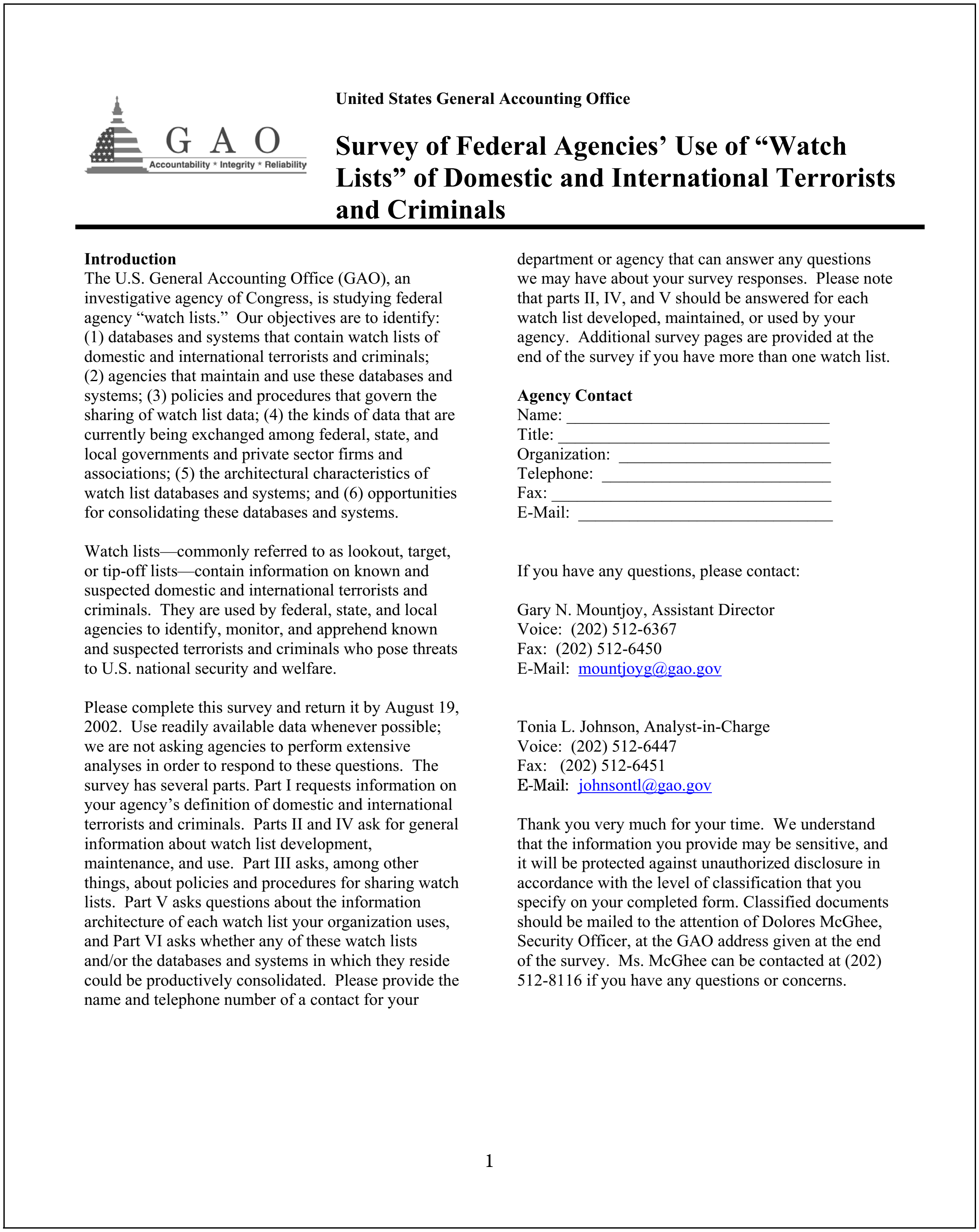


INS's NAILS to the Australian and Canadian governments, no matter what software and systems architecture was used. Development of automated data sharing will be challenged by security restrictions and the cost and lack of singular authority to replace agency-specific existing legacy systems.

The report also suggests that policies and procedures should be developed to define the rules of sharing information. The Department agrees and wishes to note that it has been steadily working with other agencies to create Mutual Agreements of Understanding to govern sharing of this sensitive information.

Appendix IV

GAO's Survey Instrument



United States General Accounting Office

Survey of Federal Agencies' Use of "Watch Lists" of Domestic and International Terrorists and Criminals

Introduction
The U.S. General Accounting Office (GAO), an investigative agency of Congress, is studying federal agency "watch lists." Our objectives are to identify: (1) databases and systems that contain watch lists of domestic and international terrorists and criminals; (2) agencies that maintain and use these databases and systems; (3) policies and procedures that govern the sharing of watch list data; (4) the kinds of data that are currently being exchanged among federal, state, and local governments and private sector firms and associations; (5) the architectural characteristics of watch list databases and systems; and (6) opportunities for consolidating these databases and systems.

Watch lists—commonly referred to as lookout, target, or tip-off lists—contain information on known and suspected domestic and international terrorists and criminals. They are used by federal, state, and local agencies to identify, monitor, and apprehend known and suspected terrorists and criminals who pose threats to U.S. national security and welfare.

Please complete this survey and return it by August 19, 2002. Use readily available data whenever possible; we are not asking agencies to perform extensive analyses in order to respond to these questions. The survey has several parts. Part I requests information on your agency's definition of domestic and international terrorists and criminals. Parts II and IV ask for general information about watch list development, maintenance, and use. Part III asks, among other things, about policies and procedures for sharing watch lists. Part V asks questions about the information architecture of each watch list your organization uses, and Part VI asks whether any of these watch lists and/or the databases and systems in which they reside could be productively consolidated. Please provide the name and telephone number of a contact for your department or agency that can answer any questions we may have about your survey responses. Please note that parts II, IV, and V should be answered for each watch list developed, maintained, or used by your agency. Additional survey pages are provided at the end of the survey if you have more than one watch list.

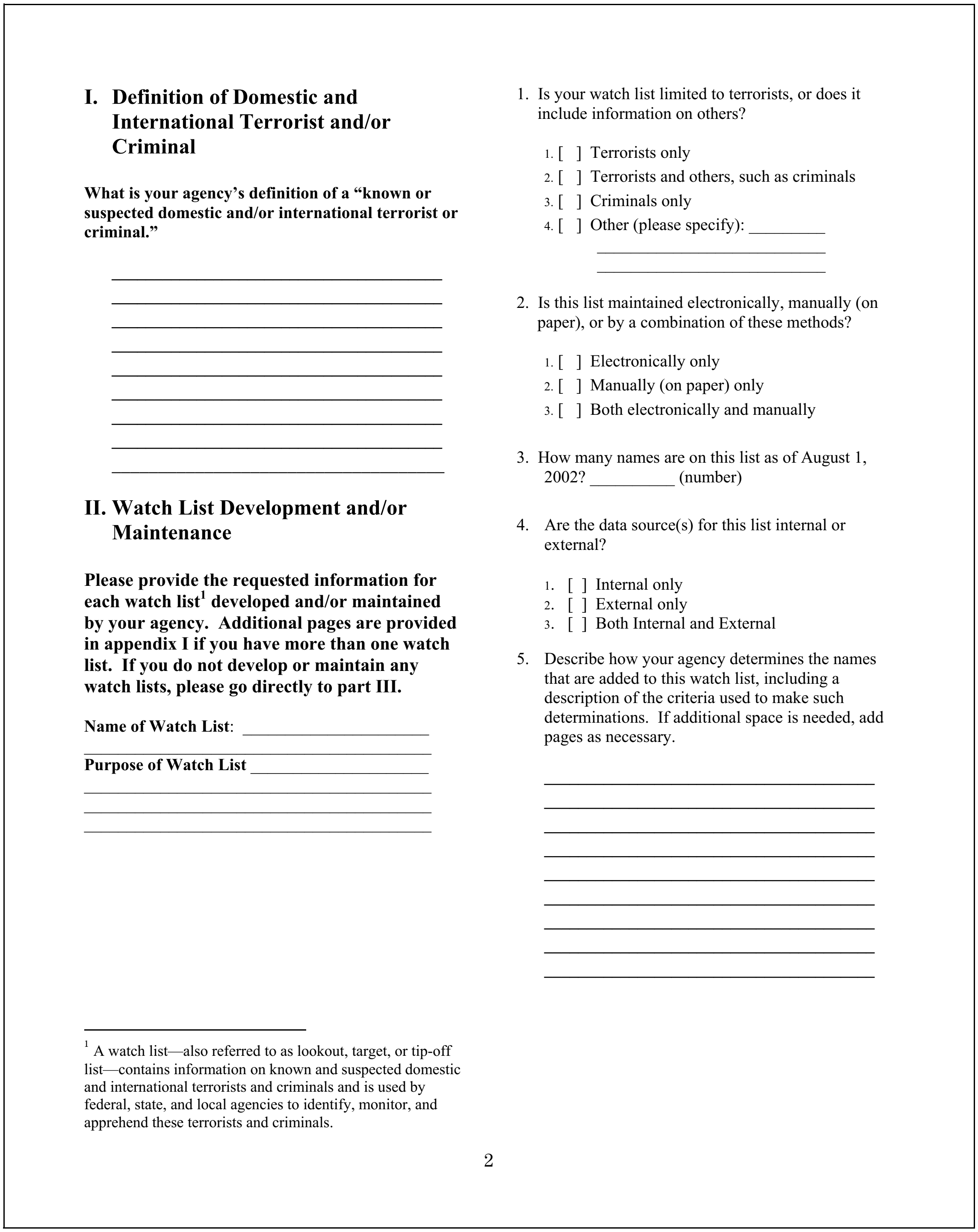
Agency Contact
Name: ______________________________
Title: ______________________________
Organization: ________________________
Telephone: __________________________
Fax: _______________________________
E-Mail: _____________________________

If you have any questions, please contact:

Gary N. Mountjoy, Assistant Director
Voice: (202) 512-6367
Fax: (202) 512-6450
E-Mail: mountjoyg@gao.gov

Tonia L. Johnson, Analyst-in-Charge
Voice: (202) 512-6447
Fax: (202) 512-6451
E-Mail: johnsontl@gao.gov

Thank you very much for your time. We understand that the information you provide may be sensitive, and it will be protected against unauthorized disclosure in accordance with the level of classification that you specify on your completed form. Classified documents should be mailed to the attention of Dolores McGhee, Security Officer, at the GAO address given at the end of the survey. Ms. McGhee can be contacted at (202) 512-8116 if you have any questions or concerns.



I. Definition of Domestic and International Terrorist and/or Criminal

What is your agency's definition of a "known or suspected domestic and/or international terrorist or criminal."

____
____
____
____
____
____
____
____
____

II. Watch List Development and/or Maintenance

Please provide the requested information for each watch list[1] developed and/or maintained by your agency. Additional pages are provided in appendix I if you have more than one watch list. If you do not develop or maintain any watch lists, please go directly to part III.

Name of Watch List: ______________________
____

Purpose of Watch List ____________________
____
____
____

1. Is your watch list limited to terrorists, or does it include information on others?

   1. [ ] Terrorists only
   2. [ ] Terrorists and others, such as criminals
   3. [ ] Criminals only
   4. [ ] Other (please specify): _________
      ____
      ____

2. Is this list maintained electronically, manually (on paper), or by a combination of these methods?

   1. [ ] Electronically only
   2. [ ] Manually (on paper) only
   3. [ ] Both electronically and manually

3. How many names are on this list as of August 1, 2002? __________ (number)

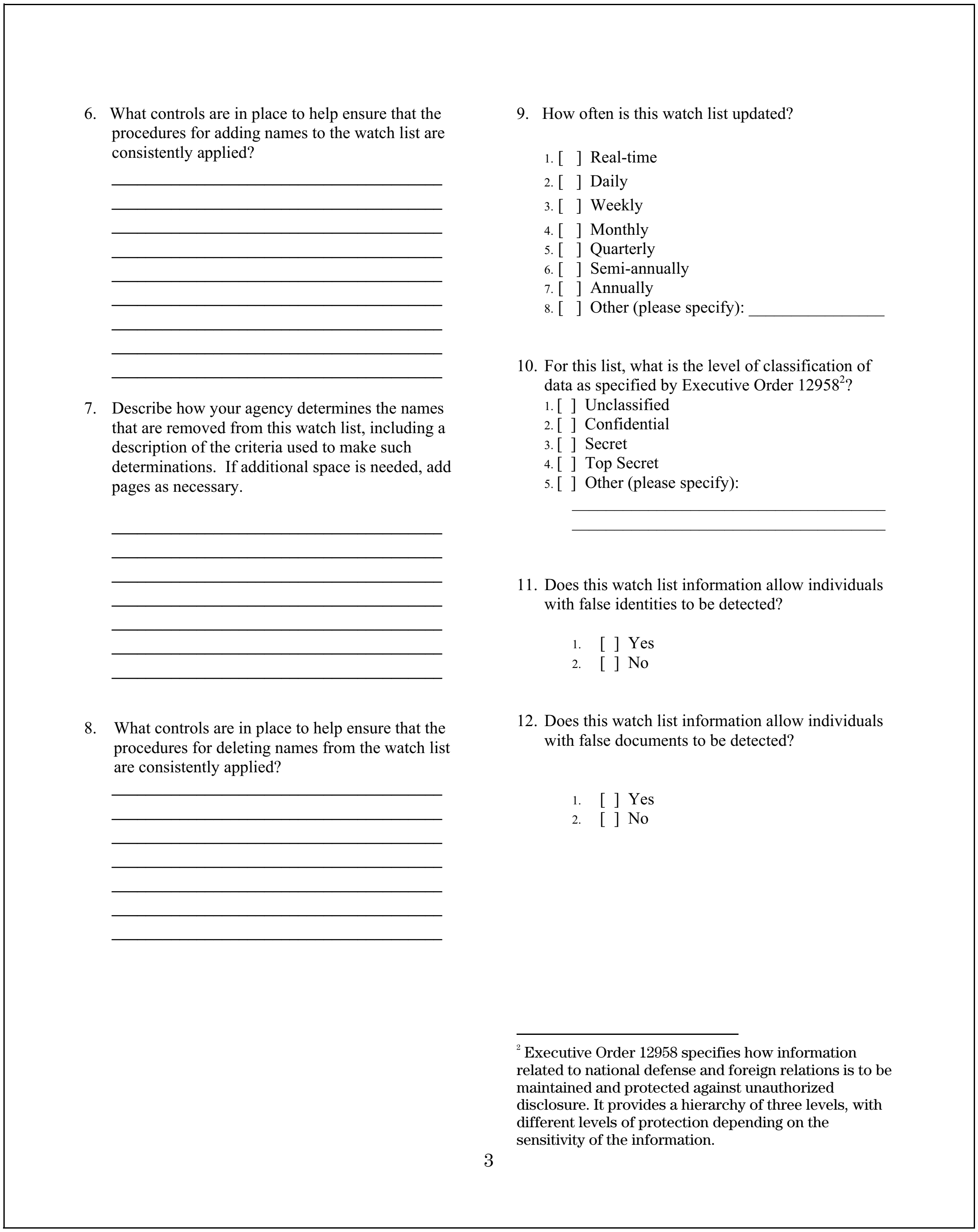
4. Are the data source(s) for this list internal or external?

   1. [ ] Internal only
   2. [ ] External only
   3. [ ] Both Internal and External

5. Describe how your agency determines the names that are added to this watch list, including a description of the criteria used to make such determinations. If additional space is needed, add pages as necessary.

____
____
____
____
____
____
____
____
____

[1] A watch list—also referred to as lookout, target, or tip-off list—contains information on known and suspected domestic and international terrorists and criminals and is used by federal, state, and local agencies to identify, monitor, and apprehend these terrorists and criminals.



6. What controls are in place to help ensure that the procedures for adding names to the watch list are consistently applied?

____
____
____
____
____
____
____
____
____

7. Describe how your agency determines the names that are removed from this watch list, including a description of the criteria used to make such determinations. If additional space is needed, add pages as necessary.

____
____
____
____
____
____
____

8. What controls are in place to help ensure that the procedures for deleting names from the watch list are consistently applied?

____
____
____
____
____
____
____

9. How often is this watch list updated?

1. [ ] Real-time
2. [ ] Daily
3. [ ] Weekly
4. [ ] Monthly
5. [ ] Quarterly
6. [ ] Semi-annually
7. [ ] Annually
8. [ ] Other (please specify): ________________

10. For this list, what is the level of classification of data as specified by Executive Order 12958[2]?

1. [ ] Unclassified
2. [ ] Confidential
3. [ ] Secret
4. [ ] Top Secret
5. [ ] Other (please specify):

____
____

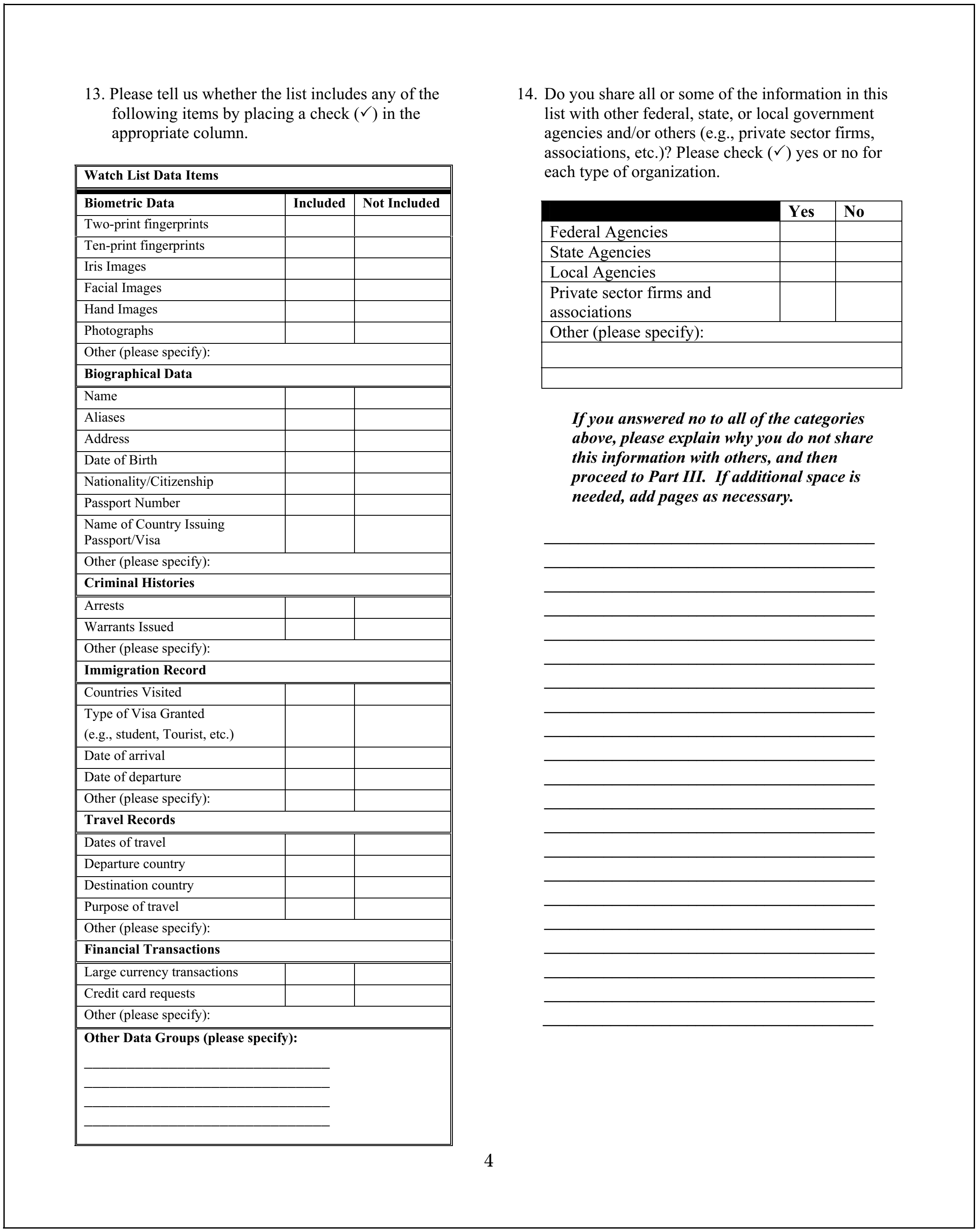
11. Does this watch list information allow individuals with false identities to be detected?

1. [ ] Yes
2. [ ] No

12. Does this watch list information allow individuals with false documents to be detected?

1. [ ] Yes
2. [ ] No

[2] Executive Order 12958 specifies how information related to national defense and foreign relations is to be maintained and protected against unauthorized disclosure. It provides a hierarchy of three levels, with different levels of protection depending on the sensitivity of the information.



13. Please tell us whether the list includes any of the following items by placing a check (✓) in the appropriate column.

Watch List Data Items		
Biometric Data	**Included**	**Not Included**
Two-print fingerprints		
Ten-print fingerprints		
Iris Images		
Facial Images		
Hand Images		
Photographs		
Other (please specify):		
Biographical Data		
Name		
Aliases		
Address		
Date of Birth		
Nationality/Citizenship		
Passport Number		
Name of Country Issuing Passport/Visa		
Other (please specify):		
Criminal Histories		
Arrests		
Warrants Issued		
Other (please specify):		
Immigration Record		
Countries Visited		
Type of Visa Granted (e.g., student, Tourist, etc.)		
Date of arrival		
Date of departure		
Other (please specify):		
Travel Records		
Dates of travel		
Departure country		
Destination country		
Purpose of travel		
Other (please specify):		
Financial Transactions		
Large currency transactions		
Credit card requests		
Other (please specify):		
Other Data Groups (please specify): ______________________________ ______________________________ ______________________________ ______________________________		

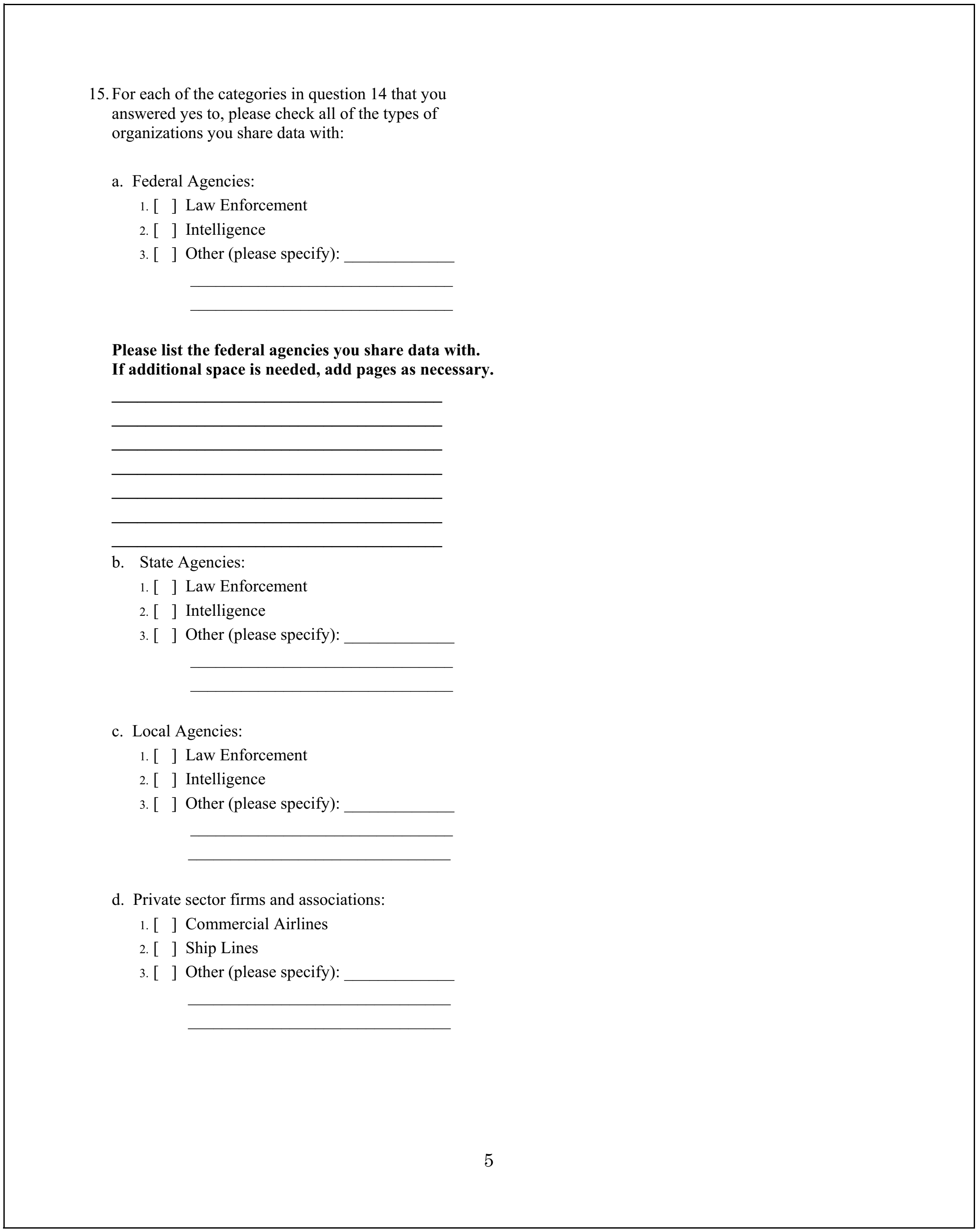
14. Do you share all or some of the information in this list with other federal, state, or local government agencies and/or others (e.g., private sector firms, associations, etc.)? Please check (✓) yes or no for each type of organization.

	Yes	No
Federal Agencies		
State Agencies		
Local Agencies		
Private sector firms and associations		
Other (please specify):		

If you answered no to all of the categories above, please explain why you do not share this information with others, and then proceed to Part III. If additional space is needed, add pages as necessary.

____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____

4



15. For each of the categories in question 14 that you answered yes to, please check all of the types of organizations you share data with:

a. Federal Agencies:
1. [ ] Law Enforcement
2. [ ] Intelligence
3. [ ] Other (please specify): _____________
____
____

Please list the federal agencies you share data with.
If additional space is needed, add pages as necessary.

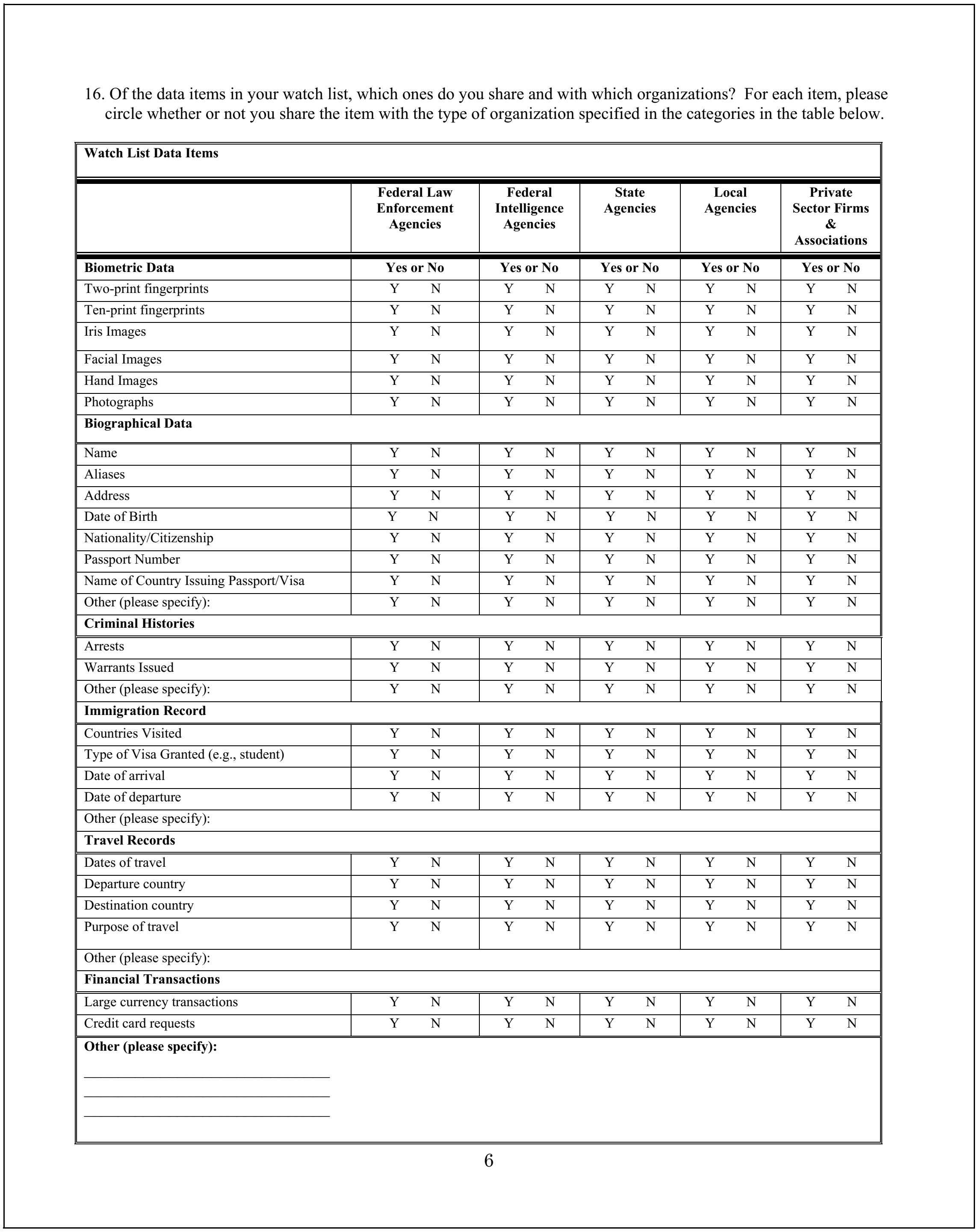
____
____
____
____
____
____
____

b. State Agencies:
1. [ ] Law Enforcement
2. [ ] Intelligence
3. [ ] Other (please specify): _____________
____
____

c. Local Agencies:
1. [ ] Law Enforcement
2. [ ] Intelligence
3. [ ] Other (please specify): _____________
____
____

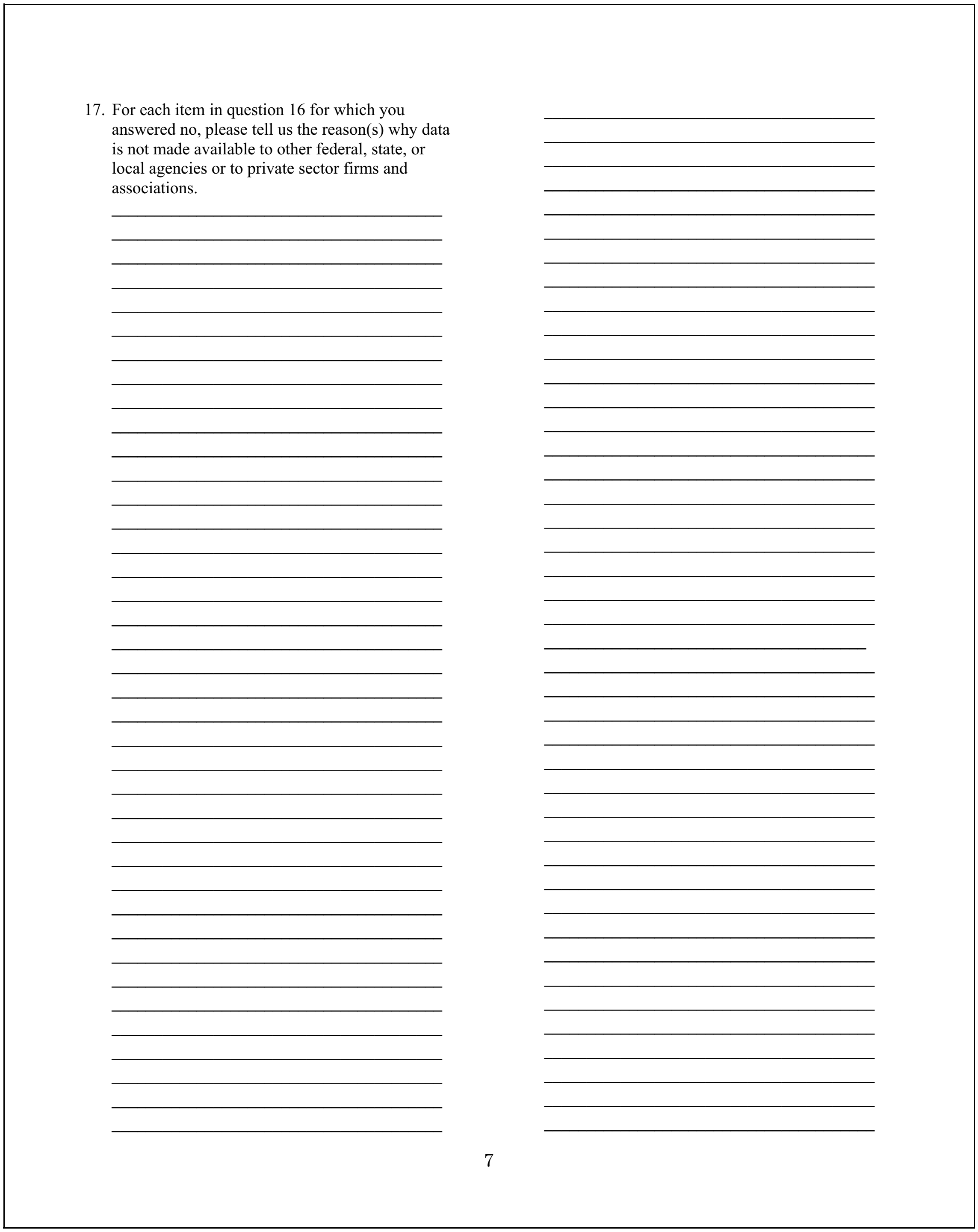
d. Private sector firms and associations:
1. [ ] Commercial Airlines
2. [ ] Ship Lines
3. [ ] Other (please specify): _____________
____
____

5



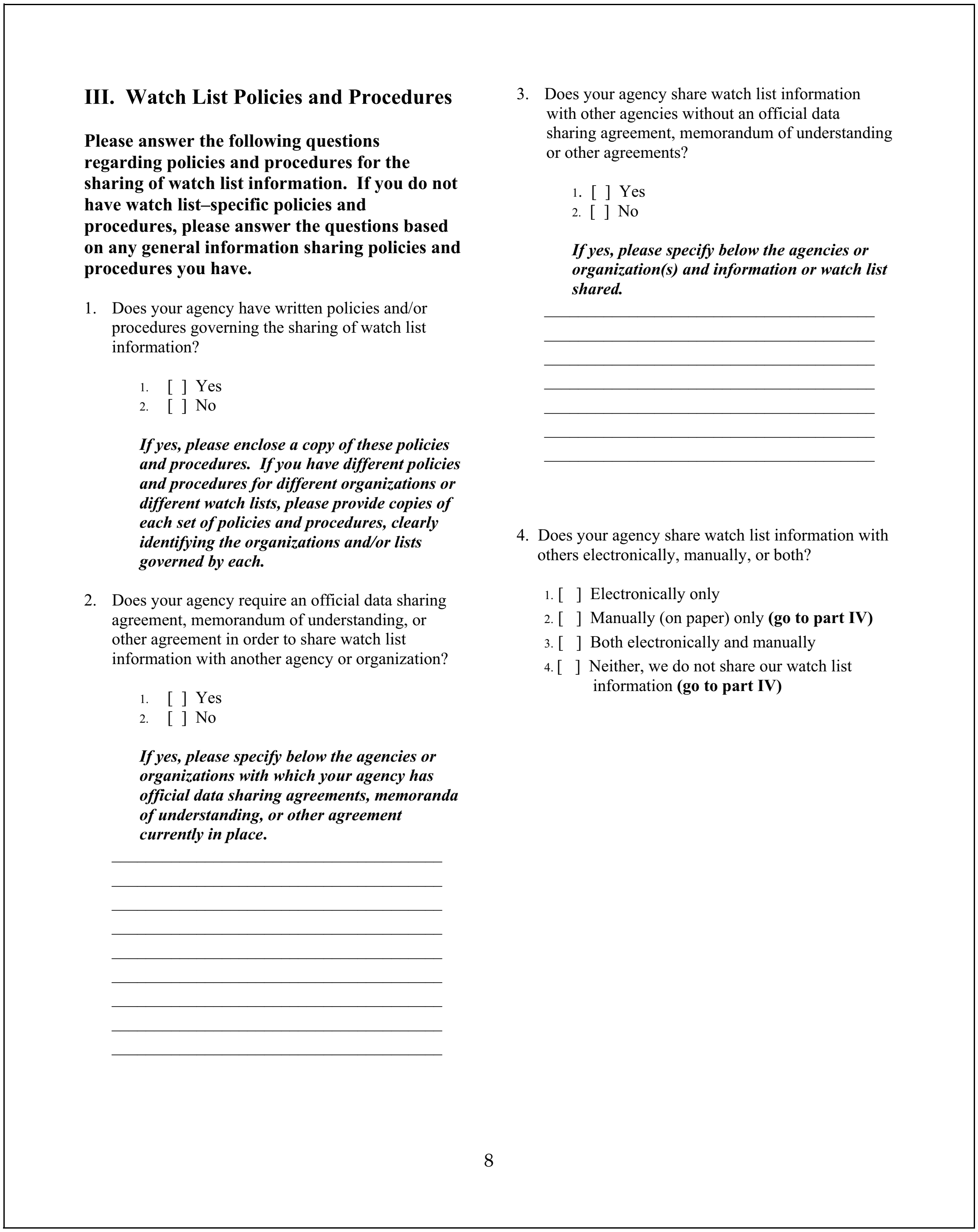
16. Of the data items in your watch list, which ones do you share and with which organizations? For each item, please circle whether or not you share the item with the type of organization specified in the categories in the table below.

Watch List Data Items					
	Federal Law Enforcement Agencies	**Federal Intelligence Agencies**	**State Agencies**	**Local Agencies**	**Private Sector Firms & Associations**
Biometric Data	**Yes or No**	**Yes or No**	**Yes or No**	**Yes or No**	**Yes or No**
Two-print fingerprints	Y N	Y N	Y N	Y N	Y N
Ten-print fingerprints	Y N	Y N	Y N	Y N	Y N
Iris Images	Y N	Y N	Y N	Y N	Y N
Facial Images	Y N	Y N	Y N	Y N	Y N
Hand Images	Y N	Y N	Y N	Y N	Y N
Photographs	Y N	Y N	Y N	Y N	Y N
Biographical Data					
Name	Y N	Y N	Y N	Y N	Y N
Aliases	Y N	Y N	Y N	Y N	Y N
Address	Y N	Y N	Y N	Y N	Y N
Date of Birth	Y N	Y N	Y N	Y N	Y N
Nationality/Citizenship	Y N	Y N	Y N	Y N	Y N
Passport Number	Y N	Y N	Y N	Y N	Y N
Name of Country Issuing Passport/Visa	Y N	Y N	Y N	Y N	Y N
Other (please specify):	Y N	Y N	Y N	Y N	Y N
Criminal Histories					
Arrests	Y N	Y N	Y N	Y N	Y N
Warrants Issued	Y N	Y N	Y N	Y N	Y N
Other (please specify):	Y N	Y N	Y N	Y N	Y N
Immigration Record					
Countries Visited	Y N	Y N	Y N	Y N	Y N
Type of Visa Granted (e.g., student)	Y N	Y N	Y N	Y N	Y N
Date of arrival	Y N	Y N	Y N	Y N	Y N
Date of departure	Y N	Y N	Y N	Y N	Y N
Other (please specify):					
Travel Records					
Dates of travel	Y N	Y N	Y N	Y N	Y N
Departure country	Y N	Y N	Y N	Y N	Y N
Destination country	Y N	Y N	Y N	Y N	Y N
Purpose of travel	Y N	Y N	Y N	Y N	Y N
Other (please specify):					
Financial Transactions					
Large currency transactions	Y N	Y N	Y N	Y N	Y N
Credit card requests	Y N	Y N	Y N	Y N	Y N
Other (please specify): ____________________________ ____________________________ ____________________________					



17. For each item in question 16 for which you answered no, please tell us the reason(s) why data is not made available to other federal, state, or local agencies or to private sector firms and associations.

7



III. Watch List Policies and Procedures

Please answer the following questions regarding policies and procedures for the sharing of watch list information. If you do not have watch list–specific policies and procedures, please answer the questions based on any general information sharing policies and procedures you have.

1. Does your agency have written policies and/or procedures governing the sharing of watch list information?

   1. [ ] Yes
   2. [ ] No

   If yes, please enclose a copy of these policies and procedures. If you have different policies and procedures for different organizations or different watch lists, please provide copies of each set of policies and procedures, clearly identifying the organizations and/or lists governed by each.

2. Does your agency require an official data sharing agreement, memorandum of understanding, or other agreement in order to share watch list information with another agency or organization?

   1. [ ] Yes
   2. [ ] No

   If yes, please specify below the agencies or organizations with which your agency has official data sharing agreements, memoranda of understanding, or other agreement currently in place.

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

3. Does your agency share watch list information with other agencies without an official data sharing agreement, memorandum of understanding or other agreements?

   1. [ ] Yes
   2. [ ] No

   If yes, please specify below the agencies or organization(s) and information or watch list shared.

   ____

   ____

   ____

   ____

   ____

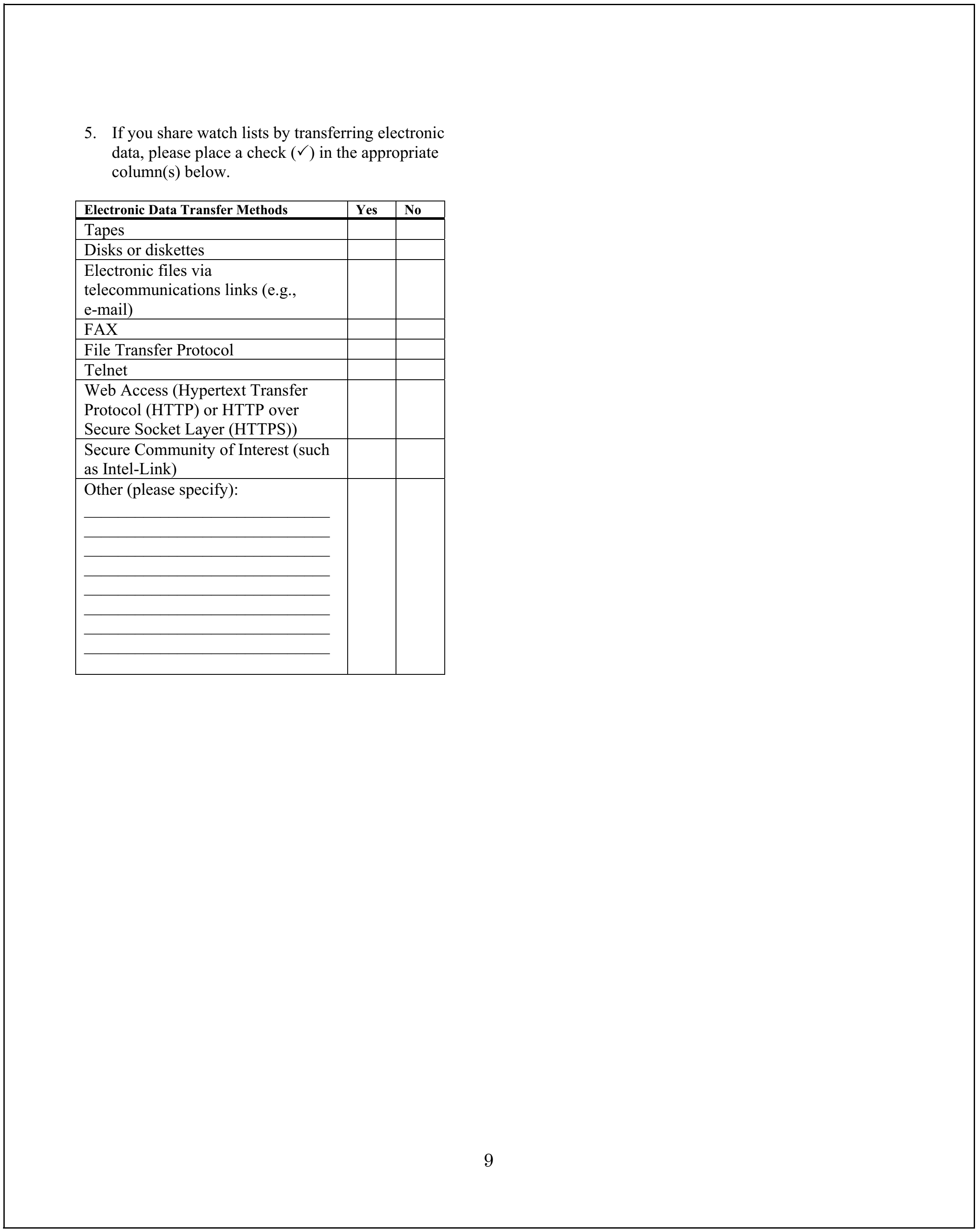
   ____

   ____

4. Does your agency share watch list information with others electronically, manually, or both?

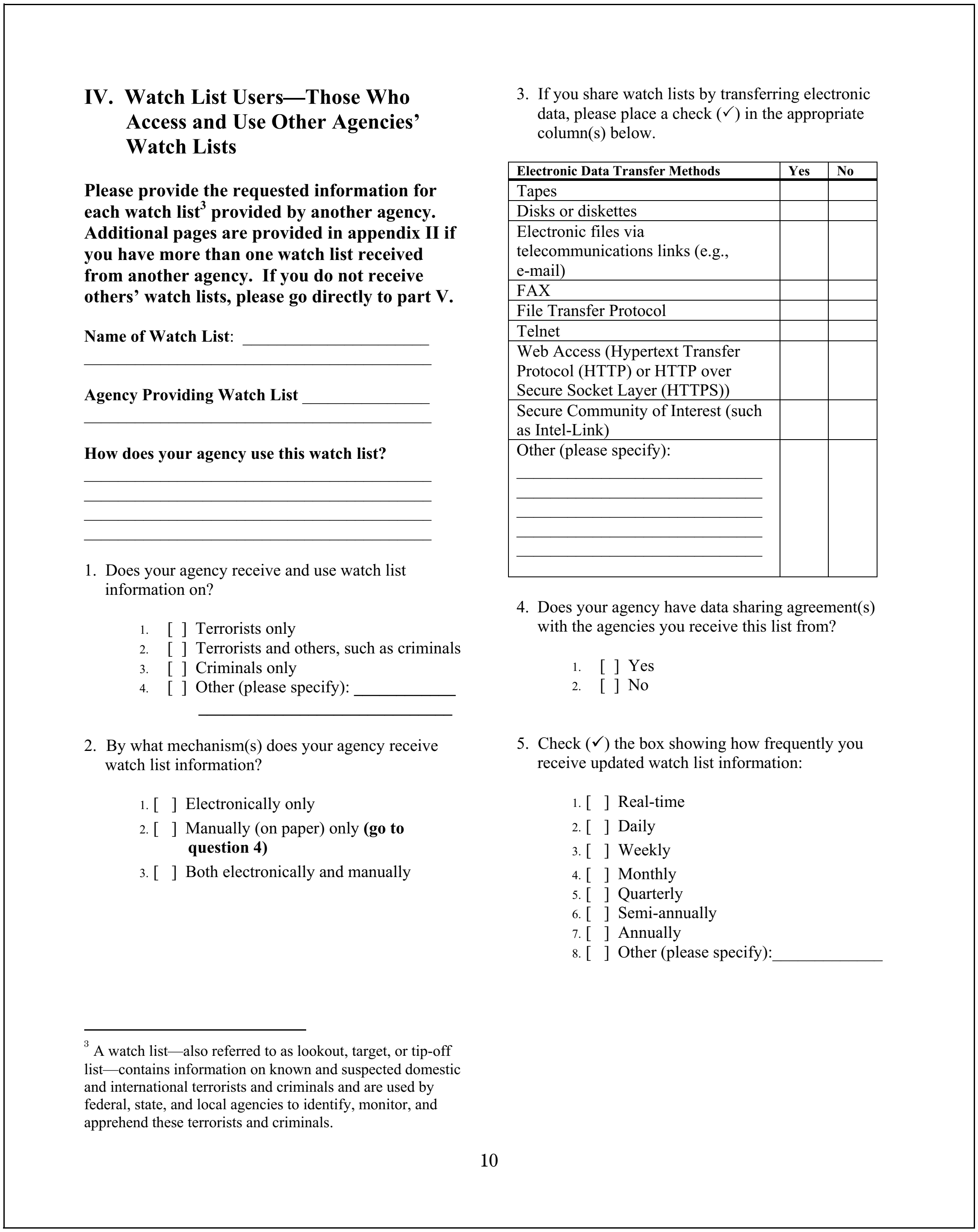
   1. [ ] Electronically only
   2. [ ] Manually (on paper) only **(go to part IV)**
   3. [ ] Both electronically and manually
   4. [ ] Neither, we do not share our watch list information **(go to part IV)**

8



5. If you share watch lists by transferring electronic data, please place a check (✓) in the appropriate column(s) below.

Electronic Data Transfer Methods	Yes	No
Tapes		
Disks or diskettes		
Electronic files via telecommunications links (e.g., e-mail)		
FAX		
File Transfer Protocol		
Telnet		
Web Access (Hypertext Transfer Protocol (HTTP) or HTTP over Secure Socket Layer (HTTPS))		
Secure Community of Interest (such as Intel-Link)		
Other (please specify): ______________________________ ______________________________ ______________________________ ______________________________ ______________________________ ______________________________ ______________________________ ______________________________		



IV. Watch List Users—Those Who Access and Use Other Agencies' Watch Lists

Please provide the requested information for each watch list[3] provided by another agency. Additional pages are provided in appendix II if you have more than one watch list received from another agency. If you do not receive others' watch lists, please go directly to part V.

Name of Watch List: ______________________
____

Agency Providing Watch List _______________
____

How does your agency use this watch list?
____
____
____
____

1. Does your agency receive and use watch list information on?

   1. [ ] Terrorists only
   2. [ ] Terrorists and others, such as criminals
   3. [ ] Criminals only
   4. [ ] Other (please specify): ____________
   ____

2. By what mechanism(s) does your agency receive watch list information?

   1. [ ] Electronically only
   2. [ ] Manually (on paper) only **(go to question 4)**
   3. [ ] Both electronically and manually

3. If you share watch lists by transferring electronic data, please place a check (✓) in the appropriate column(s) below.

Electronic Data Transfer Methods	Yes	No
Tapes		
Disks or diskettes		
Electronic files via telecommunications links (e.g., e-mail)		
FAX		
File Transfer Protocol		
Telnet		
Web Access (Hypertext Transfer Protocol (HTTP) or HTTP over Secure Socket Layer (HTTPS))		
Secure Community of Interest (such as Intel-Link)		
Other (please specify): ______________________________ ______________________________ ______________________________ ______________________________ ______________________________		

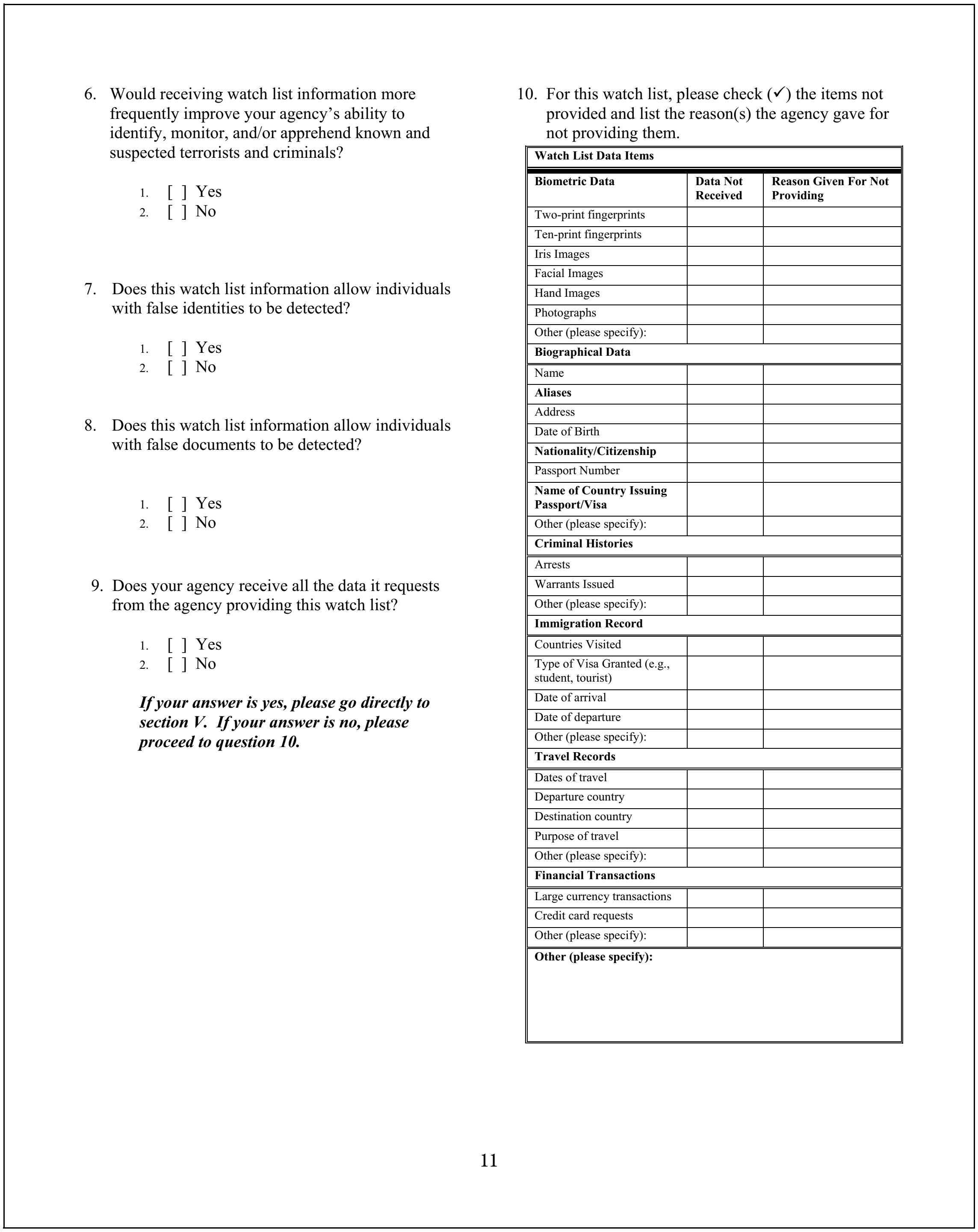
4. Does your agency have data sharing agreement(s) with the agencies you receive this list from?

   1. [ ] Yes
   2. [ ] No

5. Check (✓) the box showing how frequently you receive updated watch list information:

   1. [ ] Real-time
   2. [ ] Daily
   3. [ ] Weekly
   4. [ ] Monthly
   5. [ ] Quarterly
   6. [ ] Semi-annually
   7. [ ] Annually
   8. [ ] Other (please specify):_____________

[3] A watch list—also referred to as lookout, target, or tip-off list—contains information on known and suspected domestic and international terrorists and criminals and are used by federal, state, and local agencies to identify, monitor, and apprehend these terrorists and criminals.



6. Would receiving watch list information more frequently improve your agency's ability to identify, monitor, and/or apprehend known and suspected terrorists and criminals?

   1. [ ] Yes
   2. [ ] No

7. Does this watch list information allow individuals with false identities to be detected?

   1. [ ] Yes
   2. [ ] No

8. Does this watch list information allow individuals with false documents to be detected?

   1. [ ] Yes
   2. [ ] No

9. Does your agency receive all the data it requests from the agency providing this watch list?

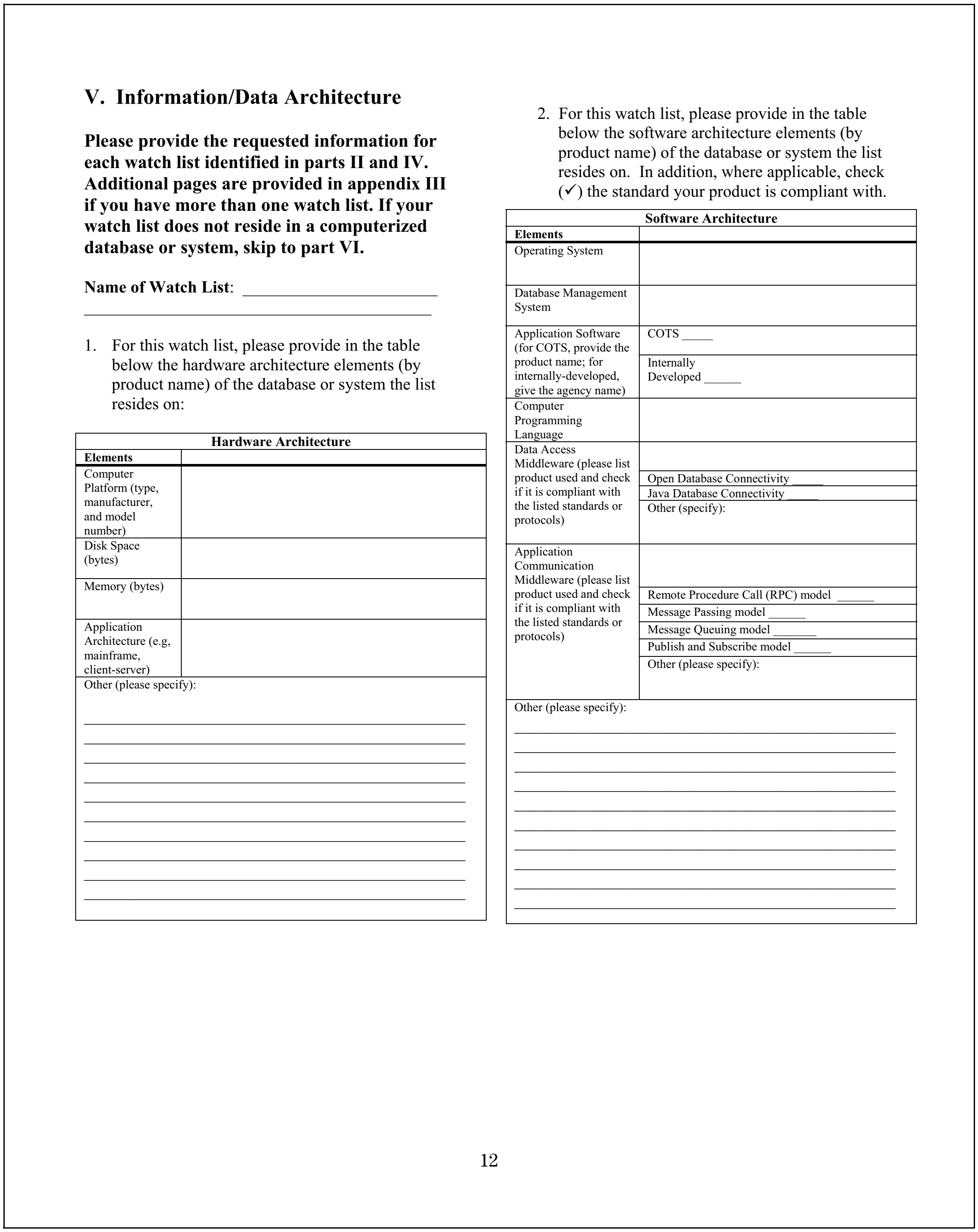
   1. [ ] Yes
   2. [ ] No

   If your answer is yes, please go directly to section V. If your answer is no, please proceed to question 10.

10. For this watch list, please check (✓) the items not provided and list the reason(s) the agency gave for not providing them.

Watch List Data Items		
Biometric Data	**Data Not Received**	**Reason Given For Not Providing**
Two-print fingerprints		
Ten-print fingerprints		
Iris Images		
Facial Images		
Hand Images		
Photographs		
Other (please specify):		
Biographical Data		
Name		
Aliases		
Address		
Date of Birth		
Nationality/Citizenship		
Passport Number		
Name of Country Issuing Passport/Visa		
Other (please specify):		
Criminal Histories		
Arrests		
Warrants Issued		
Other (please specify):		
Immigration Record		
Countries Visited		
Type of Visa Granted (e.g., student, tourist)		
Date of arrival		
Date of departure		
Other (please specify):		
Travel Records		
Dates of travel		
Departure country		
Destination country		
Purpose of travel		
Other (please specify):		
Financial Transactions		
Large currency transactions		
Credit card requests		
Other (please specify):		
Other (please specify):		

11



V. Information/Data Architecture

Please provide the requested information for each watch list identified in parts II and IV. Additional pages are provided in appendix III if you have more than one watch list. If your watch list does not reside in a computerized database or system, skip to part VI.

Name of Watch List: ________________________
____

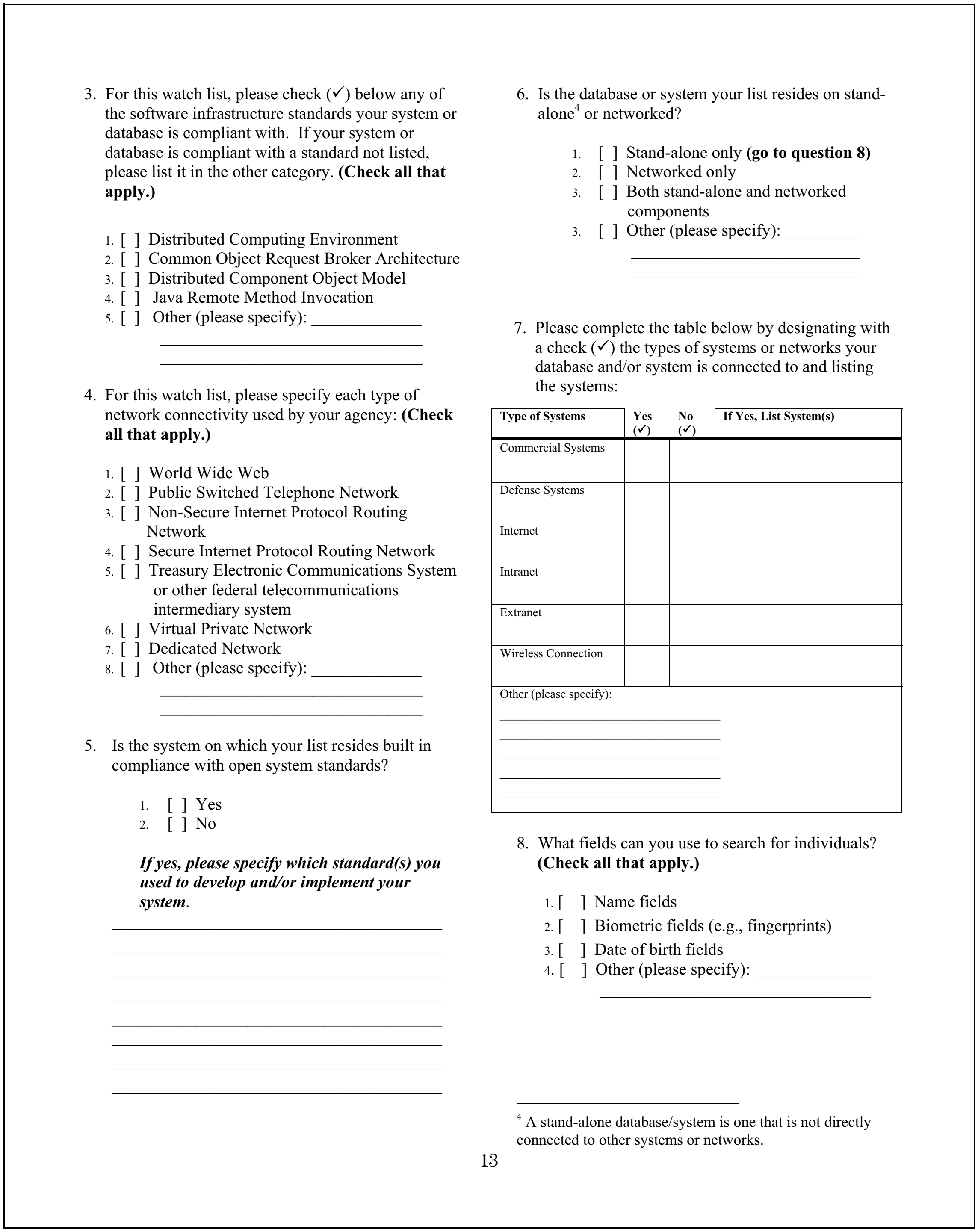
1. For this watch list, please provide in the table below the hardware architecture elements (by product name) of the database or system the list resides on:

Hardware Architecture	
Elements	
Computer Platform (type, manufacturer, and model number)	
Disk Space (bytes)	
Memory (bytes)	
Application Architecture (e.g, mainframe, client-server)	
Other (please specify):	

2. For this watch list, please provide in the table below the software architecture elements (by product name) of the database or system the list resides on. In addition, where applicable, check (✓) the standard your product is compliant with.

Software Architecture	
Elements	
Operating System	
Database Management System	
Application Software (for COTS, provide the product name; for internally-developed, give the agency name)	COTS _____ Internally Developed ______
Computer Programming Language	
Data Access Middleware (please list product used and check if it is compliant with the listed standards or protocols)	 Open Database Connectivity _____ Java Database Connectivity _____ Other (specify):
Application Communication Middleware (please list product used and check if it is compliant with the listed standards or protocols)	 Remote Procedure Call (RPC) model ______ Message Passing model ______ Message Queuing model _______ Publish and Subscribe model ______ Other (please specify):
Other (please specify):	

12



3. For this watch list, please check (✓) below any of the software infrastructure standards your system or database is compliant with. If your system or database is compliant with a standard not listed, please list it in the other category. **(Check all that apply.)**

1. [ ] Distributed Computing Environment
2. [ ] Common Object Request Broker Architecture
3. [ ] Distributed Component Object Model
4. [ ] Java Remote Method Invocation
5. [ ] Other (please specify): _____________
____
____

4. For this watch list, please specify each type of network connectivity used by your agency: **(Check all that apply.)**

1. [ ] World Wide Web
2. [ ] Public Switched Telephone Network
3. [ ] Non-Secure Internet Protocol Routing Network
4. [ ] Secure Internet Protocol Routing Network
5. [ ] Treasury Electronic Communications System or other federal telecommunications intermediary system
6. [ ] Virtual Private Network
7. [ ] Dedicated Network
8. [ ] Other (please specify): _____________
____
____

5. Is the system on which your list resides built in compliance with open system standards?

1. [ ] Yes
2. [ ] No

If yes, please specify which standard(s) you used to develop and/or implement your system**.**

____
____
____
____
____
____
____
____

6. Is the database or system your list resides on stand-alone[4] or networked?

1. [ ] Stand-alone only **(go to question 8)**
2. [ ] Networked only
3. [ ] Both stand-alone and networked components
3. [ ] Other (please specify): _________
____
____

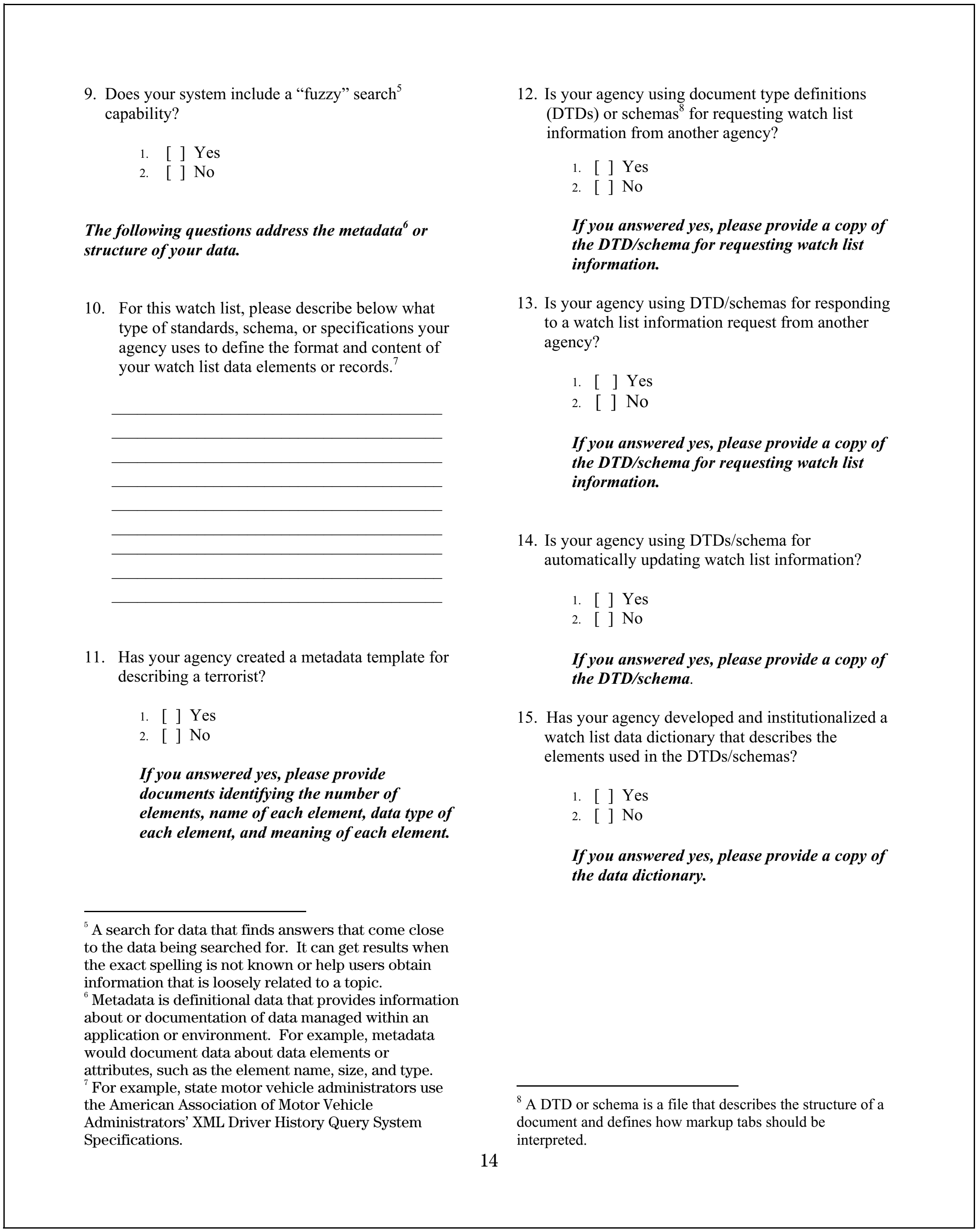
7. Please complete the table below by designating with a check (✓) the types of systems or networks your database and/or system is connected to and listing the systems:

Type of Systems	Yes (✓)	No (✓)	If Yes, List System(s)
Commercial Systems			
Defense Systems			
Internet			
Intranet			
Extranet			
Wireless Connection			
Other (please specify): ___________________________ ___________________________ ___________________________ ___________________________ ___________________________			

8. What fields can you use to search for individuals? **(Check all that apply.)**

1. [ ] Name fields
2. [ ] Biometric fields (e.g., fingerprints)
3. [ ] Date of birth fields
4. [ ] Other (please specify): ______________
____

[4] A stand-alone database/system is one that is not directly connected to other systems or networks.



9. Does your system include a "fuzzy" search[5] capability?

    1. [ ] Yes
    2. [ ] No

The following questions address the metadata[6] or structure of your data.

10. For this watch list, please describe below what type of standards, schema, or specifications your agency uses to define the format and content of your watch list data elements or records.[7]

    ____
    ____
    ____
    ____
    ____
    ____
    ____
    ____
    ____

11. Has your agency created a metadata template for describing a terrorist?

    1. [ ] Yes
    2. [ ] No

    If you answered yes, please provide documents identifying the number of elements, name of each element, data type of each element, and meaning of each element.

12. Is your agency using document type definitions (DTDs) or schemas[8] for requesting watch list information from another agency?

    1. [ ] Yes
    2. [ ] No

    If you answered yes, please provide a copy of the DTD/schema for requesting watch list information.

13. Is your agency using DTD/schemas for responding to a watch list information request from another agency?

    1. [ ] Yes
    2. [ ] No

    If you answered yes, please provide a copy of the DTD/schema for requesting watch list information.

14. Is your agency using DTDs/schema for automatically updating watch list information?

    1. [ ] Yes
    2. [ ] No

    If you answered yes, please provide a copy of the DTD/schema.

15. Has your agency developed and institutionalized a watch list data dictionary that describes the elements used in the DTDs/schemas?

    1. [ ] Yes
    2. [ ] No

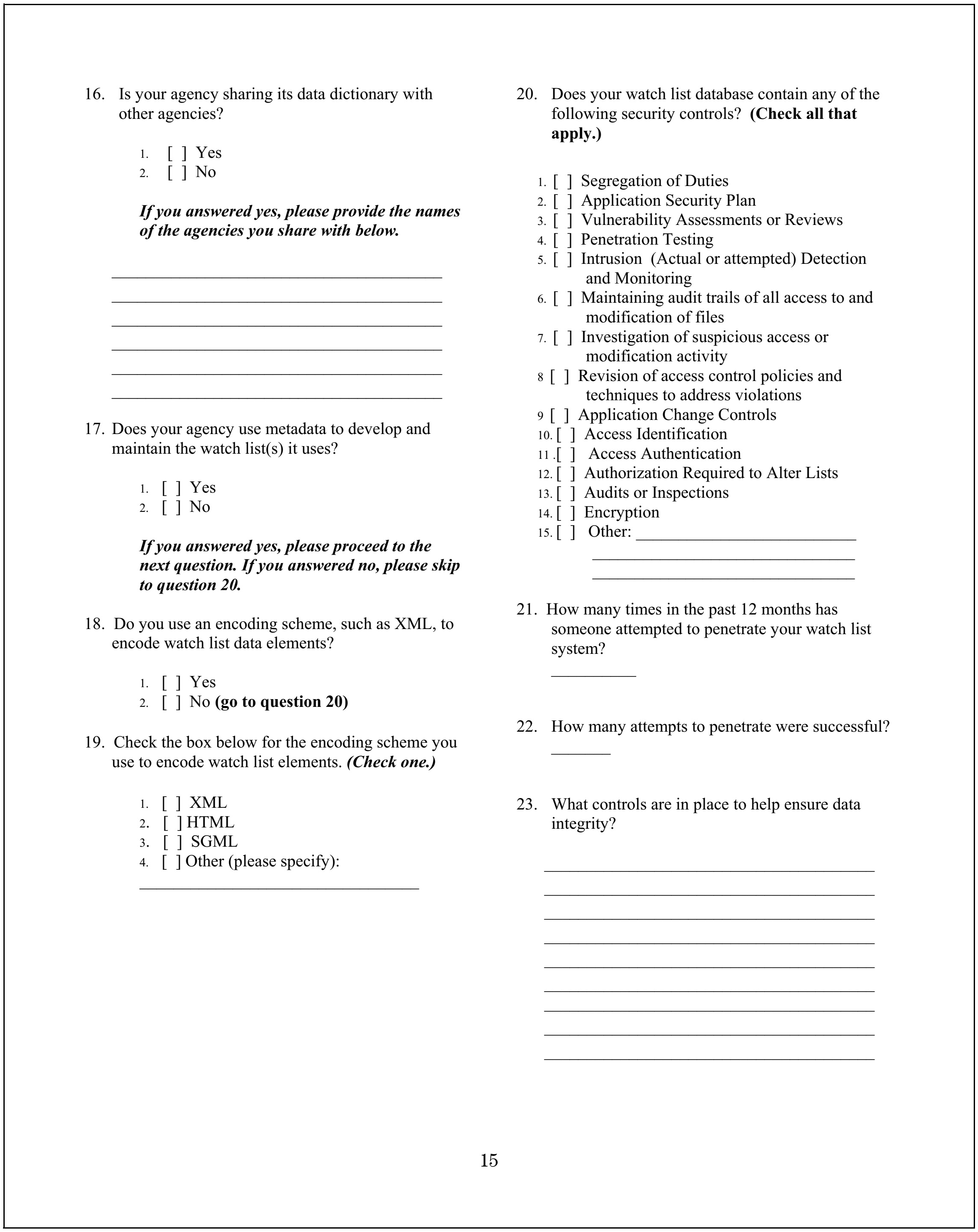
    If you answered yes, please provide a copy of the data dictionary.

[5] A search for data that finds answers that come close to the data being searched for. It can get results when the exact spelling is not known or help users obtain information that is loosely related to a topic.

[6] Metadata is definitional data that provides information about or documentation of data managed within an application or environment. For example, metadata would document data about data elements or attributes, such as the element name, size, and type.

[7] For example, state motor vehicle administrators use the American Association of Motor Vehicle Administrators' XML Driver History Query System Specifications.

[8] A DTD or schema is a file that describes the structure of a document and defines how markup tabs should be interpreted.



16. Is your agency sharing its data dictionary with other agencies?

1. [ ] Yes
2. [ ] No

If you answered yes, please provide the names of the agencies you share with below.

____
____
____
____
____
____

17. Does your agency use metadata to develop and maintain the watch list(s) it uses?

1. [ ] Yes
2. [ ] No

If you answered yes, please proceed to the next question. If you answered no, please skip to question 20.

18. Do you use an encoding scheme, such as XML, to encode watch list data elements?

1. [ ] Yes
2. [ ] No **(go to question 20)**

19. Check the box below for the encoding scheme you use to encode watch list elements. ***(Check one.)***

1. [ ] XML
2. [ ] HTML
3. [ ] SGML
4. [ ] Other (please specify):

____

20. Does your watch list database contain any of the following security controls? **(Check all that apply.)**

1. [ ] Segregation of Duties
2. [ ] Application Security Plan
3. [ ] Vulnerability Assessments or Reviews
4. [ ] Penetration Testing
5. [ ] Intrusion (Actual or attempted) Detection and Monitoring
6. [ ] Maintaining audit trails of all access to and modification of files
7. [ ] Investigation of suspicious access or modification activity
8 [ ] Revision of access control policies and techniques to address violations
9 [ ] Application Change Controls
10. [ ] Access Identification
11 .[ ] Access Authentication
12. [ ] Authorization Required to Alter Lists
13. [ ] Audits or Inspections
14. [ ] Encryption
15. [ ] Other: __________________________
____
____

21. How many times in the past 12 months has someone attempted to penetrate your watch list system?

____

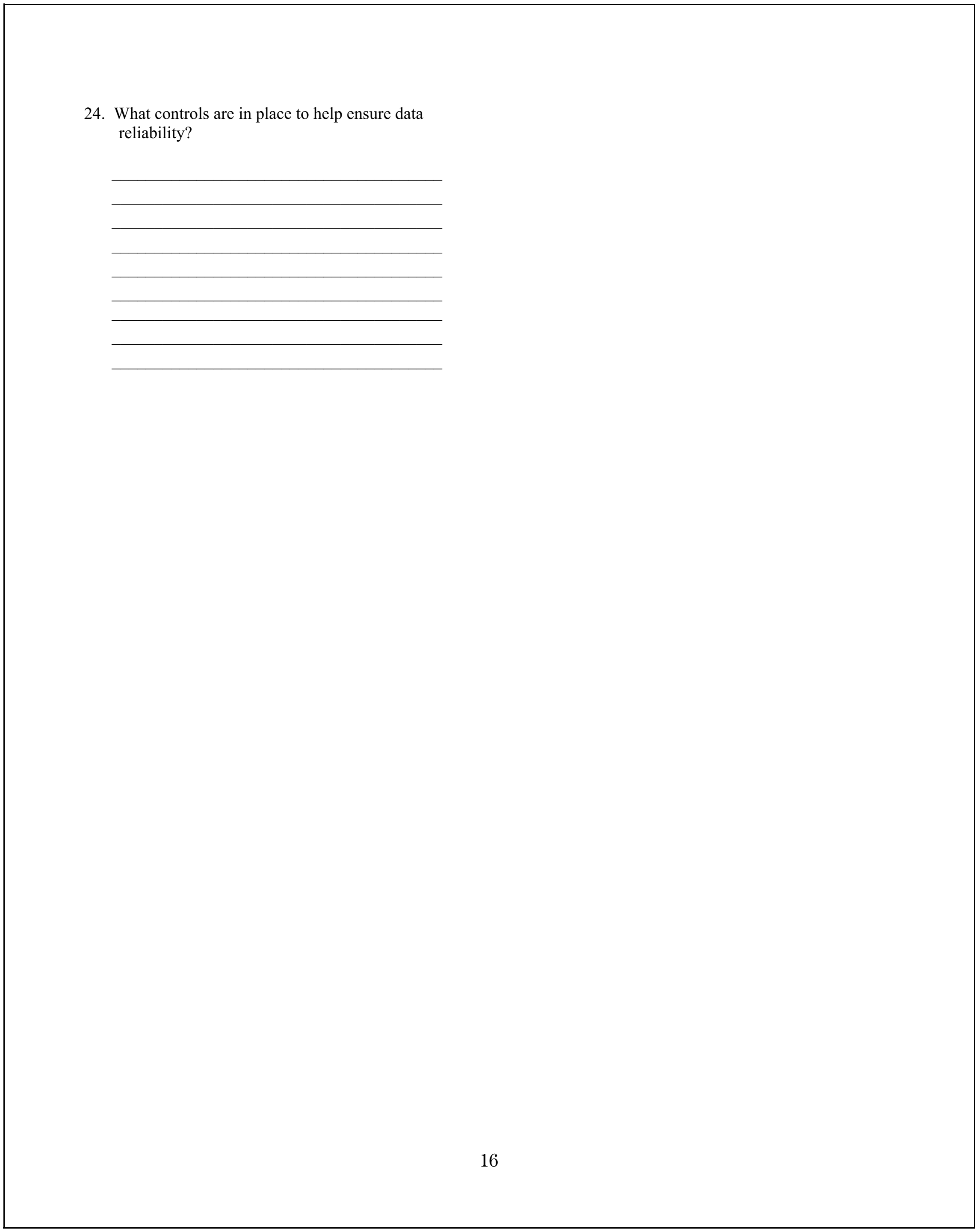
22. How many attempts to penetrate were successful?

____

23. What controls are in place to help ensure data integrity?

____
____
____
____
____
____
____
____
____

15



24. What controls are in place to help ensure data reliability?

____

____

____

____

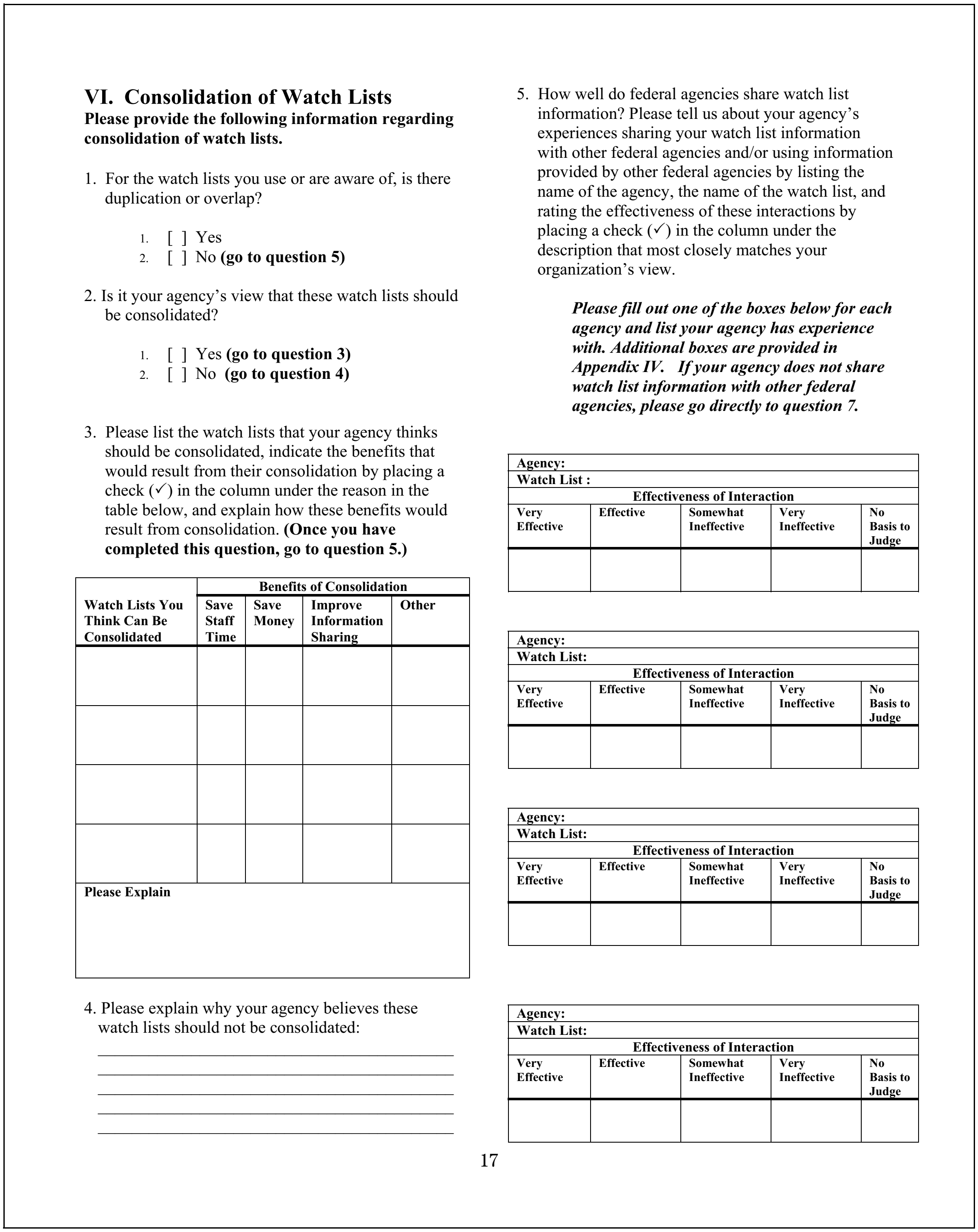
____

____

____

____

____



VI. Consolidation of Watch Lists

Please provide the following information regarding consolidation of watch lists.

1. For the watch lists you use or are aware of, is there duplication or overlap?

1. [ ] Yes
2. [ ] No **(go to question 5)**

2. Is it your agency's view that these watch lists should be consolidated?

1. [ ] Yes **(go to question 3)**
2. [ ] No **(go to question 4)**

3. Please list the watch lists that your agency thinks should be consolidated, indicate the benefits that would result from their consolidation by placing a check (✓) in the column under the reason in the table below, and explain how these benefits would result from consolidation. **(Once you have completed this question, go to question 5.)**

Watch Lists You Think Can Be Consolidated	Benefits of Consolidation			
	Save Staff Time	Save Money	Improve Information Sharing	Other
Please Explain				

4. Please explain why your agency believes these watch lists should not be consolidated:

____
____
____
____
____

5. How well do federal agencies share watch list information? Please tell us about your agency's experiences sharing your watch list information with other federal agencies and/or using information provided by other federal agencies by listing the name of the agency, the name of the watch list, and rating the effectiveness of these interactions by placing a check (✓) in the column under the description that most closely matches your organization's view.

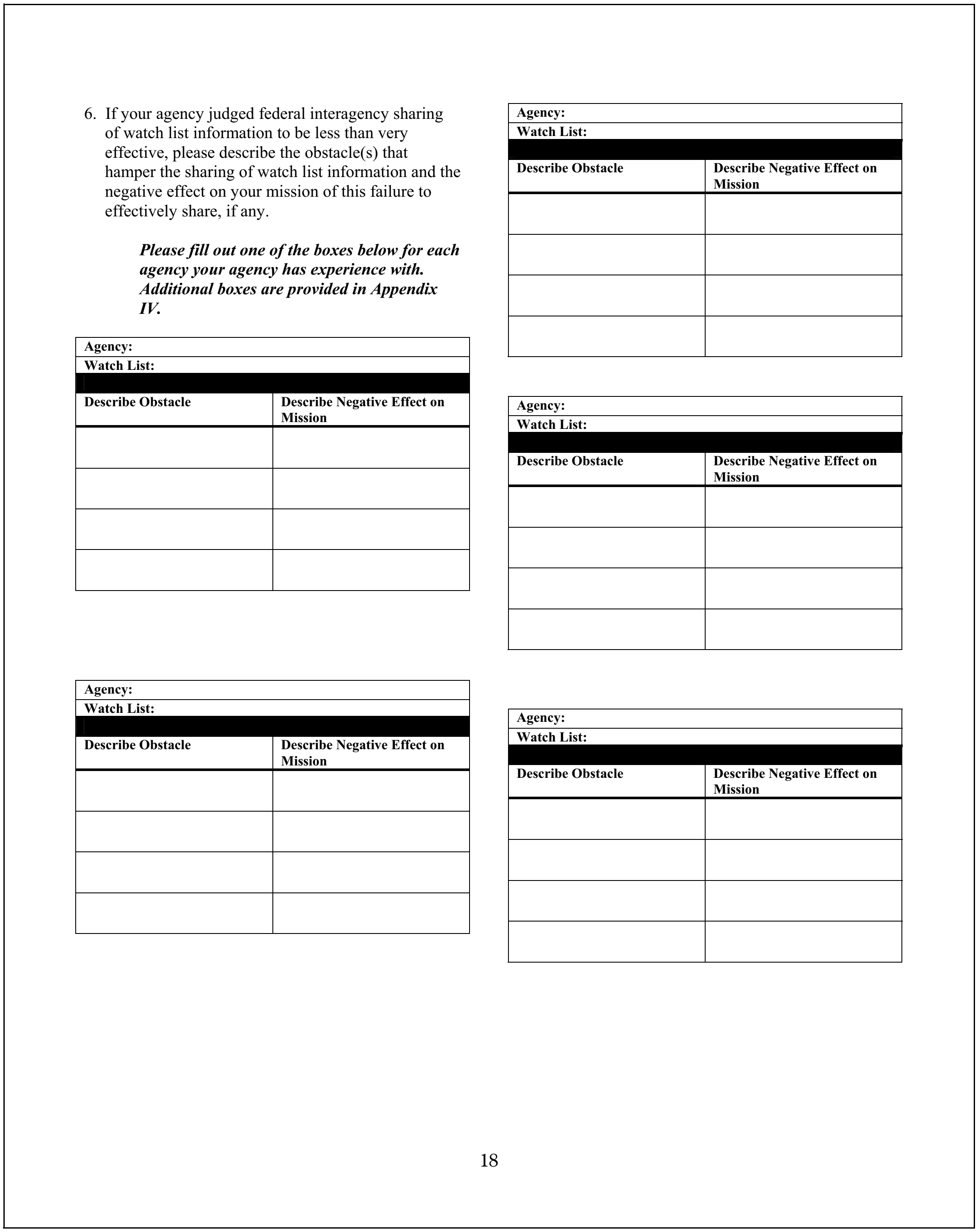
Please fill out one of the boxes below for each agency and list your agency has experience with. Additional boxes are provided in Appendix IV. If your agency does not share watch list information with other federal agencies, please go directly to question 7.

Agency:				
Watch List :				
Effectiveness of Interaction				
Very Effective	Effective	Somewhat Ineffective	Very Ineffective	No Basis to Judge

Agency:				
Watch List:				
Effectiveness of Interaction				
Very Effective	Effective	Somewhat Ineffective	Very Ineffective	No Basis to Judge

Agency:				
Watch List:				
Effectiveness of Interaction				
Very Effective	Effective	Somewhat Ineffective	Very Ineffective	No Basis to Judge

Agency:				
Watch List:				
Effectiveness of Interaction				
Very Effective	Effective	Somewhat Ineffective	Very Ineffective	No Basis to Judge



6. If your agency judged federal interagency sharing of watch list information to be less than very effective, please describe the obstacle(s) that hamper the sharing of watch list information and the negative effect on your mission of this failure to effectively share, if any.

    Please fill out one of the boxes below for each agency your agency has experience with. Additional boxes are provided in Appendix IV.

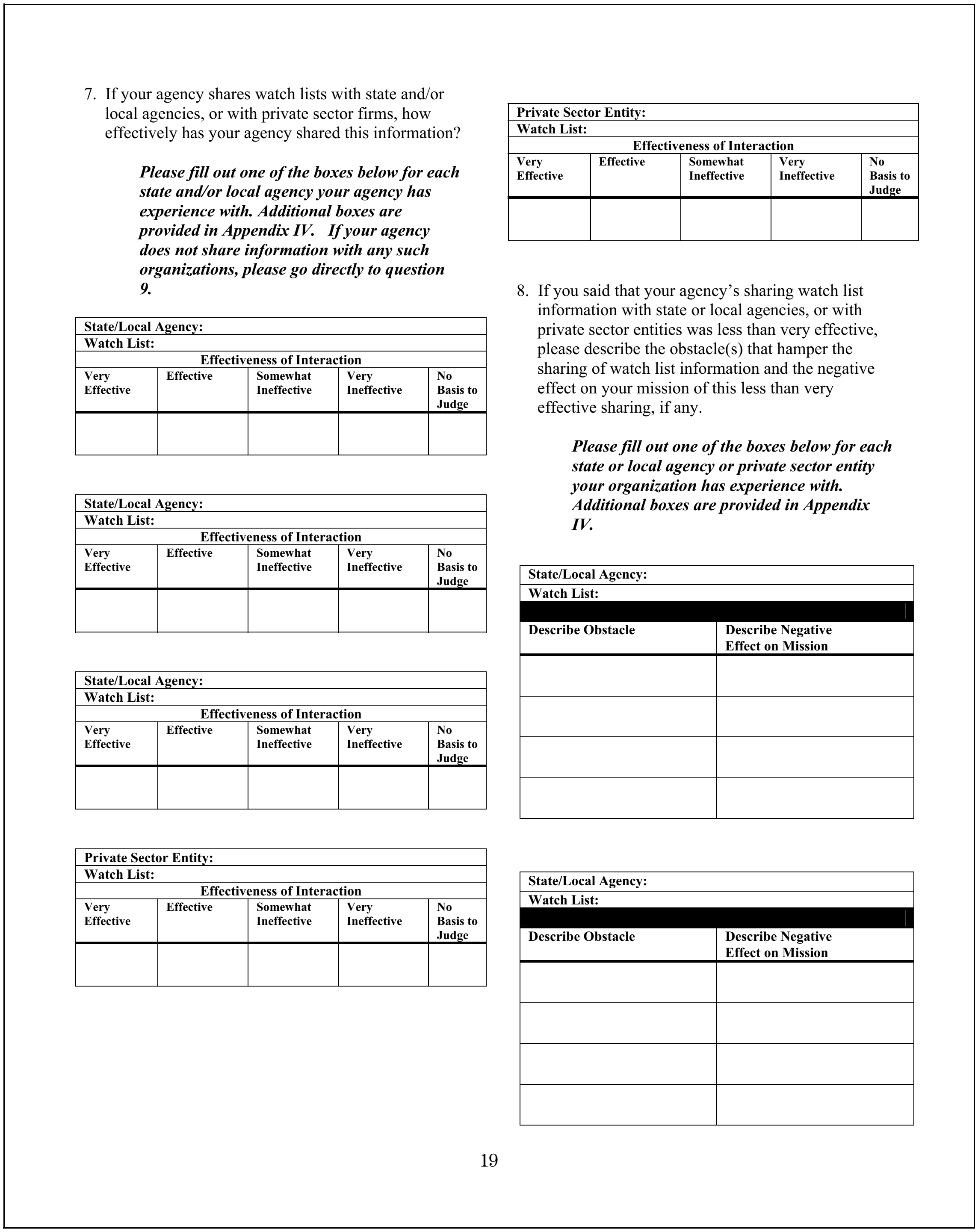
Agency:	
Watch List:	
Describe Obstacle	**Describe Negative Effect on Mission**

Agency:	
Watch List:	
Describe Obstacle	**Describe Negative Effect on Mission**

Agency:	
Watch List:	
Describe Obstacle	**Describe Negative Effect on Mission**

Agency:	
Watch List:	
Describe Obstacle	**Describe Negative Effect on Mission**

Agency:	
Watch List:	
Describe Obstacle	**Describe Negative Effect on Mission**



7. If your agency shares watch lists with state and/or local agencies, or with private sector firms, how effectively has your agency shared this information?

Please fill out one of the boxes below for each state and/or local agency your agency has experience with. Additional boxes are provided in Appendix IV. If your agency does not share information with any such organizations, please go directly to question 9.

State/Local Agency:				
Watch List:				
Effectiveness of Interaction				
Very Effective	**Effective**	**Somewhat Ineffective**	**Very Ineffective**	**No Basis to Judge**

State/Local Agency:				
Watch List:				
Effectiveness of Interaction				
Very Effective	**Effective**	**Somewhat Ineffective**	**Very Ineffective**	**No Basis to Judge**

State/Local Agency:				
Watch List:				
Effectiveness of Interaction				
Very Effective	**Effective**	**Somewhat Ineffective**	**Very Ineffective**	**No Basis to Judge**

Private Sector Entity:				
Watch List:				
Effectiveness of Interaction				
Very Effective	**Effective**	**Somewhat Ineffective**	**Very Ineffective**	**No Basis to Judge**

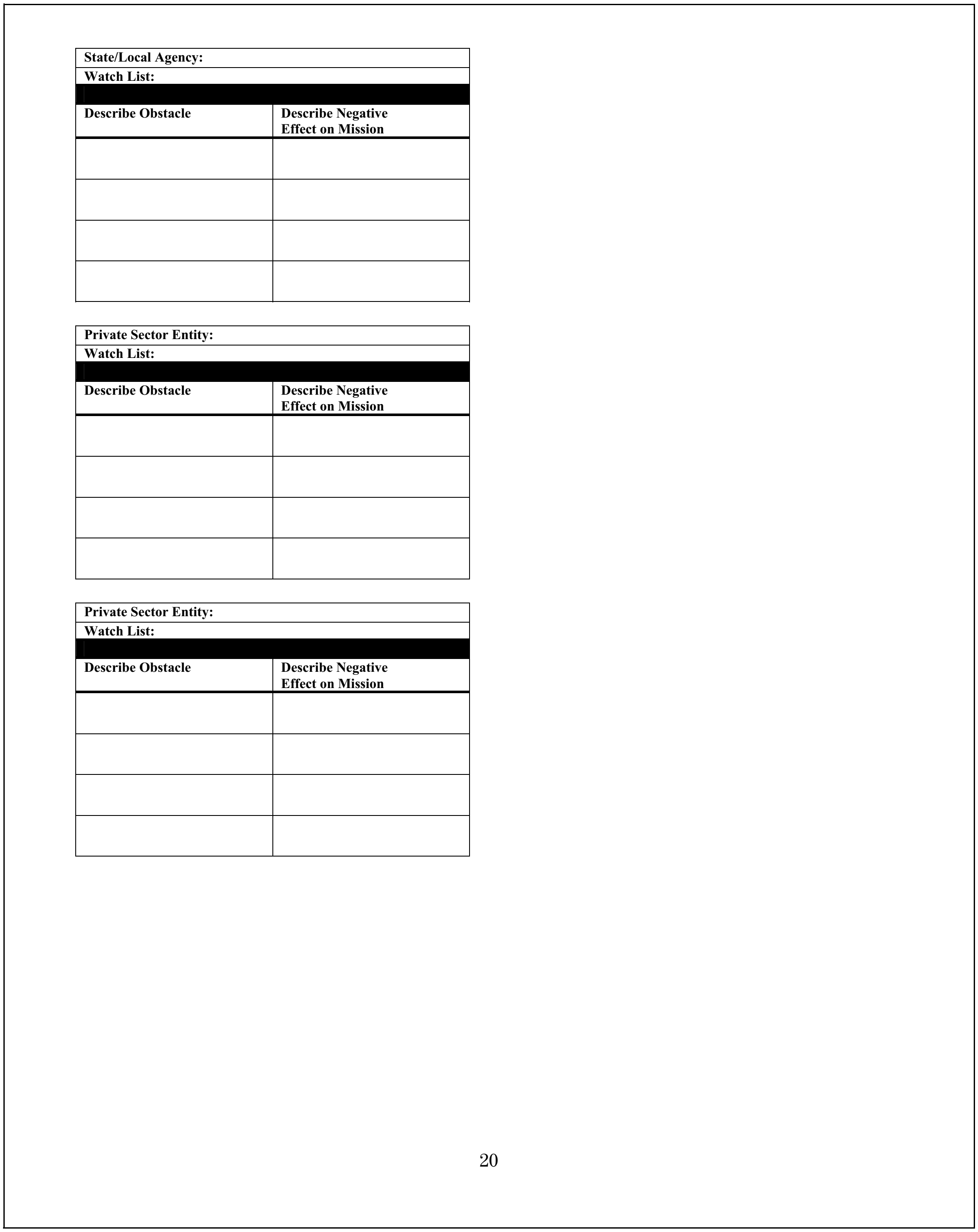
Private Sector Entity:				
Watch List:				
Effectiveness of Interaction				
Very Effective	**Effective**	**Somewhat Ineffective**	**Very Ineffective**	**No Basis to Judge**

8. If you said that your agency's sharing watch list information with state or local agencies, or with private sector entities was less than very effective, please describe the obstacle(s) that hamper the sharing of watch list information and the negative effect on your mission of this less than very effective sharing, if any.

Please fill out one of the boxes below for each state or local agency or private sector entity your organization has experience with. Additional boxes are provided in Appendix IV.

State/Local Agency:	
Watch List:	
Describe Obstacle	**Describe Negative Effect on Mission**

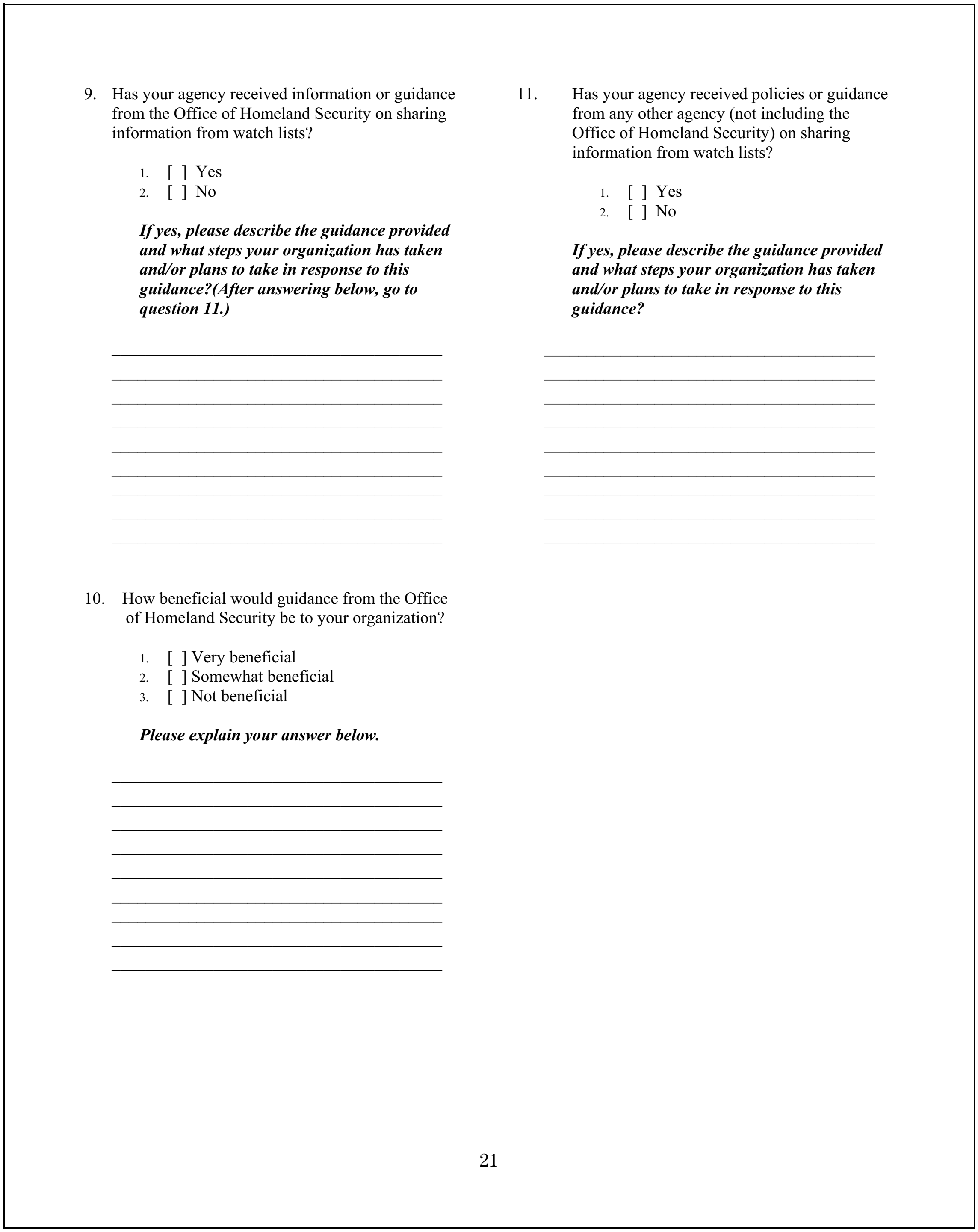
State/Local Agency:	
Watch List:	
Describe Obstacle	**Describe Negative Effect on Mission**



State/Local Agency:	
Watch List:	
Describe Obstacle	**Describe Negative Effect on Mission**

Private Sector Entity:	
Watch List:	
Describe Obstacle	**Describe Negative Effect on Mission**

Private Sector Entity:	
Watch List:	
Describe Obstacle	**Describe Negative Effect on Mission**



9. Has your agency received information or guidance from the Office of Homeland Security on sharing information from watch lists?

1. [ ] Yes
2. [ ] No

If yes, please describe the guidance provided and what steps your organization has taken and/or plans to take in response to this guidance?(After answering below, go to question 11.)

____
____
____
____
____
____
____
____
____

10. How beneficial would guidance from the Office of Homeland Security be to your organization?

1. [ ] Very beneficial
2. [ ] Somewhat beneficial
3. [ ] Not beneficial

Please explain your answer below.

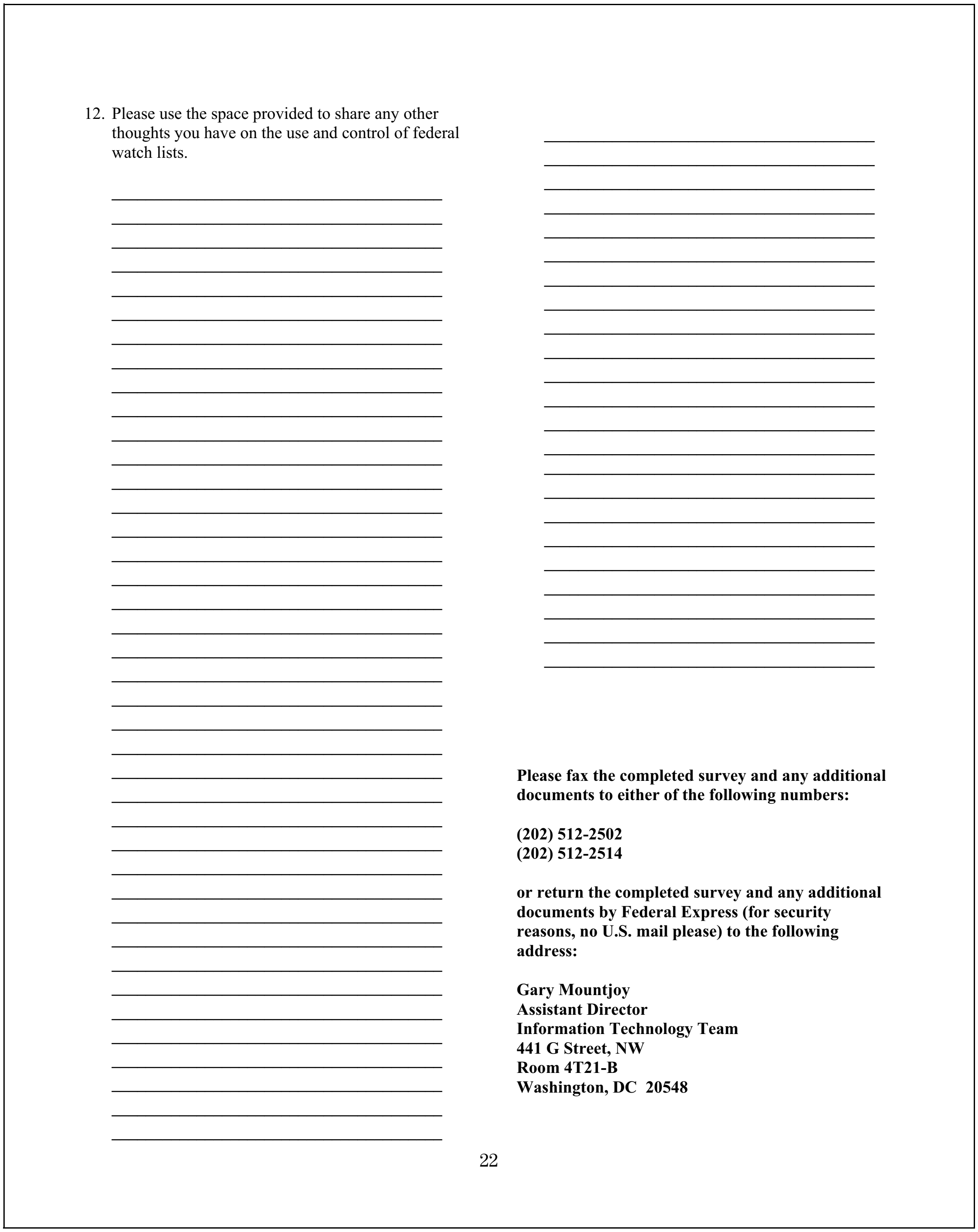
____
____
____
____
____
____
____
____
____

11. Has your agency received policies or guidance from any other agency (not including the Office of Homeland Security) on sharing information from watch lists?

1. [ ] Yes
2. [ ] No

If yes, please describe the guidance provided and what steps your organization has taken and/or plans to take in response to this guidance?

____
____
____
____
____
____
____
____
____



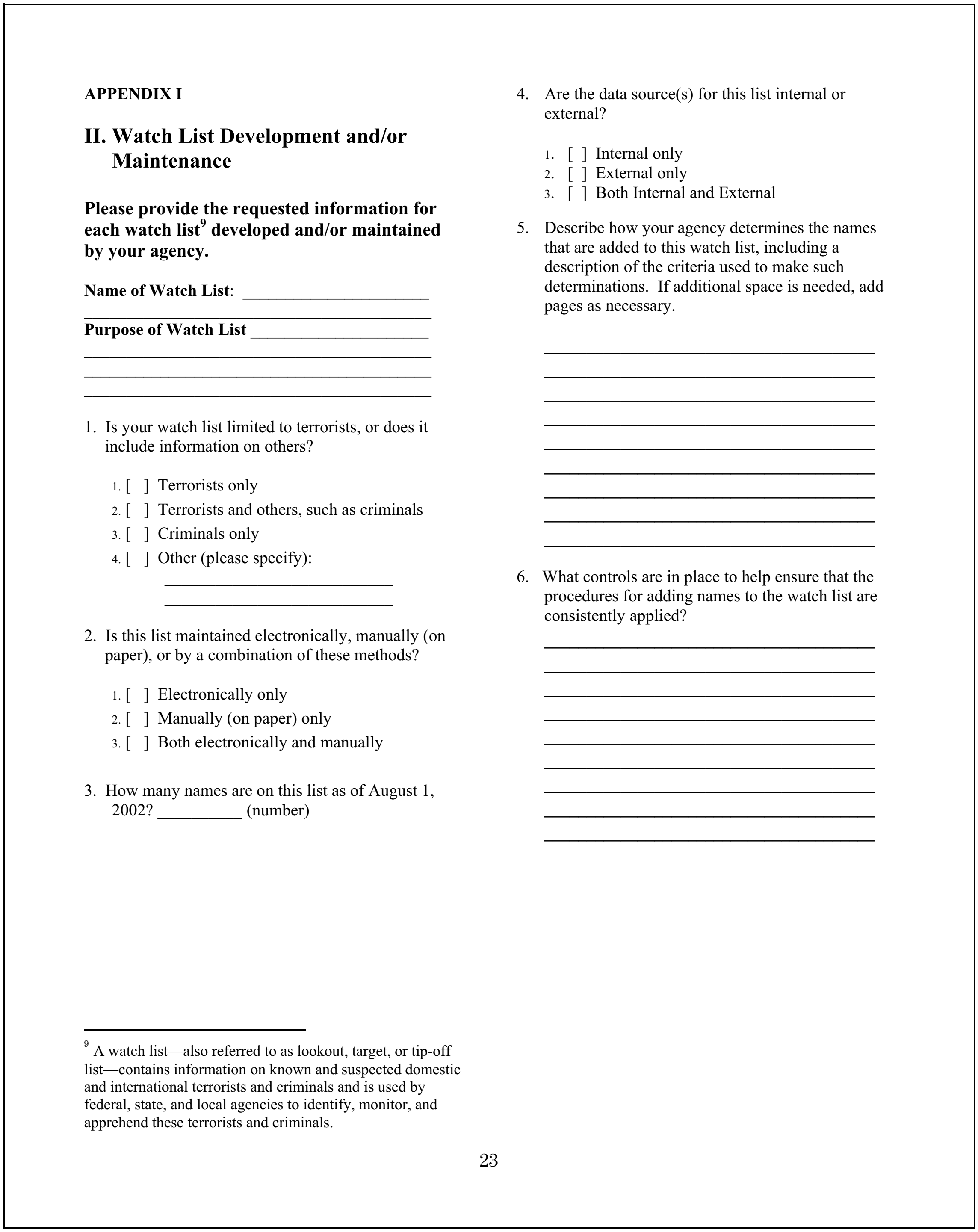
12. Please use the space provided to share any other thoughts you have on the use and control of federal watch lists.

Please fax the completed survey and any additional documents to either of the following numbers:

(202) 512-2502
(202) 512-2514

or return the completed survey and any additional documents by Federal Express (for security reasons, no U.S. mail please) to the following address:

Gary Mountjoy
Assistant Director
Information Technology Team
441 G Street, NW
Room 4T21-B
Washington, DC 20548



II. Watch List Development and/or Maintenance

Please provide the requested information for each watch list[9] developed and/or maintained by your agency.

Name of Watch List: ______________________
____

Purpose of Watch List _____________________
____
____
____

1. Is your watch list limited to terrorists, or does it include information on others?

   1. [ ] Terrorists only
   2. [ ] Terrorists and others, such as criminals
   3. [ ] Criminals only
   4. [ ] Other (please specify):
      ____
      ____

2. Is this list maintained electronically, manually (on paper), or by a combination of these methods?

   1. [ ] Electronically only
   2. [ ] Manually (on paper) only
   3. [ ] Both electronically and manually

3. How many names are on this list as of August 1, 2002? __________ (number)

4. Are the data source(s) for this list internal or external?

   1. [ ] Internal only
   2. [ ] External only
   3. [ ] Both Internal and External

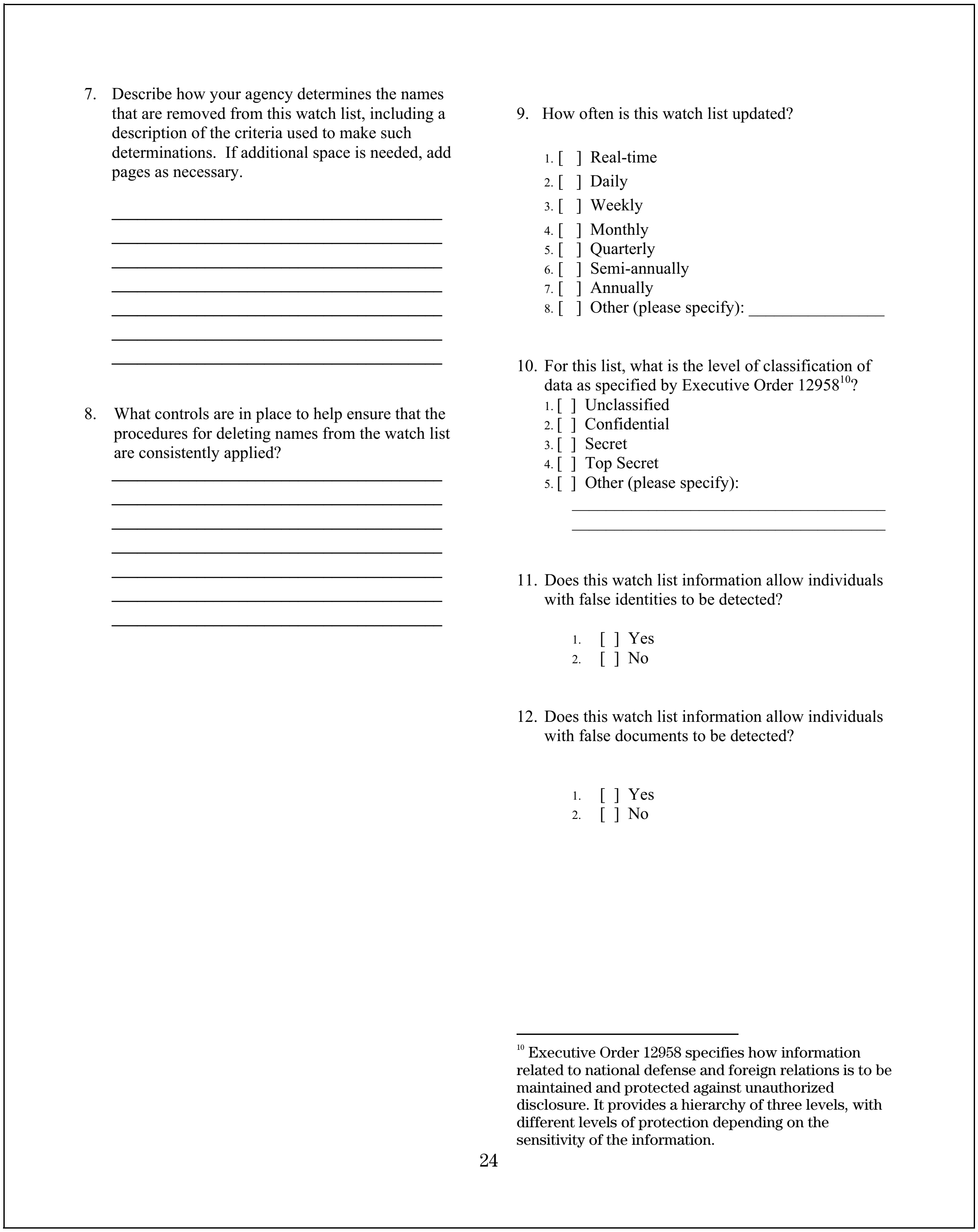
5. Describe how your agency determines the names that are added to this watch list, including a description of the criteria used to make such determinations. If additional space is needed, add pages as necessary.

   ____
   ____
   ____
   ____
   ____
   ____
   ____
   ____
   ____

6. What controls are in place to help ensure that the procedures for adding names to the watch list are consistently applied?

   ____
   ____
   ____
   ____
   ____
   ____
   ____
   ____
   ____

[9] A watch list—also referred to as lookout, target, or tip-off list—contains information on known and suspected domestic and international terrorists and criminals and is used by federal, state, and local agencies to identify, monitor, and apprehend these terrorists and criminals.



7. Describe how your agency determines the names that are removed from this watch list, including a description of the criteria used to make such determinations. If additional space is needed, add pages as necessary.

____
____
____
____
____
____
____

8. What controls are in place to help ensure that the procedures for deleting names from the watch list are consistently applied?

____
____
____
____
____
____
____

9. How often is this watch list updated?

1. [ ] Real-time
2. [ ] Daily
3. [ ] Weekly
4. [ ] Monthly
5. [ ] Quarterly
6. [ ] Semi-annually
7. [ ] Annually
8. [ ] Other (please specify): ________________

10. For this list, what is the level of classification of data as specified by Executive Order 12958[10]?

1. [ ] Unclassified
2. [ ] Confidential
3. [ ] Secret
4. [ ] Top Secret
5. [ ] Other (please specify):

____
____

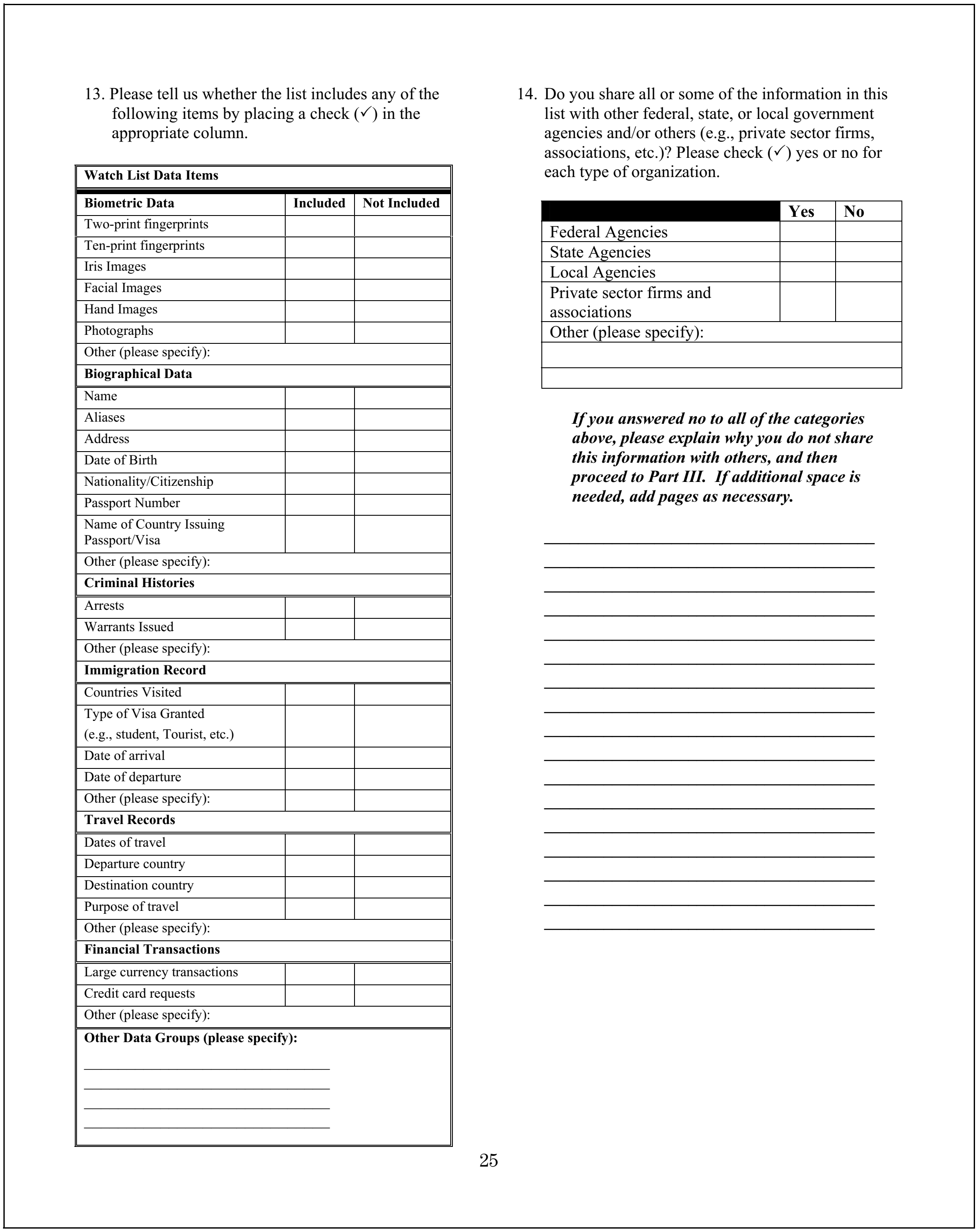
11. Does this watch list information allow individuals with false identities to be detected?

1. [ ] Yes
2. [ ] No

12. Does this watch list information allow individuals with false documents to be detected?

1. [ ] Yes
2. [ ] No

[10] Executive Order 12958 specifies how information related to national defense and foreign relations is to be maintained and protected against unauthorized disclosure. It provides a hierarchy of three levels, with different levels of protection depending on the sensitivity of the information.



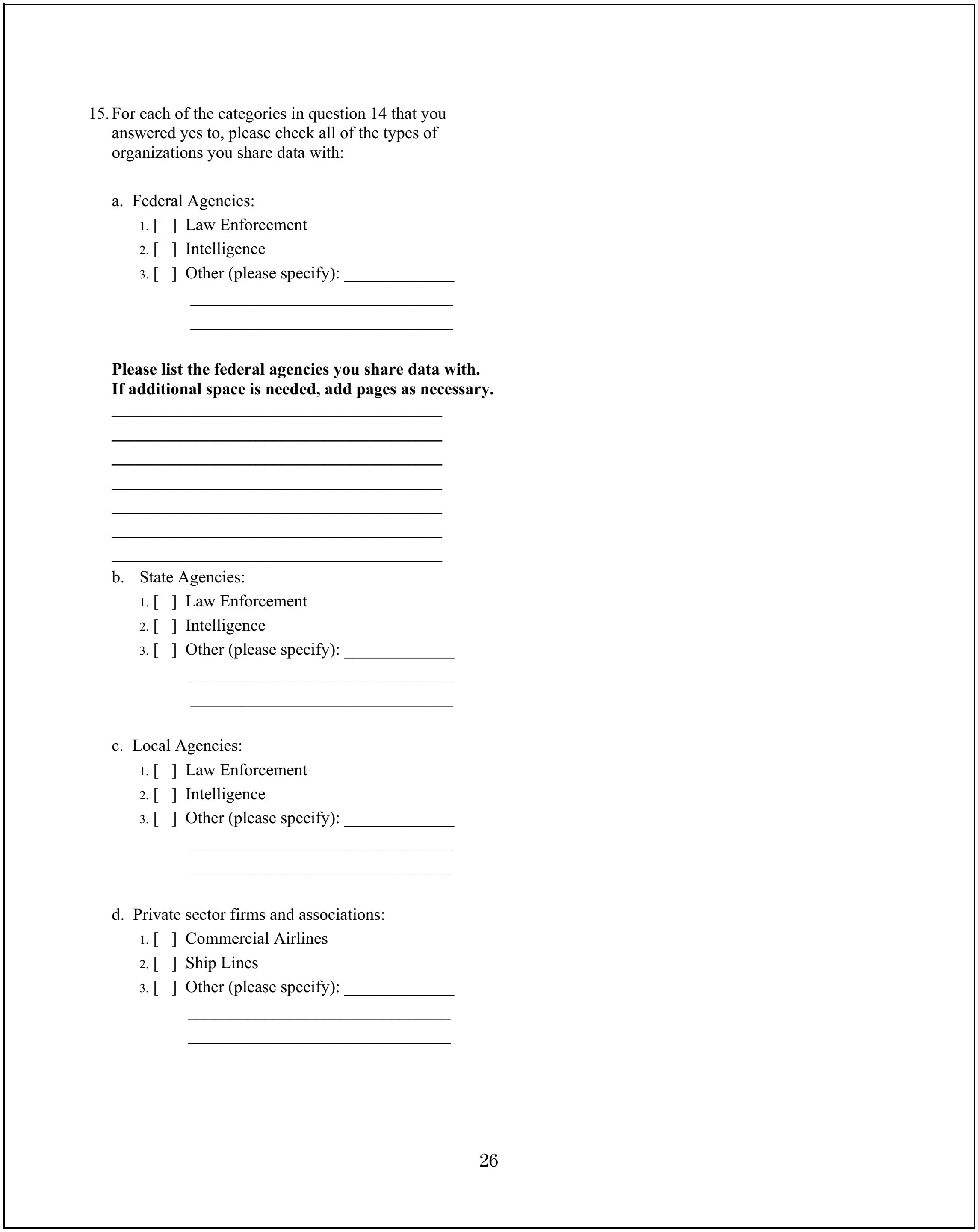
13. Please tell us whether the list includes any of the following items by placing a check (✓) in the appropriate column.

Watch List Data Items		
Biometric Data	**Included**	**Not Included**
Two-print fingerprints		
Ten-print fingerprints		
Iris Images		
Facial Images		
Hand Images		
Photographs		
Other (please specify):		
Biographical Data		
Name		
Aliases		
Address		
Date of Birth		
Nationality/Citizenship		
Passport Number		
Name of Country Issuing Passport/Visa		
Other (please specify):		
Criminal Histories		
Arrests		
Warrants Issued		
Other (please specify):		
Immigration Record		
Countries Visited		
Type of Visa Granted (e.g., student, Tourist, etc.)		
Date of arrival		
Date of departure		
Other (please specify):		
Travel Records		
Dates of travel		
Departure country		
Destination country		
Purpose of travel		
Other (please specify):		
Financial Transactions		
Large currency transactions		
Credit card requests		
Other (please specify):		
Other Data Groups (please specify):		

14. Do you share all or some of the information in this list with other federal, state, or local government agencies and/or others (e.g., private sector firms, associations, etc.)? Please check (✓) yes or no for each type of organization.

	Yes	No
Federal Agencies		
State Agencies		
Local Agencies		
Private sector firms and associations		
Other (please specify):		

If you answered no to all of the categories above, please explain why you do not share this information with others, and then proceed to Part III. If additional space is needed, add pages as necessary.



15. For each of the categories in question 14 that you answered yes to, please check all of the types of organizations you share data with:

a. Federal Agencies:
1. [ ] Law Enforcement
2. [ ] Intelligence
3. [ ] Other (please specify): _____________
____
____

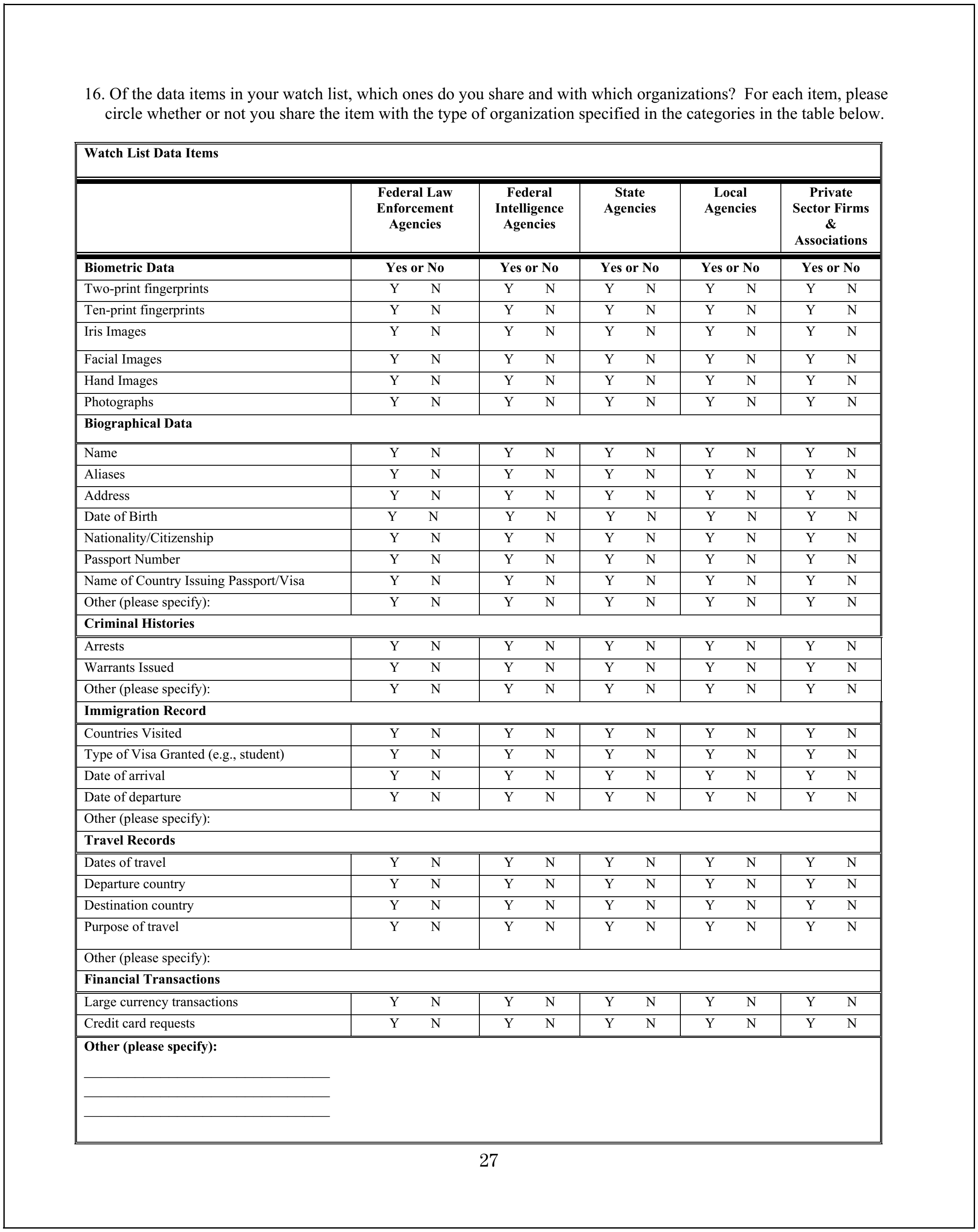
Please list the federal agencies you share data with.
If additional space is needed, add pages as necessary.
____
____
____
____
____
____
____

b. State Agencies:
1. [ ] Law Enforcement
2. [ ] Intelligence
3. [ ] Other (please specify): _____________
____
____

c. Local Agencies:
1. [ ] Law Enforcement
2. [ ] Intelligence
3. [ ] Other (please specify): _____________
____
____

d. Private sector firms and associations:
1. [ ] Commercial Airlines
2. [ ] Ship Lines
3. [ ] Other (please specify): _____________
____
____

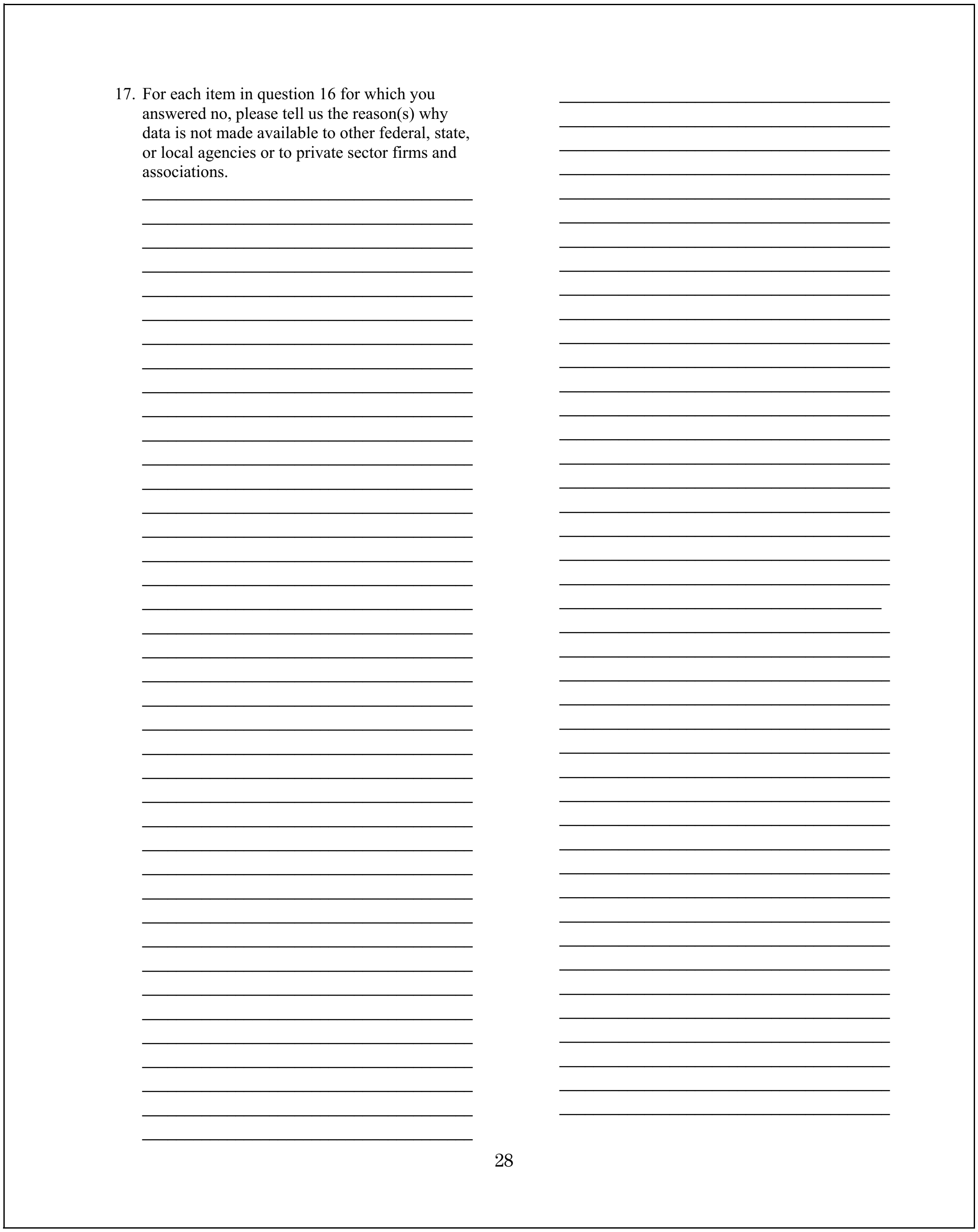
26



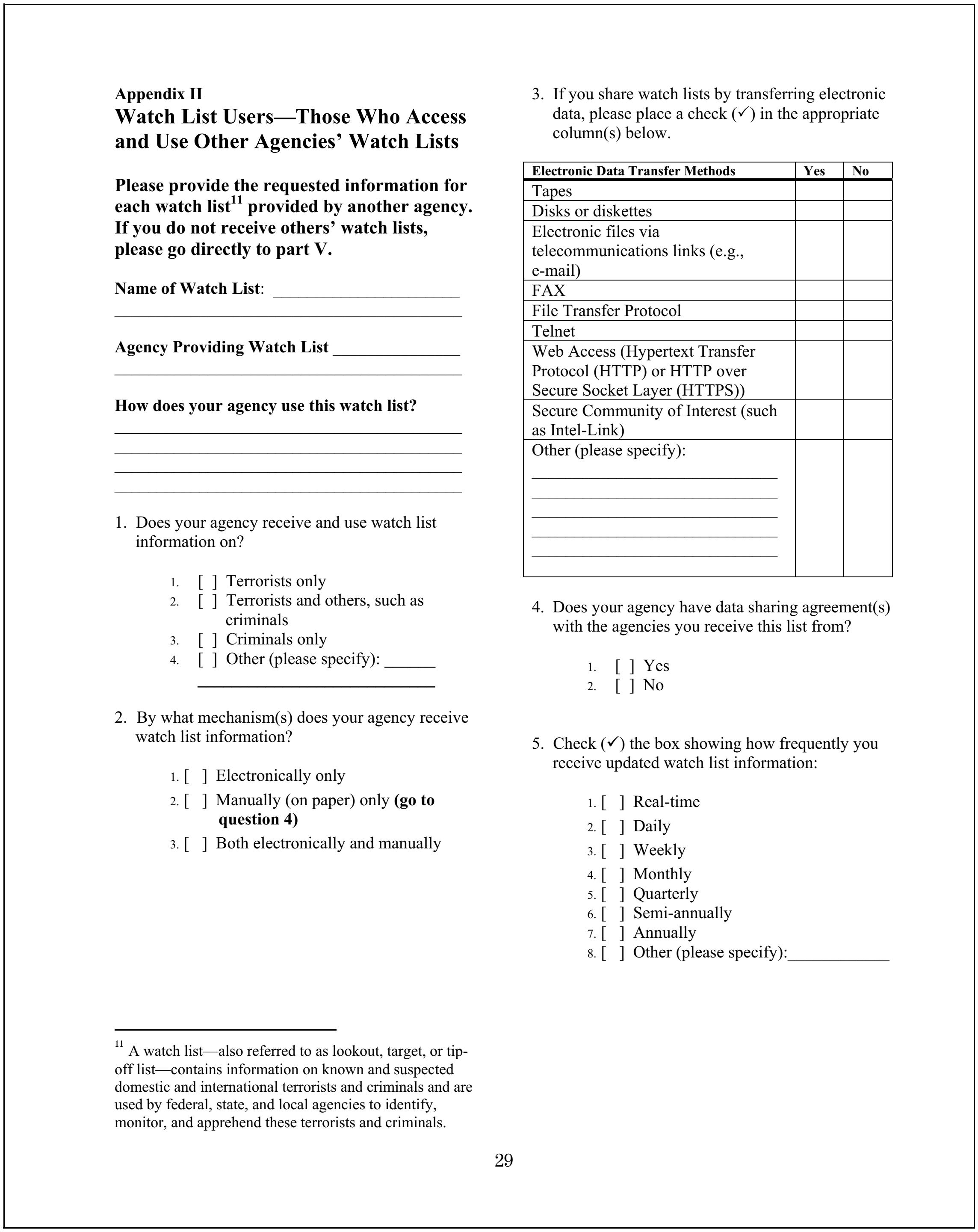
16. Of the data items in your watch list, which ones do you share and with which organizations? For each item, please circle whether or not you share the item with the type of organization specified in the categories in the table below.

Watch List Data Items	Federal Law Enforcement Agencies	Federal Intelligence Agencies	State Agencies	Local Agencies	Private Sector Firms & Associations
Biometric Data	**Yes or No**	**Yes or No**	**Yes or No**	**Yes or No**	**Yes or No**
Two-print fingerprints	Y N	Y N	Y N	Y N	Y N
Ten-print fingerprints	Y N	Y N	Y N	Y N	Y N
Iris Images	Y N	Y N	Y N	Y N	Y N
Facial Images	Y N	Y N	Y N	Y N	Y N
Hand Images	Y N	Y N	Y N	Y N	Y N
Photographs	Y N	Y N	Y N	Y N	Y N
Biographical Data					
Name	Y N	Y N	Y N	Y N	Y N
Aliases	Y N	Y N	Y N	Y N	Y N
Address	Y N	Y N	Y N	Y N	Y N
Date of Birth	Y N	Y N	Y N	Y N	Y N
Nationality/Citizenship	Y N	Y N	Y N	Y N	Y N
Passport Number	Y N	Y N	Y N	Y N	Y N
Name of Country Issuing Passport/Visa	Y N	Y N	Y N	Y N	Y N
Other (please specify):	Y N	Y N	Y N	Y N	Y N
Criminal Histories					
Arrests	Y N	Y N	Y N	Y N	Y N
Warrants Issued	Y N	Y N	Y N	Y N	Y N
Other (please specify):	Y N	Y N	Y N	Y N	Y N
Immigration Record					
Countries Visited	Y N	Y N	Y N	Y N	Y N
Type of Visa Granted (e.g., student)	Y N	Y N	Y N	Y N	Y N
Date of arrival	Y N	Y N	Y N	Y N	Y N
Date of departure	Y N	Y N	Y N	Y N	Y N
Other (please specify):					
Travel Records					
Dates of travel	Y N	Y N	Y N	Y N	Y N
Departure country	Y N	Y N	Y N	Y N	Y N
Destination country	Y N	Y N	Y N	Y N	Y N
Purpose of travel	Y N	Y N	Y N	Y N	Y N
Other (please specify):					
Financial Transactions					
Large currency transactions	Y N	Y N	Y N	Y N	Y N
Credit card requests	Y N	Y N	Y N	Y N	Y N
Other (please specify): ______________________________ ______________________________ ______________________________					

27



17. For each item in question 16 for which you answered no, please tell us the reason(s) why data is not made available to other federal, state, or local agencies or to private sector firms and associations.



Appendix II

Watch List Users—Those Who Access and Use Other Agencies' Watch Lists

Please provide the requested information for each watch list[11] provided by another agency. If you do not receive others' watch lists, please go directly to part V.

Name of Watch List: ______________________
____

Agency Providing Watch List _______________
____

How does your agency use this watch list?
____
____
____
____

1. Does your agency receive and use watch list information on?

   1. [ ] Terrorists only
   2. [ ] Terrorists and others, such as criminals
   3. [ ] Criminals only
   4. [ ] Other (please specify): ______
   ____

2. By what mechanism(s) does your agency receive watch list information?

   1. [ ] Electronically only
   2. [ ] Manually (on paper) only **(go to question 4)**
   3. [ ] Both electronically and manually

3. If you share watch lists by transferring electronic data, please place a check (✓) in the appropriate column(s) below.

Electronic Data Transfer Methods	Yes	No
Tapes		
Disks or diskettes		
Electronic files via telecommunications links (e.g., e-mail)		
FAX		
File Transfer Protocol		
Telnet		
Web Access (Hypertext Transfer Protocol (HTTP) or HTTP over Secure Socket Layer (HTTPS))		
Secure Community of Interest (such as Intel-Link)		
Other (please specify): ____________________________ ____________________________ ____________________________ ____________________________ ____________________________		

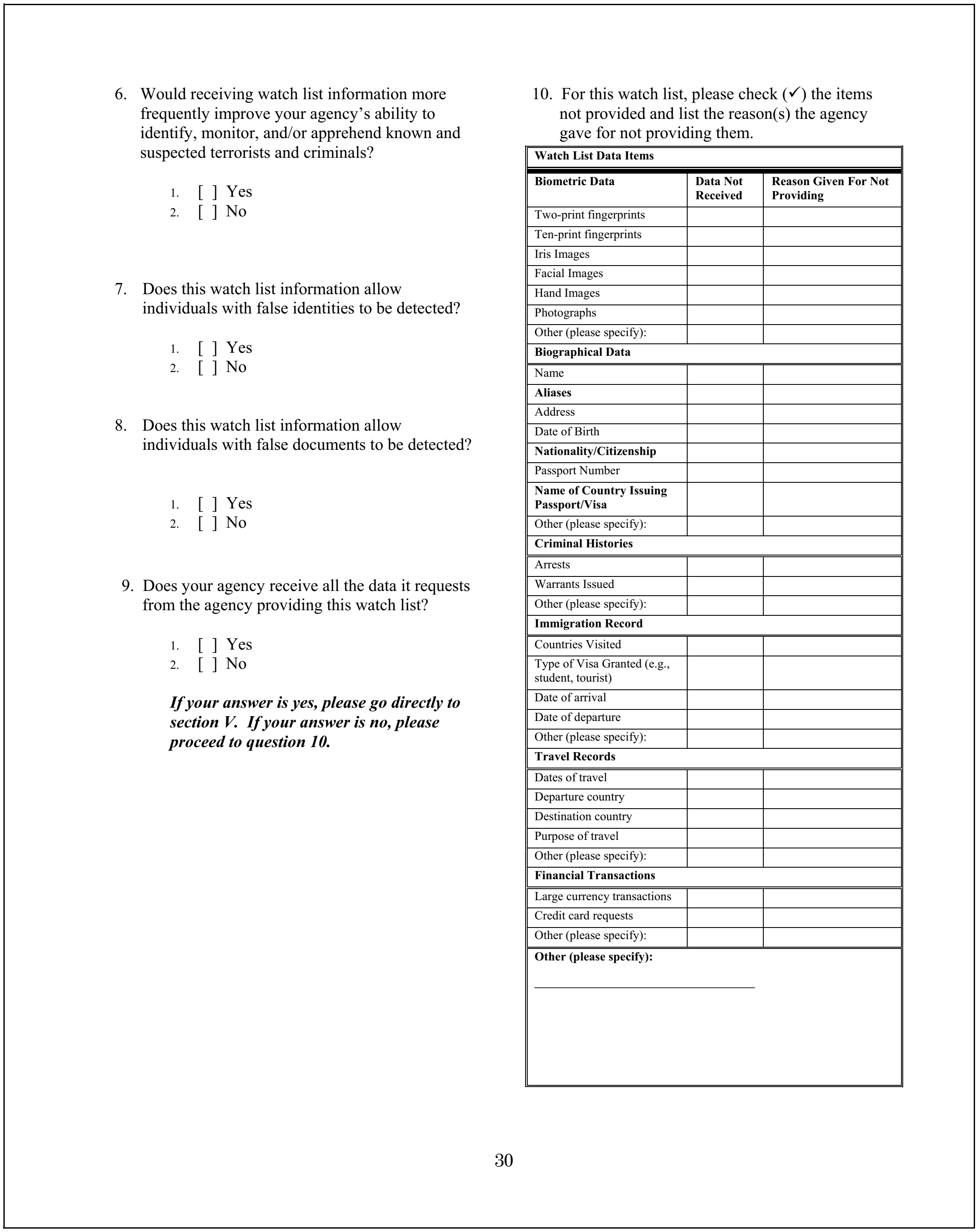
4. Does your agency have data sharing agreement(s) with the agencies you receive this list from?

   1. [ ] Yes
   2. [ ] No

5. Check (✓) the box showing how frequently you receive updated watch list information:

   1. [ ] Real-time
   2. [ ] Daily
   3. [ ] Weekly
   4. [ ] Monthly
   5. [ ] Quarterly
   6. [ ] Semi-annually
   7. [ ] Annually
   8. [ ] Other (please specify):____________

[11] A watch list—also referred to as lookout, target, or tip-off list—contains information on known and suspected domestic and international terrorists and criminals and are used by federal, state, and local agencies to identify, monitor, and apprehend these terrorists and criminals.



6. Would receiving watch list information more frequently improve your agency's ability to identify, monitor, and/or apprehend known and suspected terrorists and criminals?

   1. [ ] Yes
   2. [ ] No

7. Does this watch list information allow individuals with false identities to be detected?

   1. [ ] Yes
   2. [ ] No

8. Does this watch list information allow individuals with false documents to be detected?

   1. [ ] Yes
   2. [ ] No

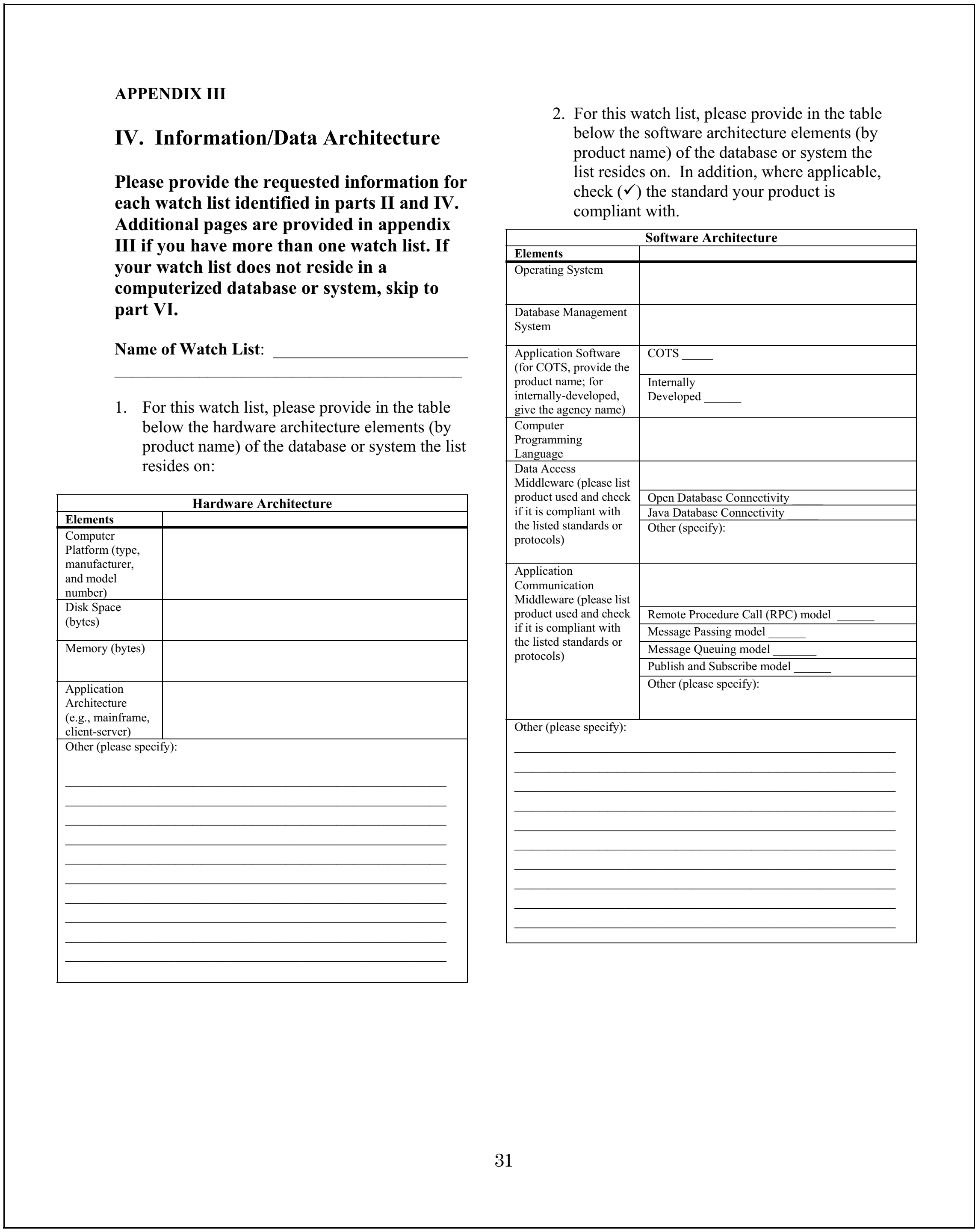
9. Does your agency receive all the data it requests from the agency providing this watch list?

   1. [ ] Yes
   2. [ ] No

   If your answer is yes, please go directly to section V. If your answer is no, please proceed to question 10.

10. For this watch list, please check (✓) the items not provided and list the reason(s) the agency gave for not providing them.

Watch List Data Items		
Biometric Data	**Data Not Received**	**Reason Given For Not Providing**
Two-print fingerprints		
Ten-print fingerprints		
Iris Images		
Facial Images		
Hand Images		
Photographs		
Other (please specify):		
Biographical Data		
Name		
Aliases		
Address		
Date of Birth		
Nationality/Citizenship		
Passport Number		
Name of Country Issuing Passport/Visa		
Other (please specify):		
Criminal Histories		
Arrests		
Warrants Issued		
Other (please specify):		
Immigration Record		
Countries Visited		
Type of Visa Granted (e.g., student, tourist)		
Date of arrival		
Date of departure		
Other (please specify):		
Travel Records		
Dates of travel		
Departure country		
Destination country		
Purpose of travel		
Other (please specify):		
Financial Transactions		
Large currency transactions		
Credit card requests		
Other (please specify):		
Other (please specify): __________________________________		



APPENDIX III

IV. Information/Data Architecture

Please provide the requested information for each watch list identified in parts II and IV. Additional pages are provided in appendix III if you have more than one watch list. If your watch list does not reside in a computerized database or system, skip to part VI.

Name of Watch List: ________________________
____

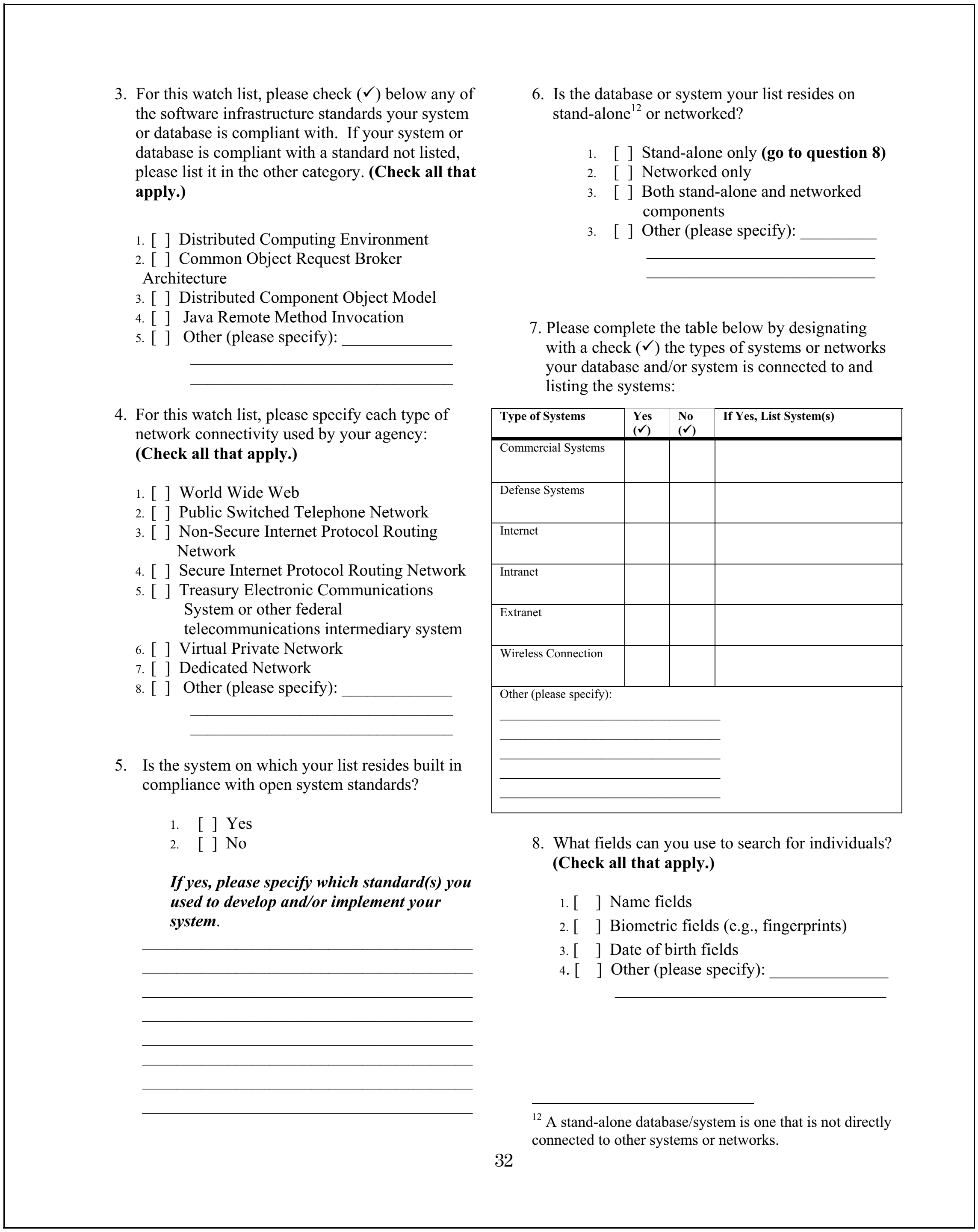
1. For this watch list, please provide in the table below the hardware architecture elements (by product name) of the database or system the list resides on:

Hardware Architecture	
Elements	
Computer Platform (type, manufacturer, and model number)	
Disk Space (bytes)	
Memory (bytes)	
Application Architecture (e.g., mainframe, client-server)	
Other (please specify): ____ ____ ____ ____ ____ ____ ____ ____ ____ ____	

2. For this watch list, please provide in the table below the software architecture elements (by product name) of the database or system the list resides on. In addition, where applicable, check (✓) the standard your product is compliant with.

Software Architecture	
Elements	
Operating System	
Database Management System	
Application Software (for COTS, provide the product name; for internally-developed, give the agency name)	COTS _____ Internally Developed ______
Computer Programming Language	
Data Access Middleware (please list product used and check if it is compliant with the listed standards or protocols)	 Open Database Connectivity _____ Java Database Connectivity _____ Other (specify):
Application Communication Middleware (please list product used and check if it is compliant with the listed standards or protocols)	 Remote Procedure Call (RPC) model ______ Message Passing model ______ Message Queuing model _______ Publish and Subscribe model ______ Other (please specify):
Other (please specify): ____ ____ ____ ____ ____ ____ ____ ____ ____ ____	

31



3. For this watch list, please check (✓) below any of the software infrastructure standards your system or database is compliant with. If your system or database is compliant with a standard not listed, please list it in the other category. **(Check all that apply.)**

1. [ ] Distributed Computing Environment
2. [ ] Common Object Request Broker Architecture
3. [ ] Distributed Component Object Model
4. [ ] Java Remote Method Invocation
5. [ ] Other (please specify): _____________
____
____

4. For this watch list, please specify each type of network connectivity used by your agency: **(Check all that apply.)**

1. [ ] World Wide Web
2. [ ] Public Switched Telephone Network
3. [ ] Non-Secure Internet Protocol Routing Network
4. [ ] Secure Internet Protocol Routing Network
5. [ ] Treasury Electronic Communications System or other federal telecommunications intermediary system
6. [ ] Virtual Private Network
7. [ ] Dedicated Network
8. [ ] Other (please specify): _____________
____
____

5. Is the system on which your list resides built in compliance with open system standards?

1. [ ] Yes
2. [ ] No

If yes, please specify which standard(s) you used to develop and/or implement your system.

____
____
____
____
____
____
____
____

6. Is the database or system your list resides on stand-alone[12] or networked?

1. [ ] Stand-alone only **(go to question 8)**
2. [ ] Networked only
3. [ ] Both stand-alone and networked components
3. [ ] Other (please specify): _________
____
____

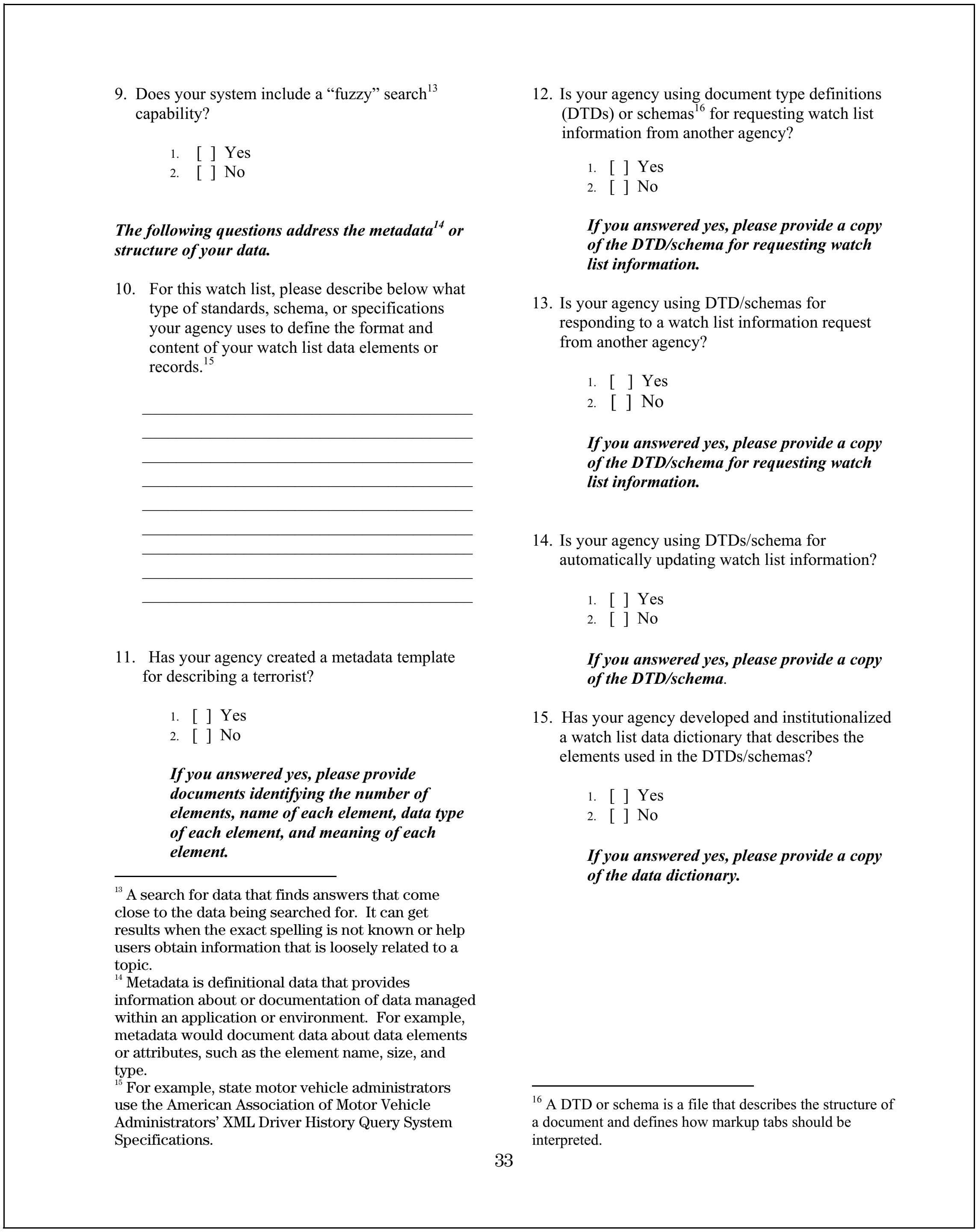
7. Please complete the table below by designating with a check (✓) the types of systems or networks your database and/or system is connected to and listing the systems:

Type of Systems	Yes (✓)	No (✓)	If Yes, List System(s)
Commercial Systems			
Defense Systems			
Internet			
Intranet			
Extranet			
Wireless Connection			
Other (please specify): _________________________ _________________________ _________________________ _________________________ _________________________			

8. What fields can you use to search for individuals? **(Check all that apply.)**

1. [ ] Name fields
2. [ ] Biometric fields (e.g., fingerprints)
3. [ ] Date of birth fields
4. [ ] Other (please specify): ______________
____

[12] A stand-alone database/system is one that is not directly connected to other systems or networks.



9. Does your system include a "fuzzy" search[13] capability?

1. [ ] Yes
2. [ ] No

The following questions address the metadata[14] or structure of your data.

10. For this watch list, please describe below what type of standards, schema, or specifications your agency uses to define the format and content of your watch list data elements or records.[15]

____
____
____
____
____
____
____
____
____

11. Has your agency created a metadata template for describing a terrorist?

1. [ ] Yes
2. [ ] No

If you answered yes, please provide documents identifying the number of elements, name of each element, data type of each element, and meaning of each element.

12. Is your agency using document type definitions (DTDs) or schemas[16] for requesting watch list information from another agency?

1. [ ] Yes
2. [ ] No

If you answered yes, please provide a copy of the DTD/schema for requesting watch list information.

13. Is your agency using DTD/schemas for responding to a watch list information request from another agency?

1. [ ] Yes
2. [ ] No

If you answered yes, please provide a copy of the DTD/schema for requesting watch list information.

14. Is your agency using DTDs/schema for automatically updating watch list information?

1. [ ] Yes
2. [ ] No

If you answered yes, please provide a copy of the DTD/schema.

15. Has your agency developed and institutionalized a watch list data dictionary that describes the elements used in the DTDs/schemas?

1. [ ] Yes
2. [ ] No

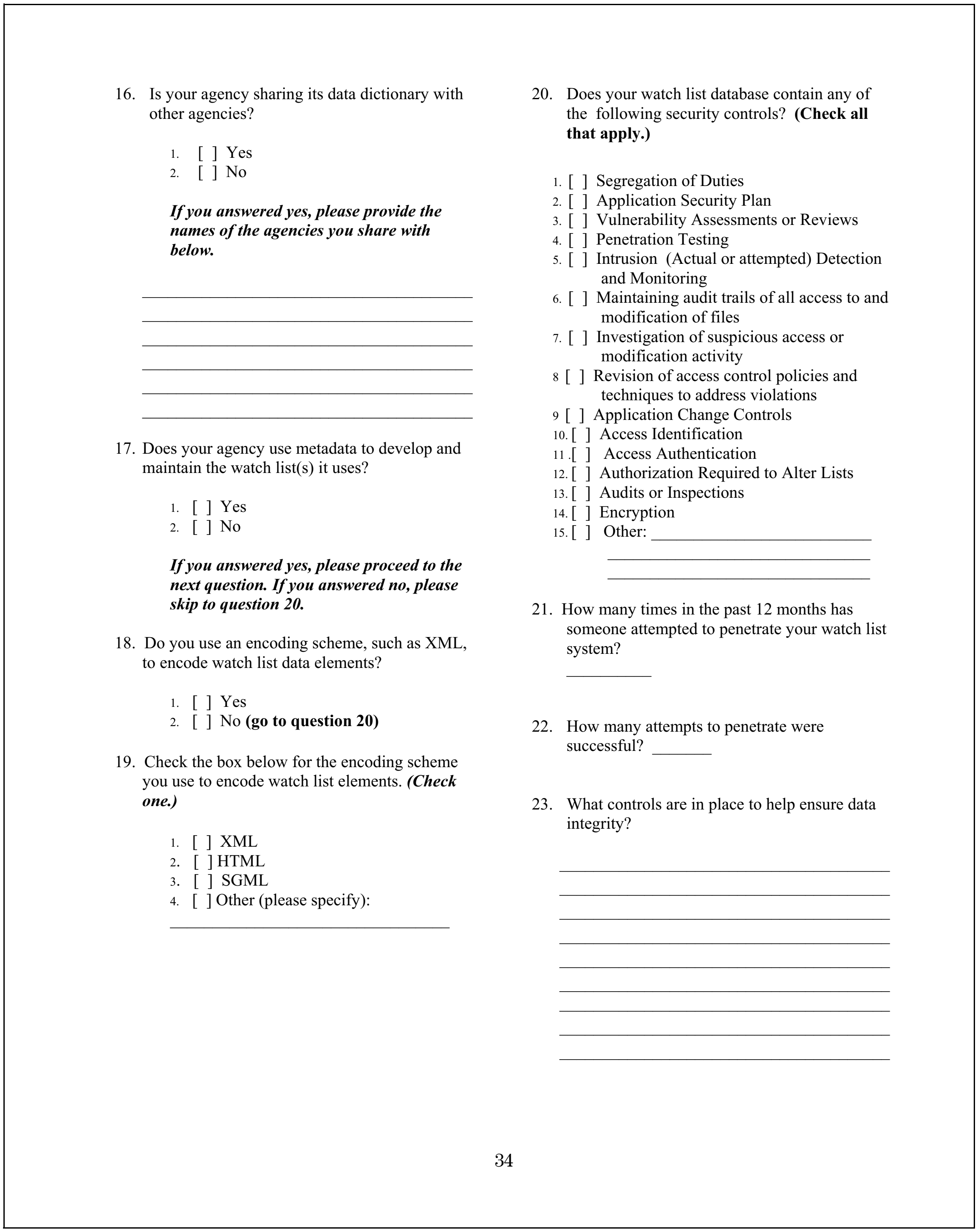
If you answered yes, please provide a copy of the data dictionary.

[13] A search for data that finds answers that come close to the data being searched for. It can get results when the exact spelling is not known or help users obtain information that is loosely related to a topic.

[14] Metadata is definitional data that provides information about or documentation of data managed within an application or environment. For example, metadata would document data about data elements or attributes, such as the element name, size, and type.

[15] For example, state motor vehicle administrators use the American Association of Motor Vehicle Administrators' XML Driver History Query System Specifications.

[16] A DTD or schema is a file that describes the structure of a document and defines how markup tabs should be interpreted.



16. Is your agency sharing its data dictionary with other agencies?

1. [ ] Yes
2. [ ] No

If you answered yes, please provide the names of the agencies you share with below.

____
____
____
____
____
____

17. Does your agency use metadata to develop and maintain the watch list(s) it uses?

1. [ ] Yes
2. [ ] No

If you answered yes, please proceed to the next question. If you answered no, please skip to question 20.

18. Do you use an encoding scheme, such as XML, to encode watch list data elements?

1. [ ] Yes
2. [ ] No **(go to question 20)**

19. Check the box below for the encoding scheme you use to encode watch list elements. ***(Check one.)***

1. [ ] XML
2. [ ] HTML
3. [ ] SGML
4. [ ] Other (please specify):

____

20. Does your watch list database contain any of the following security controls? **(Check all that apply.)**

1. [ ] Segregation of Duties
2. [ ] Application Security Plan
3. [ ] Vulnerability Assessments or Reviews
4. [ ] Penetration Testing
5. [ ] Intrusion (Actual or attempted) Detection and Monitoring
6. [ ] Maintaining audit trails of all access to and modification of files
7. [ ] Investigation of suspicious access or modification activity
8 [ ] Revision of access control policies and techniques to address violations
9 [ ] Application Change Controls
10. [ ] Access Identification
11 .[ ] Access Authentication
12. [ ] Authorization Required to Alter Lists
13. [ ] Audits or Inspections
14. [ ] Encryption
15. [ ] Other: _________________________

____
____

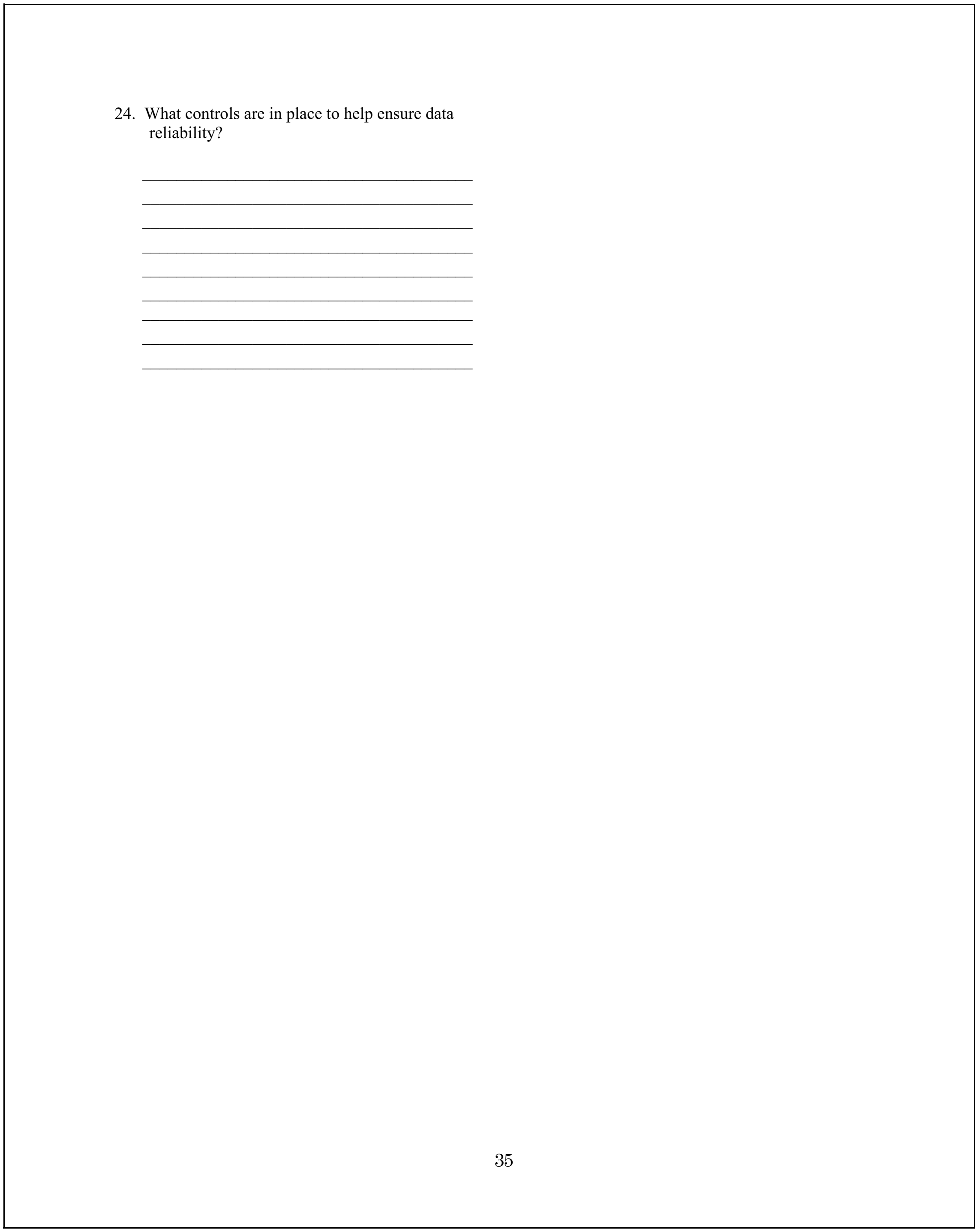
21. How many times in the past 12 months has someone attempted to penetrate your watch list system?

____

22. How many attempts to penetrate were successful? _______

23. What controls are in place to help ensure data integrity?

____
____
____
____
____
____
____
____
____



24. What controls are in place to help ensure data reliability?

____

____

____

____

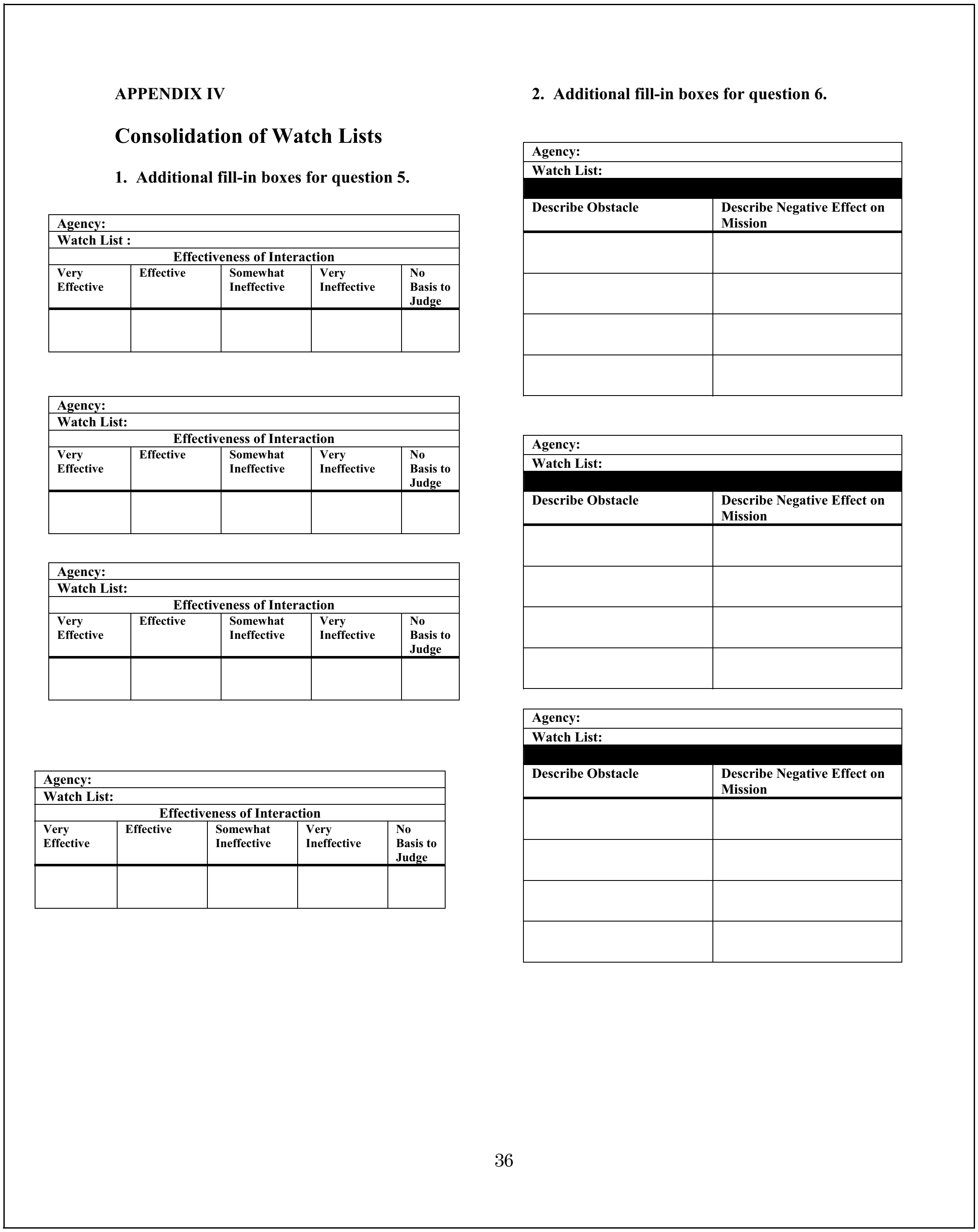
____

____

____

____

____



APPENDIX IV

Consolidation of Watch Lists

1. Additional fill-in boxes for question 5.

Agency:				
Watch List :				
Effectiveness of Interaction				
Very Effective	Effective	Somewhat Ineffective	Very Ineffective	No Basis to Judge

Agency:				
Watch List:				
Effectiveness of Interaction				
Very Effective	Effective	Somewhat Ineffective	Very Ineffective	No Basis to Judge

Agency:				
Watch List:				
Effectiveness of Interaction				
Very Effective	Effective	Somewhat Ineffective	Very Ineffective	No Basis to Judge

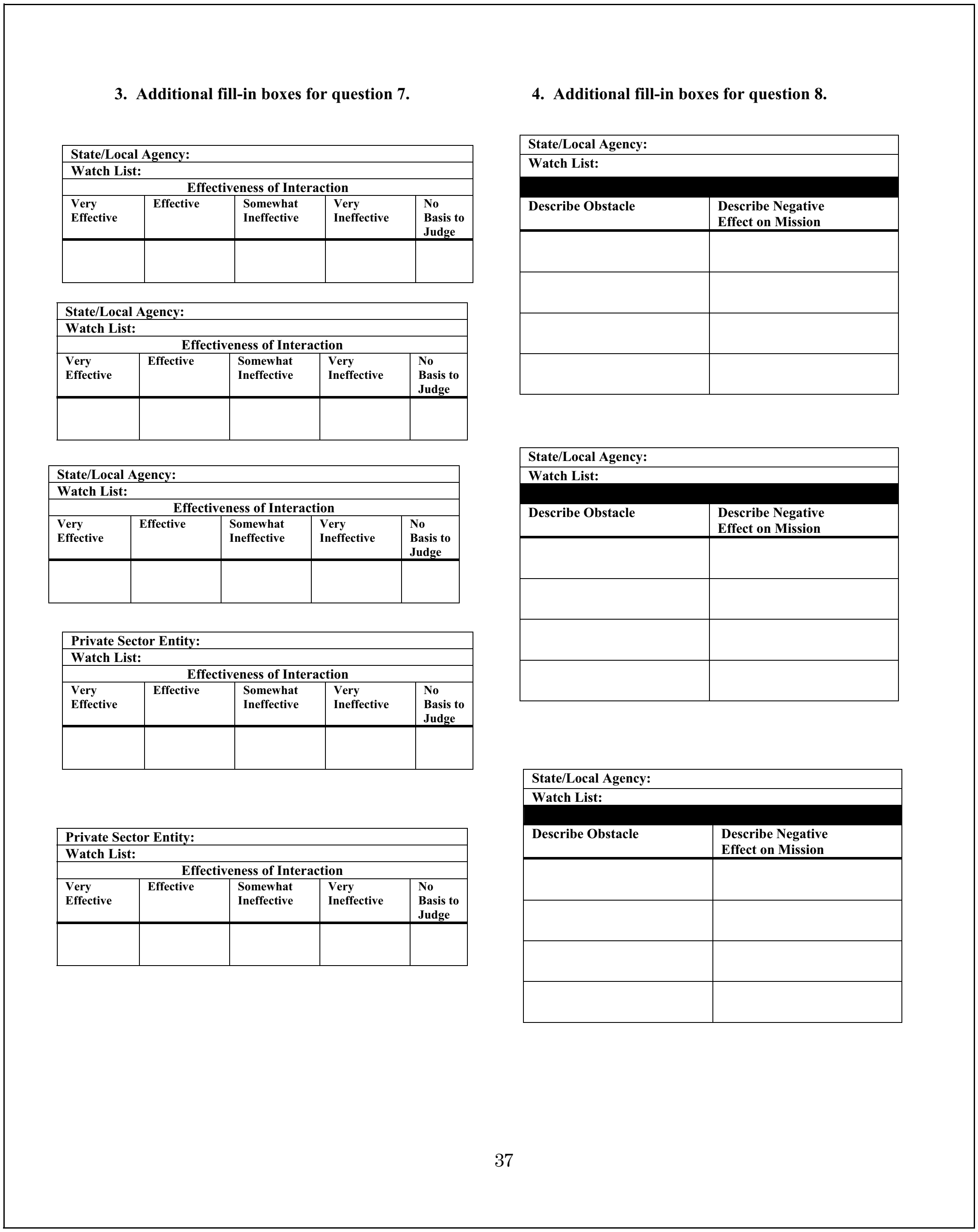
Agency:				
Watch List:				
Effectiveness of Interaction				
Very Effective	Effective	Somewhat Ineffective	Very Ineffective	No Basis to Judge

2. Additional fill-in boxes for question 6.

Agency:	
Watch List:	
Describe Obstacle	Describe Negative Effect on Mission

Agency:	
Watch List:	
Describe Obstacle	Describe Negative Effect on Mission

Agency:	
Watch List:	
Describe Obstacle	Describe Negative Effect on Mission



3. Additional fill-in boxes for question 7.

State/Local Agency:				
Watch List:				
Effectiveness of Interaction				
Very Effective	Effective	Somewhat Ineffective	Very Ineffective	No Basis to Judge

State/Local Agency:				
Watch List:				
Effectiveness of Interaction				
Very Effective	Effective	Somewhat Ineffective	Very Ineffective	No Basis to Judge

State/Local Agency:				
Watch List:				
Effectiveness of Interaction				
Very Effective	Effective	Somewhat Ineffective	Very Ineffective	No Basis to Judge

Private Sector Entity:				
Watch List:				
Effectiveness of Interaction				
Very Effective	Effective	Somewhat Ineffective	Very Ineffective	No Basis to Judge

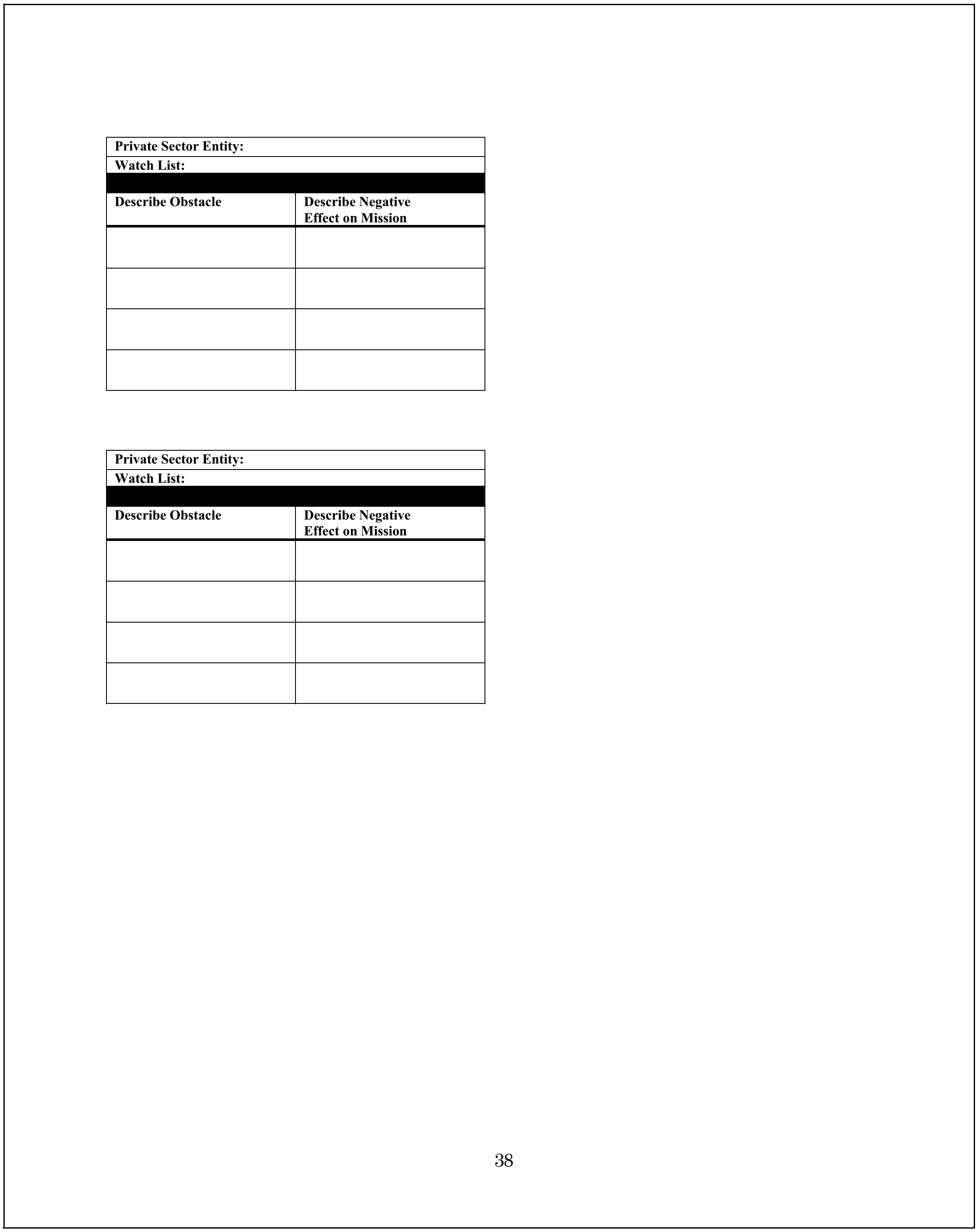
Private Sector Entity:				
Watch List:				
Effectiveness of Interaction				
Very Effective	Effective	Somewhat Ineffective	Very Ineffective	No Basis to Judge

4. Additional fill-in boxes for question 8.

State/Local Agency:	
Watch List:	
Describe Obstacle	Describe Negative Effect on Mission

State/Local Agency:	
Watch List:	
Describe Obstacle	Describe Negative Effect on Mission

State/Local Agency:	
Watch List:	
Describe Obstacle	Describe Negative Effect on Mission



Private Sector Entity:	
Watch List:	
Describe Obstacle	**Describe Negative Effect on Mission**

Private Sector Entity:	
Watch List:	
Describe Obstacle	**Describe Negative Effect on Mission**

GAO Contact and Staff Acknowledgments

GAO Contact

Gary Mountjoy, (202) 512-6367.

Staff Acknowledgments

In addition to the individual named above, Elizabeth Bernard, Neil Doherty, Joanne Fiorino, Will Holloway, Tonia Johnson, Anh Le, Kevin Tarmann, and Angela Watson made key contributions to this report.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to GAO Mailing Lists" under "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON ♻ RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

[redacted]