April 26, 2012

VIA FAX (202) 482-0800
Freedom of Information Act Request
Freedom of Information Officer
Department of Commerce
Bureau of Industry and Security, Room 6622
U.S. Department of Commerce
Washington, DC 20230

Re: Freedom of Information Act Request and Request for Expedited Processing

Dear FOIA Officer:

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the Bureau of Industry and Security ("BIS"). As detailed below, EPIC seeks agency records concerning investigations by BIS into the export of surveillance technology by U.S. firms.

Factual Background

The Electronic Privacy Information Center ("EPIC") is a public interest research center located in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues. EPIC has a demonstrated interest in international privacy issues[1] and has written to the Department of Commerce in the past concerning the export of surveillance technology to China.[2]

BIS is responsible for implementing and enforcing the Export Administration Regulations ("EAR").[3] The EAR covers "dual use" commodities, software, and technology that have both military and commercial applications.[4] The EAR also contains the Commerce Control List ("CCL")[5] and the Commerce Country Chart.[6] If the reason

[1] *See generally* EPIC AND PRIVACY INTERNATIONAL, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS (2006).
[2] *See* Letter from Marc Rotenberg, Executive Director, EPIC, to Carlos M. Gutierrez, Secretary, Department of Commerce, (Sept. 20, 2006), https://epic.org/privacy/intl/doc_china_letter.pdf (urging the reexamination of export policies that "prohibit[] the export of traditional security devices while permitting the sale of products that make possible far more widespread surveillance and political control.").
[3] *See* 15 C.F.R. §§ 730-774 (2012).
[4] *See* 15 C.F.R. ch. VII, subch. C.
[5] *See* 15 C.F.R. § 774, Supp. 1 (2012).
[6] *See* 15 C.F.R. § 738, Supp. 1 (2012).

for control of a commodity, software, or technology listed on the CCL applies to a country on the Commerce Country Chart, a license is required unless there is an exception available.[7] Items not appearing on the CCL are subject to the catch-all "EAR99" designation, under which a license is required if the item is bound for an embargoed nation or the item will be used for prohibited end-uses or by prohibited end-users.[8] Export regulations also require a license for the export of "items that may be used for the surreptitious interception of wire, oral, or electronic communications. . . ."[9] Finally, The Department of Commerce is also responsible for launching investigations into violations of these licensing restrictions.

Recently, reports have indicated that Syrian officials used devices manufactured by U.S. companies to monitor Internet usage in the country in October, 2011.[10] These devices, made by Blue Coat Systems ("Blue Coat") of Sunnyvale, California, have the functionality to monitor network traffic and block websites.[11] Blue Coat initially denied that they sold products to Syria, but admitted that the devices could have made their way to Syria through third parties.[12] Furthermore, these devices were "transmitting automatic status messages back to [Blue Coat] as [they] censored the Syrian Web."[13]

On November 9, 2011, during a hearing before the Senate Subcommittee on Near Eastern and South and Central Asian Affairs, Jeffrey Feltman said that "The Department of Commerce is looking into . . . this very specific case because there was no license issue[d] to send this stuff to Syria. . . . [A]ny such item like this that would be exported to Syria, requires on a case by case examination and an export license. . . . [T]he Department of Commerce is investigating it."[14] Several U.S. Senators responded by sending a letter to the Secretaries of the Department of State and the Department of Commerce requesting that they

> "investigate and report to us on the following issues: 1) whether the reports of [Blue Coat's] involvement in providing technology to the Syrian government is [sic] accurate; 2) if these reports are accurate, whether such

[7] *See* 15 C.F.R. § 738.4 (2012).
[8] *See* 15 C.F.R. §§ 736, 742, 744, 746 (2012).
[9] 15 C.F.R. § 742.13 (2012).
[10] Sari Horwitz, *Syria Using American Software to Censor Internet, Experts Say*, Wash. Post, Oct. 22, 2011, *available at* http://www.washingtonpost.com/world/national-security/syria-using-american-software-to-censor-internet-experts-say/2011/10/22/gIQA5mPr7L_story.html.
[11] *Id.*
[12] *Id.*
[13] Jennifer Valentino-Devries, Paul Sonne & Nour Malas, *U.S. Firm Acknowledges Syria Uses Its Gear to Block Web*, Wall St. J., Oct. 29, 2011, *available at* http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html.
[14] *Hearing on U.S. Policy in Syria: Hearing Before the Subcomm. on Near Eastern & South & Central Asian Affairs of the S. Comm. on Foreign Relations*, 112th Cong. (2011) (testimony of Jeffrey Feltman, Assistant Secretary of State for Near Eastern Affairs, Department of State).

equipment has been used to carry out human rights abuses; and 3) whether [Blue Coat's] sales are in violation of U.S. export law."[15]

On November 17, 2011, the Washington Post reported that the Department of Commerce had launched an investigation into how the Syrian regime both owned and used surveillance equipment manufactured by Blue Coat.[16] The article stated that "[c]ommerce officials are attempting to determine whether [Blue Coat] had prior knowledge that its equipment and software was being used by the Syrian government, according to several U.S. officials."[17] On December 16, 2011, BIS determined that two third-party individuals that Blue Coat had sold devices to "act[ed] contrary to the national security or foreign policy interests of the United States" in selling these Blue Coat devices to Syria and added them to the Entity List, limiting their ability to trade with U.S. companies.[18]

Blue Coat is not the only company selling technology that will enable repressive regimes to monitor and control their population's Internet usage. Syrian officials contracted with an Italian company to build a system "with the power to intercept, scan and catalog virtually every e-mail that flows through the country" using storage hardware and software from California-based NetApp,[19] a move criticized by Senators Kirk, Casey, and Coons.[20] McAfee has provided "content-filtering software used by Internet-service providers in Bahrain, Saudi Arabia and Kuwait" and Websense, Inc. sold its Web-filtering technology in Yemen.[21] Narus, a Boeing subsidiary, sold surveillance

---

[15] Letter from Mark Kirk, Sen., Robert P. Casey, Jr., Sen., & Christopher A. Coons, Sen., to Hillary Rodham Clinton, Secretary of State, & John Bryson, Secretary of Commerce (Nov. 10, 2011), *available at* http://www.kirk.senate.gov/pdfs/KirkCaseyCoons.pdf.

[16] Sari Horwitz & Shyamantha Asokan, *U.S. Probing Use of Surveillance Technology in Syria*, Wash. Post, Nov. 17, 2011, *available at* http://www.washingtonpost.com/world/national-security/us-probes-use-of-surveillance-technology-in-syria/2011/11/17/gIQAS1iEVN_story.html.

[17] *Id.*

[18] Addition of Certain Persons to the Entity List; and Implementation of Entity List Annual Review Changes 76 Fed. Reg. 242 (Dep't of Commerce Dec. 16, 2011) (final rule), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-12-16/html/2011-32341.htm. *See also* Press Release, Bureau of Industry and Security, Dep't of State, BIS Adds Two Parties to Entity List for Sending Internet Filtering Equipment to Syria (Dec. 15, 2011), *available at* http://www.bis.doc.gov/news/2011/bis_press12152011.htm.

[19] Ben Elgin & Vernon Silver, *Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear*, Bloomberg, Nov. 3, 2011, *available at* http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html.

[20] *See* Kirk, Casey, & Coonz *supra* note 18.

[21] *See* Paul Sonne & Steve Stecklow, *U.S. Products Help Block Mideast Web*, Wall St. J., Mar. 27, 2011, *available at* http://online.wsj.com/article/SB10001424052748704438104576219190417124226.html; *see also* James Temple, *Bay Area Firms' Technology Used for Oppression*, San. Fran. Chronicle, Mar. 11, 2012, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2012/03/10/BUU01NIMCF.DTL.

technology to Egypt,[22] Cisco Systems allegedly sold surveillance equipment that China used to facilitate human rights abuses.[23]

Documents Requested

EPIC requests copies of the following agency records in possession of the Department of Commerce:

1. Any agency records created by the Department of Commerce as part of its investigation into Blue Coat Systems;

2. Any communications or briefings to members of Congress regarding this investigation;

3. Any communications with other agencies regarding the sale of surveillance technology by U.S. firms to violators of human rights;

4. Any agency records related to investigations into the sale of surveillance technology by U.S. companies—including, but not limited to, NetApp, McAfee, Websense, Narus/Boeing, or Cisco Systems—to countries or entities based in countries deemed "Not Free" in 2011 by Freedom House[24].

Request for Expedited Processing

This request warrants expedited processing because it is made by "a person primarily engaged in disseminating information …" and it pertains to a matter about which there is an "urgency to inform the public about an actual or alleged federal government activity."[25]

---

[22] Timothy Karr, *One U.S. Corporation's Role in Egypt's Brutal Crackdown*, HUFFINGTON POST, Jan. 28, 2011, www.huffingtonpost.com/timothy---karr/one---us---corporations---role---_b_815281.html.
[23] Rainey Reitman, *Cisco and Abuses of Human Rights in China: Part 1*, ELEC. FRONTIER FOUND., Aug. 22, 2011, https://www.eff.org/deeplinks/2011/08/cisco---and---abuses---human---rights---china---part---1.
[24] In 2011, Freedom House's Freedom in the World report listed the following countries as "Not Free": Afghanistan, Algeria, Angola, Azerbaijan, Bahrain, Belarus, Brunei, Burma, Cambodia, Cameroon, Chad, China, Congo, Democratic Republic of (Kinshasa), Congo, Republic of (Brazzaville), Côte d'Ivoire, Cuba, Djibouti, Egypt, Equatorial Guinea, Eritrea, Ethiopia, Gabon, Gaza Strip, Iran, Iraq, Jordan, Kazakhstan, Laos, Libya, Mauritania, Nagorno-Karabakh, North Korea, Oman, Pakistani Kashmir, Qatar, Russia, Rwanda, Saudi Arabia, Somalia, South Ossetia, Sudan, Swaziland, Syria, Tajikistan, Tibet, Transnistria, Tunisia, Turkmenistan, United Arab Emirates, Uzbekistan, Vietnam, West Bank, Western Sahara, Yemen, Zimbabwe. The report can be found online at http://www.freedomhouse.org/report/freedom-world/freedom-world-2011.
[25] 5 U.S.C. § 552(a)(6)(E)(v)(II) (2008); *Al-Fayed v. CIA*, 254 F.3d 300, 306 (D.C. Cir. 2001).

EPIC is "primarily engaged in disseminating information."[26]

There is a particular urgency for the public to obtain information about the export of surveillance technology by U.S. firms to repressive regimes. These activities have been the subject of numerous reports by the national media,[27] requests for information by members of Congress,[28] and even federal lawsuits.[29] Many of the firms in question also sell their products and services in the United States. There is uncertainty over whether current legal regimes are able to hold these firms accountable. Thus, one of the only remaining accountability options is consumer spending patterns, a mechanism which requires that consumers possess sufficient information about the firms' business activities.

Furthermore, President Obama recently signed an executive order authorizing U.S. officials to impose sanctions against persons involved in the use of information and communications technology to facilitate human rights abuses in Syria and Iran.[30] The existence of this order provides further support for the importance and timeliness of this issue.

Request for "News Media" Fee Status

EPIC is a "representative of the news media" for fee waiver purposes.[31] Based on our status as a "news media" requester, we are entitled to receive the requested record with only duplication fees assessed. Further, because disclosure of this information will "contribute significantly to public understanding of the operations or activities of the government," any duplication fees should be waived.

---

[26] *American Civil Liberties Union v. Department of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).
[27] *See* James Temple, *Bay Area Firms' Technology Used for Oppression*, San. Fran. Chronicle, Mar. 11, 2012, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2012/03/10/BUU01NIMCF.DTL; Paul Sonne & Steve Stecklow, *U.S. Products Help Block Mideast Web*, Wall St. J., Mar. 27, 2011, *available at* http://online.wsj.com/article/SB10001424052748704438104576219190417124226.html; Ben Elgin & Vernon Silver, *Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear*, Bloomberg, Nov. 3, 2011, *available at* http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html; *The Technology Helping Repressive Regimes Spy*, NPR, Dec. 14, 2011, https://www.npr.org/2011/12/14/143639670/the-technology-helping-repressive-regimes-spy; Sari Horwitz & Shyamantha Asokan, *U.S. Probing Use of Surveillance Technology in Syria*, Wash. Post, Nov. 17, 2011, *available at* http://www.washingtonpost.com/world/national-security/us-probes-use-of-surveillance-technology-in-syria/2011/11/17/gIQAS1iEVN_story.html.
[28] *See* Kirk, Casey, & Coonz *supra* note 18.
[29] *See* Rainey Reitman, Cisco and Abuses of Human Rights in China: Part 1, Electronic Frontier Foundation, Aug. 22, 2011, https://www.eff.org/deeplinks/2011/08/cisco-and-abuses-human-rights-china-part-1.
[30] Exec. Order No. 13606, 77 Fed. Reg. 24571 (Apr. 22, 2012) *available at* http://www.gpo.gov/fdsys/pkg/FR-2012-04-24/html/X12-10424.htm.
[31] *EPIC v. Department of Defense*, 241 F. Supp. 2d 5 (D.D.C. 2003).

Thank you for your consideration of this request. As provided in 15 C.F.R. § 4.6(e)(4), I will anticipate your determination on our request for expedited processing within ten (10) calendar days.

Respectfully Submitted,

Ginger McCall
Director, EPIC Open Government Program

David Jacobs
EPIC Consumer Protection Fellow