GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

June 30, 2011

Congressional Committees:

Subject: *The U.S. Government Is Establishing Procedures for a Procurement Ban against Firms that Sell Iran Technology to Disrupt Communications but Has Not Identified Any Firms*

The U.S. Congress has found that the Iranian government continues to engage in systematic and ongoing violations of human rights, including the suppression of freedom of expression. Such violations have reportedly increased in the aftermath of the disputed presidential election in Iran on June 12, 2009. Of particular concern has been the Iranian regime's crackdown on freedom of expression and interference with the use of the Internet, mobile phones, and other means of communication in order to restrict the free flow of information. According to a Freedom House report, the Iranian authorities have employed extensive and sophisticated methods to tamper with Internet access, mobile phone services, and satellite broadcasting; monitor dissenters online; and use monitored information to intimidate and arrest dissenters.[1]

The U.S. government, governments of other nations, and nongovernmental organizations have expressed concern that firms outside Iran have aided the Iranian government in monitoring and suppressing its citizens' activities. For example, in 2008, Nokia Siemens Network,[2] as part of a contract for mobile phone network technology, sold communications monitoring equipment to the Iranian government. As a result of credible reports that the Iranian government misused the technology to suppress dissent and freedom of speech, the company halted all work related to monitoring centers in Iran in March 2009, according to a Nokia Siemens Network statement.

Congress directed us to review issues related to Iran's monitoring, filtering, and disruption of information and communications flows in two mandates: (1) Section 106 of the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010

[1]Freedom House, *Freedom on the Net 2011; A Global Assessment of Internet and Digital Media* (Washington, D.C., and New York, New York, Apr. 18, 2011). According to Freedom House, it is an independent watchdog organization that functions as a catalyst for freedom, democracy, and the rule of law through its analysis, advocacy, and action.

[2]Nokia Siemens Network is a joint venture between the Finnish cell phone maker Nokia and the German company Siemens.

(CISADA) requires us to review a procurement ban against entities that export technologies to the Iranian government for monitoring, filtering, and disrupting information and communications flows,[3] and (2) Senate Report 111-201 related to the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 directs us to identify entities that have a financial interest in the development of Iran's ability to monitor, filter, and disrupt information and communication flows and determine which entities have contracts with the U.S. government.

To address these mandates, this report (1) identifies the steps the U.S. government is taking to implement the procurement ban in Section 106 of CISADA and (2) reviews open source information to identify the firms that export technologies to the Iranian government to disrupt information and communication flows.

To conduct our review, we reviewed documents and interviewed officials from U.S. government agencies including the Departments of State, Commerce, Defense, and the Treasury; Broadcasting Board of Governors;[4] General Services Administration (GSA); U.S. intelligence agencies; nongovernmental organizations; and private sector firms. Specifically, to identify the steps the U.S. government has taken to implement the CISADA procurement ban, we interviewed and reviewed documents from U.S. agency officials responsible for implementing the ban. To conduct our open source review, we conducted searches of industry standard trade publications, marketing reports, corporate statements, Securities Exchange Commission filings, and additional materials. See enclosure I for a full description of our scope and methodology.

We conducted this performance audit from February 2011 to June 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Summary

The U.S. government is establishing procedures to implement the procurement ban, such as issuing an interim rule to federal agencies prohibiting procurement from firms that export sensitive technology to Iran. However, as of June 24, 2011, the U.S. government had identified no entities subject to this ban. Moreover, based on our review of credible open source information, we did not identify any firms that export technologies to the Iranian government for monitoring, filtering, and disrupting information and communications flows. There are several possible reasons for the difficulty in identifying any such firms, including (1) the competitive and proprietary nature of the communication industry limits information, if any, reported in open sources and (2) the lack of a clear distinction between technology exported to Iran to

[3]Pub. L. No. 111-195, § 106, 124 Stat. 1336, codified at 22 U.S.C. § 8515.

[4]The Broadcasting Board of Governors encompasses all U.S. civilian international broadcasting, including the Voice of America, Radio Free Europe/Radio Liberty, Radio Free Asia, Radio and TV Martí, and the Middle East Broadcasting Networks—Radio Sawa and Alhurra Television.

disrupt the free flow of information versus technology exported to Iran to support necessary and acceptable filtering and monitoring of communication. In addition, Iran's growing capacity to develop its own monitoring, filtering, and disrupting technology suggests it is relying less on non-Iranian technology to monitor and filter internal communications.

We are making no recommendations in this report.

Background

The United States' 2010 National Security Strategy states that for decades, the Islamic Republic of Iran has endangered the security of the greater Middle East region and has failed to live up to its international responsibilities. In addition to its illicit nuclear program, Iran continues to support terrorism, undermine peace between Israelis and Palestinians, and deny its people their universal rights. To address these concerns, the United States employs a range of tools, including diplomacy, a military presence in the Persian Gulf, and unilateral sanctions. Since 1987, the United States has implemented numerous sanctions against Iran including a 1995 comprehensive ban on almost all U.S. trade or investment activity involving Iran.[5] On July 1, 2010, Congress enacted CISADA.[6] The law expands existing sanctions and imposes other measures, such as a ban on U.S. government procurement from any person who exports sensitive technology, as defined by the statute, to Iran.[7]

Section 106 of CISADA prohibits the head of an executive agency from entering into or renewing a contract 90 days after July 1, 2010, for the procurement of goods or services with a person who exports sensitive technology to Iran.[8] Section 106 defines sensitive technology as hardware, software, telecommunications equipment, or any other technology that the President determines is to be used specifically to (1) restrict the free flow of unbiased information in Iran or (2) disrupt, monitor, or

[5]A ban on imports of Iranian-origin goods and services was enacted in October 1987 via Executive Order 12613, 52 Fed. Reg. 41,940 (Oct. 29, 1987). In March 1995, the President issued Executive Order 12957, 60 Fed. Reg. 14,615 (Mar. 15, 1995) prohibiting U.S. involvement with petroleum development in Iran. Executive Order 12959, 60 Fed. Reg. 24,757 (May 6, 1995) was issued 2 months later, banning specified exports and investment. On August 19, 1997, the President signed Executive Order 13059, 62 Fed. Reg. 44,531 (Aug. 19, 1997) which consolidated prior executive orders and prohibits virtually all trade and investment activities with Iran by U.S. persons, wherever located, or from the United States.

[6]Pub. L. No. 111-195.

[7]"United States person" in CISADA is defined as a natural person who is a citizen or resident of the United States or a national of the United States; and as an entity that is organized under the laws of the United States or any State. In this report, we use entities to refer to firms or companies.

[8]CISADA section 106 also provides authority to exempt certain products, as defined by the Trade Agreements Act of 1979, from the procurement ban. In addition, CISADA section 401(b) authorizes the Secretary of State, in consultation with the Secretary of Commerce, to waive the imposition of the procurement ban in the national interest of the United States. See 22 U.S.C. § 8551 and Delegation of Certain Functions and Authorities Under the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010, 75 Fed. Reg. 67,025 (Sept. 23, 2010).

otherwise restrict speech of the people of Iran.[9] Under Section 106, we are to assess the extent to which executive agencies would have entered into or renewed contracts for the procurement of goods or services with persons who export sensitive technology to Iran if the prohibition to do so were not in effect.

Senate Report 111-201 directs us to identify entities through open source information that have a financial interest in the development of Iran's online monitoring and filtering, cell phone disruption and monitoring activities, and radio and television signal jamming; and determine which entities have contracts, awards, or purchasing agreements with the U.S. government. We previously reported on commercial activity in Iran's oil, gas, and petrochemical sectors based on a review of open source information. The Senate report also mandates that we update our March 2010 report on firms that have a commercial activity in Iran's energy sector.[10] We will provide this update in a separate report.

U.S. Government Is Establishing Procedures to Implement the Procurement Ban, but Has Not Identified Firms Subject to the Ban

On September 23, 2010, the President delegated authority under CISADA section 106 to the Secretary of State, in consultation with the Secretary of Commerce, including the authority to determine what products are considered sensitive technology.[11] According to State Department (State) officials, they do not plan to further refine the definition of sensitive technologies beyond hardware, software, telecommunications equipment, or any other technology the President determines is to be used to monitor, filter, or disrupt information and communication flows in Iran. State officials stated that creating a list of specific products that are barred under the definition of sensitive technology is impractical and possibly counterproductive due to the rapid changes in technology. Further, State officials said the same technology that enables Internet access and facilitates communications can also be used to monitor, filter, or disrupt the communications of the Iranian people. According to State officials, they want to abide by the broad definition in the statute so they can evaluate firms potentially providing sensitive technologies to Iran on a case-by-case basis.

On September 29, 2010, the Department of Defense, GSA, and the National Aeronautics and Space Administration issued an interim rule that partially

---

[9]CISADA section 103 prohibits the export of goods, services, or technologies of U.S. origin to Iran from the United States or by a U.S. person, wherever located, but also allows for several exceptions including an exception for (1) services incident to the exchange of personal communications over the Internet or software necessary to enable such services, as provided for in section 560.540 of title 31, Code of Federal Regulations; (2) hardware necessary to enable such services; or (3) hardware, software, or technology necessary for access to the Internet. However, pursuant to CISADA and the Iranian Transactions Regulations (31 C.F.R. part 560), individuals and entities will still need to obtain a license from the Treasury Department to export certain items falling under the CISADA section 103 exceptions. See 75 Fed. Reg. 59,611 (Sept. 28, 2010).

[10]GAO, *Firms Reported in Open Sources as Having Commercial Activity in Iran's Oil, Gas, and Petrochemical Sectors*, GAO-10-515R (Washington, D.C.: Mar. 23, 2010).

[11]Delegation of Certain Functions and Authorities Under the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010, 75 Fed. Reg. 67,025 (Sept. 23, 2010).

implements CISADA section 106 by prohibiting agencies from entering into or extending a contract for the procurement of goods or services with a person who exports certain sensitive technology, as defined in CISADA section 106, to Iran.[12] The Federal Register notice also stated that further implementation of CISADA section 106 will follow in an additional Federal Acquisition Regulation case.

According to GSA officials, as of June 15, 2011, the additional provision that further implements CISADA section 106 is in draft form. The provision will require contractors to represent[13] that they do not export sensitive technology, as defined in section 106, to the Iranian government or any entities or individuals owned, controlled, or acting on behalf or at the direction of the Iranian government.[14] According to GSA officials, this provision is in draft form and subject to change; however, they expect the provision to be finalized and published in the Federal Register as an interim rule by August 2011. According to State officials, one of the goals of the contractor representation is to impel contractors to make informed decisions as to what their products are used for and where their products are shipped. According to GSA, a contractor must represent that it does not export sensitive technology, or the contractor will not be able to submit an offer for a U.S. government contract.

According to State officials, they are actively working to identify firms that are knowingly providing technologies to Iran that will be used for the purpose of suppressing the free flow of information and communications. State is reviewing information from open sources, including media outlets. State is also consulting with private firms, nongovernmental organizations, and the intelligence community to help identify such firms. State is still gathering and assessing information but has not identified firms that have provided sensitive information and communications technology to Iran as of June 24, 2011. According to State officials, if the Secretary of State does affirm that a firm provided such technology to Iran, the firm will be recorded in the Excluded Parties List System—a database listing entities that are generally excluded from federal contracts, grants, or other financial benefits. U.S. agency contracting officers are required to check the system prior to awarding a government contract.[15]

According to U.S. government and U.S. private sector officials, CISADA's procurement ban may serve as a deterrent for firms that may otherwise engage in business with Iran. In addition to instituting the ban, State reports that it is monitoring threats to the free flow of information for its annual Human Rights Report on Iran, working with the Treasury Department to develop licensing policies that authorize appropriate new media technologies to Iranian citizens, and working with

---

[12]Federal Acquisition Regulation; Certification Requirement and Procurement Prohibition Relating to Iran Sanctions, 75 Fed. Reg. 60,254 (Sept. 29, 2010).

[13]According to GSA officials, a representation is a statement of fact in which a contractor states that he/she does not export sensitive technology to the government of Iran or entities acting on its behalf. U.S. agencies can penalize the contractor if he/she makes a false statement.

[14]Federal Acquisition Regulation case 2010-018.

[15]48 C.F.R § 9.405.

allies in the multilateral arena to raise the issue of Internet freedom.[16] State and the Broadcasting Board of Governors are also supporting the development of technologies that circumvent information and communications censorship. According to State officials, State has spent $22 million on Internet Freedom programming as of May 11, 2011, and plans to spend $28 million more in 2011. State officials testified that State's grants will support more advanced counter-censorship technologies including circumvention tools in Farsi (a language widely used in Iran), secure mobile communications, and technologies to enable activists to post their own content online and protect against cyber attacks.[17] According to Broadcasting Board of Governors officials, the board plans to spend $10 million to expand and implement new research on circumvention tools.

Challenges Exist in Identifying Firms through Open Sources

Based on our review of credible open source information,[18] we were unable to identify firms that currently export technologies to the Iranian government for monitoring, filtering, and disrupting information and communications flows. As such, we found no firms that have contracts with the U.S. government. There are several possible reasons for the difficulty in identifying any firms. First, the competitive and proprietary nature of the communication industry limits information, if any, reported in open sources. Second, a firm's intention in selling Iran technology may be difficult to discern since technology that can enable acceptable filtering for objectionable sites, such as pornography, can also be used to disrupt the free flow of information and communication. Finally, Iran's need to obtain monitoring and filtering technology from outside sources may be lessening as it develops indigenous censorship and surveillance capabilities, possibly in response to sanctions against western companies selling it sensitive technology.

Competitive and Proprietary Nature of Communication Sector May Limit Information, if any, in Open Sources

We reviewed a wide range of open source information in an attempt to identify entities that currently export technologies to the Iranian government for monitoring, filtering, and disrupting information and communications flows. We reviewed over 60 industry standard trade publications, marketing reports, corporate statements, Securities Exchange Commission filings, and general Web searches. Although we previously used an open source review successfully to report on commercial activity

[16]U.S. Department of State, *Report on Actions by Non-Iranian Companies* (Washington, D.C., Dec. 13, 2010). This report was submitted pursuant to section 1263 of the 2010 Defense Authorization Act.

[17]Michael Posner, Assistant Secretary, Bureau of Democracy, Human Rights, and Labor, and Philo Dibble, Deputy Assistant Secretary for Iran, Bureau of Near Eastern Affairs, U.S. Department of State, *Human Rights and Democratic Reform in Iran*, (written statement submitted to Senate Foreign Relations Committee, Subcommittee on Near Eastern and South and Central Asian Affairs, Washington, D.C., May 11, 2011).

[18]Under our methodology, firms are to be identified only when three reputable industry publications or the firm's corporate statements reported the firm to have signed an agreement to conduct business, invest capital, or received payment for providing goods or services. We do not consider news articles, blogs, or Iranian government statements as credible sources of evidence.

in Iran's oil, gas, and petrochemical sectors,[19] we were not able to use this method to identify firms assisting Iran in developing monitoring, filtering, and disruption technologies. The energy sector has standard industry publications and worldwide surveys where energy projects can be monitored. In contrast, the information and communications technology sector is not as closely tracked and reported on in standard publications. According to private company sources, this lack of information is partly due to the competitive nature of the information and communications industry where commercial and business information on sales and clients is not reported. Private sector officials confirmed that an open source review would not result in complete and credible information. They noted that further information may be obtained from retailers and resellers in the region. Although allegations were made in news articles about companies providing hardware and software for monitoring and filtering purposes to Iran, we were unable to find support for these allegations in open sources that we would consider as credible evidence. Further, although firms such as the Nokia Siemens Network were identified in the past as providing such technology for Iran's cellular network, we found no credible evidence through our open source review that the assistance has continued.

Technology Used for Necessary and Acceptable Operations May Also Be Used by Governments to Interfere with Information and Communication Flows

The same technologies that enable Internet access, satellite radio and television, and cellular communications are also used or manipulated by oppressive regimes for monitoring, filtering, and disrupting information and communications flows. The producing or reselling firm's intent in selling this technology to the Iranian government is difficult to determine and governments may not be transparent in their intended use of a product. Many countries monitor and filter information and communications to some extent, such as to block child pornography and for other law enforcement purposes.[20] According to the International Telecommunications Union, international treaties allow for governments to intercept and monitor Internet and telephone traffic for the purpose of enforcing national laws or executing international conventions, commonly known as lawful interception.[21] The International Telecommunications Union reports that most countries have implemented lawful interception capabilities. For example, the United States requires telecommunications carriers and manufacturers of telecommunications equipment to

[19]GAO-10-515R.

[20]For lawful interception in the United States, in October 1994, Congress enacted the Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (CALEA). The law further defines the existing statutory obligation of telecommunications carriers to assist law enforcement in executing electronic surveillance pursuant to court order or other lawful authorization. CALEA is codified at 47 U.S.C. §§ 1001-1021. According to the Federal Communications Commission, CALEA was intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure they have the necessary surveillance capabilities.

[21]Under the *Constitution of the International Telecommunication Union*, member states of the International Telecommunications Union reserve the right to report communications to the competent authorities to ensure the application of their national laws or the execution of international conventions.

design their equipment, facilities, and services according to lawful interception standards to ensure they have the necessary surveillance capabilities.

In addition to capabilities developed for lawful interception, there are numerous software products available that provide filtering and monitoring capabilities. Organizations use these products to manage their networks, including providing network security and preventing employees from using bandwidth and company time to access objectionable or productivity-affecting sites. For example, according to private sector officials, employers may block Internet sites such as pornography, gambling, dating, fantasy football, and chat sites. Parents also often use filtering software to prevent their children from accessing objectionable content. However, these software products may also be used to block any other content on the Internet. In addition to enabling access to the Internet, routers[22] also include the capability to filter and block traffic, which is necessary for basic cyber-security and network management. This capability can be exploited to block any information on the Internet.

Further, specialized equipment is not needed to disrupt or block satellites for television and radio broadcasts and cell phone use. The same technology used to transmit broadcasts can be used to disrupt it. According to the Broadcasting Board of Governors, Iran engages in two types of satellite jamming, neither of which requires specialized equipment. First, uplink or satellite jamming is done by sending signals from ground stations to the satellite using the same frequency as the service the government may want to disrupt. Second, downlink or terrestrial jamming targets the receiving satellite dishes by sending jamming signals from ground or mobile-based transmitters into dishes located in cities such as Tehran.

Iran Is Building Its Internal Capacity to Develop Monitoring and Filtering Technology

Iran is decreasing its reliance on technology and support from non-Iranian companies to filter, monitor, and disrupt information and communication flows. State reported in December 2010 that the Iranian government is now focused on building its domestic capacity in this area. State further noted that Iranian security continues to increase the budget and manpower devoted to its censorship surveillance systems. The OpenNet Initiative[23] reported in 2009 that the Iranian government is actively increasing its domestic capacity to reduce its reliance on western technologies. OpenNet Initiative also reported that several Iranian technology companies are producing hardware and software products for use in the Iranian filtering system. According to Freedom House, "Iran now employs a centralized filtering system that can effectively block a Web site within a few hours across the entire network in Iran.

[22]A router is a network device that forwards data packets from one computer network to another. Based on internal routing tables, routers read each incoming packet and decide how to forward it. The destination address in the packets determines to which line (interface) outgoing packets are directed. In large-scale enterprise routers, the current traffic load, congestion, line costs and other factors determine to which line to forward.

[23]The OpenNet Initiative is a collaborative partnership of three institutions: the Citizen Lab at the Munk School of Global Affairs, University of Toronto; the Berkman Center for Internet & Society at Harvard University; and the SecDev Group (Ottawa).

Private internet service providers were forced to either use the bandwidth provided by the government or route [requests to visit sites] through government-issued filtering boxes developed by software companies inside Iran."[24]

According to officials from U.S. firms, the sanctions on Iran and the Nokia Siemens Network case may have served as a deterrent for western companies; this may in turn have motivated Iran to develop its own capabilities. Further, nongovernmental and private sector officials noted that Iran may be able to supplement its efforts by procuring some of the technology it needs through the Internet or from resellers and retailers, including those in neighboring countries with porous borders, such as the United Arab Emirates.

Agency Comments

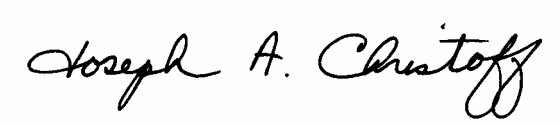
We provided drafts of this report to the Departments of State, Commerce, Defense, and the Treasury; the General Services Administration; and the Broadcasting Board of Governors for their review. Treasury and GSA provided technical comments, which we incorporated into the report as appropriate. State, Commerce, Defense, and the Broadcasting Board of Governors stated they had no comments.

- - - - - - - - - - - - -

We are sending copies of this report to the Secretary of State, Secretary of Commerce, Secretary of the Treasury, Secretary of Defense, General Services Administration Administrator, Broadcasting Board of Governors Executive Director, and appropriate congressional committees. In addition, the report will be available at no charge on GAO's Web site at http://www.gao.gov.

If you or your staffs have any questions about this report, please contact me at 202-512-8979 or christoffj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Major contributors to this report include Tetsuo Miyabara (Assistant Director), JoAnna Berry, Laura Erion, Grace Lui, Kathleen Monahan, Maria Stattel, and Adam Vogt.

Sincerely,



Joseph A. Christoff
Director, International Affairs and Trade

[24]According to Freedom House, "the boxes work by searching for banned text strings—either keywords or domain names—in the URL requests submitted by users." See Freedom House, *Freedom on the Net 2011: A Global Assessment of Internet and Digital Media* (Washington, D.C., and New York, New York, Apr. 18, 2011).

The Honorable Carl Levin
Chairman
The Honorable John McCain
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Tim Johnson
Chairman
The Honorable Richard C. Shelby
Ranking Member
Committee on Banking, Housing, and Urban Affairs
United States Senate

The Honorable Max Baucus
Chairman
The Honorable Orrin G. Hatch
Ranking Member
Committee on Finance
United States Senate

The Honorable John F. Kerry
Chairman
The Honorable Richard G. Lugar
Ranking Member
Committee on Foreign Relations
United States Senate

The Honorable Howard P. McKeon
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Spencer Bachus
Chairman
The Honorable Barney Frank
Ranking Member
Committee on Financial Services
House of Representatives

The Honorable Ileana Ros-Lehtinen
Chairman
The Honorable Howard L. Berman
Ranking Member
Committee on Foreign Affairs
House of Representatives

The Honorable Dave Camp
Chairman
The Honorable Sander Levin
Ranking Member
Committee on Ways and Means
House of Representatives

Enclosure I

Objectives, Scope, and Methodology

To identify the steps the U.S. government has taken to implement the procurement ban against firms that export technologies to the Iranian government for monitoring, filtering, and disrupting communication flows—as delineated in Section 106 of the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010—we interviewed officials and reviewed documentation from the key U.S. government agencies responsible for implementing the procurement ban. This included the Departments of State, Commerce, Defense, and the Treasury; and the General Services Administration (GSA). We reviewed applicable laws, the Federal Register, and Federal Acquisition Regulation draft and interim rules. We requested a list of firms identified for the procurement ban from the Department of State. We searched the federal government's Excluded Parties List System's online database that is maintained by GSA (1) to confirm that a code and template description was entered for the procurement ban and (2) for entities suspended or debarred from government contracts as a result of providing sensitive information and communications technology to Iran. To ensure our understanding of the technologies involved and to further discuss firms under consideration for the ban, we also interviewed and obtained documentation from the Broadcasting Board of Governors;[25] U.S. intelligence agencies; nongovernmental organizations including OpenNet Initiative and Freedom House; and private sector firms.

To identify firms, through open sources, that export technologies to the Iranian government for monitoring, filtering, and disruption of information and communications flows, we reviewed and analyzed open source information dated from January 1, 2005, to June 24, 2011, that our information specialists determined to be credible and comprehensive. Open source information is overt and publicly available information, as opposed to covert or classified. It is also a key component of information collected by traditional intelligence and information-gathering agencies, such as the Central Intelligence Agency. Open source information can provide a broad range of useful data for analysis, but the validity of an analysis can be compromised if it relies on open sources that contain inaccurate, imprecise, incomplete, or otherwise faulty information.

As a result, we relied only on information from credible sources to identify firms as having a financial interest in the development of Iran's monitoring, filtering and disruption of its information and communications infrastructure that met one of the following criteria: (1) if the firm was listed in three reputable industry publications or (2) if the firm's corporate statements reported the firm to have signed an agreement to conduct business; invested capital; or received payment for providing goods or services in connection with these technologies. We excluded sources deemed insufficiently reliable, such as newspaper reports, newswires, and direct news releases from the Iranian government.

[25]The Broadcasting Board of Governors encompasses all U.S. civilian international broadcasting, including the Voice of America, Radio Free Europe/Radio Liberty, Radio Free Asia, Radio and TV Martí, and the Middle East Broadcasting Networks—Radio Sawa and Alhurra Television.

We reviewed a wide range of open source information in an attempt to identify entities, including industry standard trade publications, marketing reports, corporate statements, Securities Exchange Commission filings, and general Web searches. We searched Nexis.com to find content files covering the Internet, telecommunications, and electronics industries between January 1, 2000, and June 24, 2011. Included in these files were over 60 industry standard trade publications, such as *Electronics Engineering Times*, *Communications Today*, and *TechWeb*. We searched Gartner.com for marketing reports and firm Web sites for press releases and corporate statements. We searched and analyzed Securities Exchange Commission filings filed between December 31, 2006, and March 14, 2011. We also conducted general Web searches for specific firms named in nongovernmental reports, in interviews with private sector firms, or extensively mentioned in the media.

To ensure our understanding of the technologies involved, to conduct follow-up research on firms alleged to be exporting sensitive technologies to Iran, and to identify the challenges involved in identifying such firms through open sources, we interviewed officials and reviewed documentation from U.S. government agencies including the Departments of State, Defense, Commerce, and the Treasury; Broadcasting Board of Governors; U.S. intelligence agencies; private sector officials; and nongovernmental organizations, including OpenNet Initiative and Freedom House, among others. Classified information was used to corroborate our unclassified findings but is not included in this report.

We conducted this performance audit from February 2011 to June 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(320832)