

VIA EMAIL

April 13, 2018

Toni Fuentes
FOIA Officer
National Protection and Programs Directorate
U.S. Department of Homeland Security
245 Murray Lane SW
STOP-0655
Washington, D.C. 20528
Email: NPPD.FOIA@dhs.gov

Dear Mr. Fuentes:

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 Department of Homeland Security (“DHS”) National Protection Programs Directorate (“NPPD”).

EPIC seeks the NPPD’s Privacy Impact Assessment for “Media Monitoring Services” and related records.¹

Documents Requested

- (1) The required Privacy Impact Assessment conducted the April 3, 2018 solicitation for “Media Monitoring Services;”
- (2) Any associated agency records including but not limited to policy guidelines, memoranda, email communications, and Privacy Threshold Analysis related to “Media Monitoring Services;”
- (3) All awarded contracts for “Media Monitoring Services.”

Background

On April 3, 2018, the NPPD posted a solicitation seeking a contractor to help monitor news sources from around the world as well as compile a database of journalists and “media influencers.”² The Draft Statement of Work (“SOW”) outlined several requirements that the contractor must provide such as media comparison tools, communication tools, and design and rebranding tools for monitoring and identifying “any and all media coverage related to the [DHS]

¹ U.S. Dep’t of Homeland Sec., RNBO-18-00041, Media Monitoring Services (Apr. 3, 2018), <https://www.fbo.gov/index.php?s=opportunity&mode=form&id=22aa793f75ce05efd160cfa36d7a8acc&tabmode=list&ab=core>

² *Id.*

or a particular event.”³ The NPPD stated that it has a “critical need to incorporate these function into their programs in order to better reach Federal, state, local, triable and private partners.”⁴

According to the SOW, the NPPD wishes to track more than 290,000 global news sources through various mediums such as “online, print, broadcast, cable, radio, trade and industry publications, local sources, national/international outlets, traditional news sources, and social media.”⁵ The NPPD wants services to track media coverage in over 100 languages including Arabic, Chinese, and Russian and have the ability to instantly translate these articles into English. Additionally, the NPPD wants to have the option to “create unlimited data tracking, statistical breakdown, and graphical analysis on any coverage on an ad-hoc basis.”⁶ The scope of the coverage includes a search feature that would create “up to 20 searches with each unlimited keywords” as well as unlimited coverage per search “with no cap on coverage.”

The selected contractor shall provide the NPPD with 24-hours a day, seven days a week access to both a “password protected” mobile application and online platform of the compiled media coverage.⁷ The SOW does not include details about whether the selected contractor must provide additional cybersecurity safeguards other than password protection. In both services, mobile and online, the NPPD wants the ability to build media lists based on “beat, location, outlet type/size, and journalist role.”⁸ The mobile and online services must include the search results in terms of both online articles and social media conversations.⁹ The SOW does not specify whether personally identifiable social media handles or article attributions would be removed prior to the media coverage being placed on the online and mobile platforms. The online platform service must allow the NPPD to analyze the collected media coverage by a variety of categories including content, volume, geographical spread, top posters, influencers, and even the journalist’s sentiment.¹⁰ The ability to not only identify top posters and media influencers but also the ability to build categorical lists that include a journalist’s role in a media outlet invariably includes personally identifiable information attributed to an individual.

In addition to data collection services, the NPPD wants a 24-hours a day, seven days a week access to a “password protected” database of media influencers, which includes journalists, bloggers, editors, correspondents, and social media influencers.¹¹ This database would be capable of searching and identifying individual media influencers based on their prior publications, their location, beat, the publications they write for, and relevant contact information.¹² The database would also be capable of keyword searches in both English and foreign languages, including

³ U.S. Dep’t of Homeland Sec., Draft Statement of Work for Media Monitoring Services 1 (2018), available at <https://www.fbo.gov/utills/view?id=d9457031df47f06feec110d18dfbc7ef> [hereinafter Draft Statement of Work].

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

⁷ *Id.* at 2

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Id.*

¹² *Id.*

Arabic, Chinese, and Russian.¹³ This database undoubtedly includes personally identifiable information about media influencers.

Responses to the solicitation are due on April 13, 2018.¹⁴

PIA Requirement

The DHS Privacy Office requires that every technology system complete a Privacy Threshold Analysis (“PTA”) as a first step in its Certification & Accreditation process, an internal security and operating compliance process that assures that the information technology systems meet the appropriate standards.¹⁵ If the DHS Privacy Office determines that the DHS program or system has privacy implications, then it will require additional privacy compliance documentation (i.e., a Privacy Impact Assessment).

According to Section 208 of the E-Government Act, an agency is required to undertake a Privacy Impact Assessment (“PIA”) when a federal agency “develop[s] or procur[es] information technology that collects, maintains, or disseminates information that is in an identifiable form,” and (2) when an agency “initiat[es] a new collection of information” that “includes any information in an identifiable form.”¹⁶ This identifiable information, referred to as personally identifiable information (“PII”), is any information in a program or system that allows the identity of an individual to be directly or indirectly inferred.¹⁷ The Office of Management and Budget (“OMB”), for the purposes of the E-Government Act, follows the Clinger-Cohen Act definition of information technology: “any equipment, software or **interconnected system or subsystem** that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.”¹⁸

The OMB further states: “Agencies should commence a PIA **when they begin to develop** a new or significantly modified IT system or information collection.” PIAs at the “IT development stage”:

1. should address privacy in the documentation related to systems development, including, as warranted and appropriate, statement of need, functional requirements

¹³ *Id.*

¹⁴ U.S. Dep’t of Homeland Sec., Media Monitoring Services, *supra* note 1.

¹⁵ U.S. Dep’t of Homeland Sec., Privacy Impact Assessments: The Privacy Office Official Guidance 1 (2010), https://www.dhs.gov/sites/default/files/publications/privacy_pia_guidance_june2010_0.pdf [hereinafter DHS PIA Official Guidance]; *See also* Privacy Compliance: Privacy Threshold Analysis (PTA), Dept. of Homeland Sec. (Mar. 30, 2017), <https://www.dhs.gov/compliance>.

¹⁶ E-Government Act of 2002, Pub. L. No. 107-347, § 208 (b)(1)(A)(i)-(ii), 116 Stat. 2899 (2002).

¹⁷ DHS PIA Official Guidance, *supra* note 15, at 4.

¹⁸ Clinger-Cohen Act of 1996, 40 U.S.C. § 11101(6) (2011) (emphasis added); *See* Exec. Office of the President, Office of Mgmt and Budget, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003), <https://www.whitehouse.gov/wp-content/uploads/2017/11/203-M-03-22-OMB-Guidance-for-Implementing-the-Privacy-Provisions-of-the-E-Government-Act-of-2002-1.pdf> [hereinafter OMB E-Government Act Guidance].

analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment;

2. should address the impact the system will have on an individual’s privacy, specifically identifying and evaluating potential threats relating to each of the elements identified in section II.C.1.a.(i)-(vii) above, to the extent these elements are known at the initial stages of development;

3. may need to be updated before deploying the system to consider elements not identified at the concept stage (e.g., retention or disposal of information), to reflect a new information collection, or to address choices made in designing the system or information collection as a result of the analysis.¹⁹

A database of journalists, the “media influencer database” described in Section 2.5 (“Task Five: Media Engagement”) of the SOW, is a system of records containing information retrievable by name. Sections 2.1, 2.2, and 2.4 would trigger Section 208 obligations as the searches, per the terms of the system description, could include personally identifiable information such as authorship attribution and social media handles.²⁰ Additionally, the platform will allow agency officials to search lists and analyze the coverage based on “top posters/influencers.”²¹

The “developing or procuring” of a “Media Monitoring System”—which is an informational technology system that will collect and maintain PII—triggers the PIA requirement. The DHS has already “beg[un] to develop” that system, which means the PIA should already be completed.²²

Request for Expedition

EPIC is entitled to expedited processing of this request under the FOIA and the DHS’s FOIA regulations. 5 U.S.C. § 552(a)(6)(E)(v)(II); 6 C.F.R. § 5.5(e)(1)(ii). Specifically, this request is entitled to expedited processing because, first, there is an “urgency to inform the public about an actual or alleged federal government activity,” and, second, because the request is “made by a person who is primarily engaged in disseminating information.” § 5.5(e)(1)(ii).

First, there is an “urgency to inform the public about an actual or alleged federal government activity.” § 5.5(e)(1)(ii). The “actual...federal government activity” at issue is

¹⁹ OMB E-Government Act Guidance, *supra* note 18, at 5–6 (emphasis added).

²⁰ Draft Statement of Work, *supra* note #, at 1–2 (describing the ability to “create unlimited data tracking. . . on any coverage,” the ability to “analyze media coverage in terms of . . . top posters, [and] influencers,” and the ability to “build media lists based on . . . journalist role”).

²¹ *Id.*

²² OMB E-Government Act Guidance, *supra* note 18, at 5–6 (stating that agencies should commence a PIA “when they begin to develop a new . . . IT system or information collection” and the PIA “may need to be updated before deploying the system”).

DHS's solicitation of a contractor to help the agency monitor social media and news sources as well as identify and compile a database of "media influencers."

"Urgency" to inform the public about this activity is clear given that the response to the solicitation are due on April 13, 2018. This solicitation comes at the heels of heightened concern about the spread of misinformation through the media and the possibility of foreign influence in U.S. democratic institutions through "fake news." In its 2017 Freedom of the Press Report, watchdog organization Freedom House reports that global media freedom reached its lowest level in 13 years in 2016 with unprecedented threats to journalism, in part by President Trump's disparagement of the credibility of the press.²³ Recently, nineteen members of Congress sent a letter to Attorney General Jeff Sessions to request Qatar-based news channel Al Jazeera to register as a "foreign agents" under the Foreign Agents Registration Act.²⁴ Led by Reps. Josh Gottheimer (D-N.J.) and Lee Zeldin (R-N.Y.), the letter states "We find it troubling that the content produced by this network often directly undermines American interests with favorable coverage of the U.S. State Department-designated Foreign Terrorist Organizations, including Hamas, Hezbollah, Palestinian Islamic Jihad, and Jabhat al-Nusra, al-Qaeda's branch in Syria." The efforts by lawmakers and the Trump administration to undermine press freedom in that past creates an urgency for the public to know to what extent are NPPD's efforts to create a database that not only identifies journalists but tracks the "sentiments" of thousands of press outlets and analyzes media coverage based on top posters and influencers.

Second, EPIC is an organization "primarily engaged in disseminating information." 6 C.F.R. § 5.5(e)(1)(ii). As the Court explained in *EPIC v. DOD*, "EPIC satisfies the definition of 'representative of the news media'" entitling it to preferred fee status under FOIA. 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

In submitting this request for expedited processing, I certify that this explanation is true and correct to the best of my knowledge and belief. 6 C.F.R. § 5.5(e)(3); 5 U.S.C. § 552(a)(6)(E)(vi).

Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for fee classification purposes. *EPIC v. DOD*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on EPIC's status as a "news media" requester, EPIC is entitled to receive the requested record with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

Further, any duplication fees should also be waived because (i) "disclosure of the requested information is in the public interest because it is likely to contribute to the public understanding of the operations or activities of the government" and (ii) "disclosure of the

²³ Jennifer Dunham, Freedom House, *Press Freedom's Dark Horizon 3* (2017), https://freedomhouse.org/sites/default/files/FOTP_2017_booklet_FINAL_April28.pdf.

²⁴ Letter from Josh Gottheimer, Rep. N.J. 5th Dist., et al, to Hon. Jeff Sessions, Attorney Gen., U.S. Dep't of Justice (Mar. 6, 2018), https://gottheimer.house.gov/uploadedfiles/3.6_gottheimer_zeldin_cruz_letter_to_doj_final_signed_copy.pdf.

information is not primarily in the commercial interest” of EPIC, the requester. 6 C.F.R. § 5.11(k)(1); 5 U.S.C. § 552(a)(4)(A)(iii). EPIC’s request satisfies this standard based on the DHS’s considerations for granting a fee waiver. 6 C.F.R. §§ 5.11(k)(2–3).

(1) Disclosure of the requested information is likely to contribute to the public understanding of the operations or activities of the government.

First, disclosure of the requested documents is “in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government.” 6 C.F.R. § 5.11(k)(2). DHS components evaluate these four factors to determine whether this requirement is met: (i) the “subject of the request must concern identifiable operations or activities of the federal government, with a connection that is direct and clear, not remote or attenuated”; (ii) disclosure “must be meaningfully informative about government operations or activities in order to be ‘likely to contribute’ to an increased public understanding of those operations or activities”; (iii) “disclosure must contribute to the understanding of a reasonably broad audience of persons interested in the subject, as opposed to the individual understanding of the requester,” and (iv) “[t]he public’s understanding of the subject in question must be enhanced by the disclosure to a significant extent.” *Id.*

On the first factor, the subject of the request self-evidently concerns “identifiable operations or activities of the federal government” because the NPPDS posted the solicitation for “Media Monitoring Services” and has a critical need to incorporate these services into its programs. 6 C.F.R. § 5.11(k)(2)(i).

On the second factor, disclosure would also be “meaningfully informative about” these operations or activities and is thus “‘likely to contribute’ to an increased understanding of government operations or activities” because there is little information available about the extent of the monitoring services and media influencer database. While the SOW describes the types of services solicited, it does not address any privacy assessments or safeguards that is required by law when an agency is procuring new technology that collects personally identifiable information. 6 C.F.R. § 5.11(k)(2)(ii).

On the third factor, disclosure will “contribute to the understanding of a reasonably broad audience of persons interested in the subject” because, as provided in the DHS FOIA regulations, DHS components will “presum[e] that a representative of the news media will satisfy this consideration.” 6 C.F.R. § 5.11(k)(2)(iii).

Finally, on the fourth factor, the public’s understanding will “be enhanced by the disclosure to a significant extent” because the solicitation was issued by a DHS component office that is actively engaged in protecting the nation’s physical and cyber infrastructure. Little information is publicly known about the extent and purpose of this database other than what has been described in the SOW. Various news outlets and organizations have expressed concerns that the creation of this database and the extent of the monitoring may have a chilling effect on press freedom.²⁵ DHS Press Secretary Tyler Houlton tweeted that “the request is nothing more

²⁵ See e.g., Michelle Fabio, *Department of Homeland Security Compiling Database of Journalists and ‘Media Influencers’*, Forbes (Apr. 6, 2018),

than the standard practice of monitoring current events in the media. Any suggestion otherwise is fit for tin foil hat wearing, black helicopter conspiracy theorists.”²⁶ Regardless of whether this is standard practice, the public has a right to know whether the NPPD has conducted a PIA or considered the privacy implications before collecting potentially large amounts of data on a targeted group of people containing personally identifiable information.

(2) Disclosure of the information is not primarily in the commercial interest of the requester

Second, “[d]isclosure of the information is not primarily in the commercial interest” of EPIC. § 5.11(k)(3). In determining whether this second requirement is met, the DHS components evaluate the following two factors: (i) whether there is “any commercial interest of the requester . . . that would be furthered by the requested disclosure”; and/or (ii) whether “the public interest is greater than any identified commercial interest in disclosure,” and “[c]omponents ordinarily shall presume that where a news media requester has satisfied the public interest standard, the public interest will be the interest primarily served by disclosure to that requester.” *Id.*

On the first factor, there is not “any commercial interest of the requester . . . that would be furthered by the requested disclosure.” 6 C.F.R. § 5.11(k)(3)(i). EPIC has no commercial interest in the requested records. EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.²⁷

On the second factor, “the public interest is greater than any identified commercial interest in disclosure.” 6 C.F.R. § 5.11(k)(3)(ii). Again, EPIC has no commercial interest in the requested records and has established that there is significant public interest in the requested records. Moreover, the DHS should presume that EPIC has satisfied 6 C.F.R. § 5.11(k)(3)(ii). The DHS FOIA regulations state “[c]omponents ordinarily shall presume that where a news media requester has satisfied the public interest standard, the public interest will be the interest primarily served by disclosure to that requester.” *Id.* EPIC is a news media requester and, as set out above, this request satisfies the public interest standard.

For these reasons, a full fee waiver should be granted for EPIC’s request.

<https://www.forbes.com/sites/michellefabio/2018/04/06/department-of-homeland-security-compiling-database-of-journalists-and-media-influencers/>; Cary O’Reilly, *Homeland Security to Compile Database of Journalists, Bloggers*, Bloomberg Big Law Business (Apr. 5, 2018), <https://biglawbusiness.com/homeland-security-to-compile-database-of-journalists-bloggers/>; Press Release, PEN America, Department of Homeland Security’s Plants for Journalists Database Must Be Quashed Immediately (Apr. 8, 2018), <https://pen.org/press-release/dhs-journalist-database-must-be-quashed/>.

²⁶ Tyler Q. Houlton (@SpoxDHS), Twitter (Apr. 6, 2018), <https://twitter.com/SpoxDHS/status/982372727309963264>

²⁷ *About EPIC*, EPIC.org, <http://epic.org/epic/about.html>.

Conclusion

Thank you for your consideration of this request. I anticipate your determination on our request within ten calendar days. 5 U.S.C. § 552(a)(6)(E)(ii)(I). For questions regarding this request I can be contacted at 202-483-1140 x104 or Zhou@epic.org, cc: FOIA@epic.org.

Respectfully submitted,

/s Enid Zhou

Enid Zhou

EPIC Open Government Fellow

/s John Davisson

John Davisson

EPIC Counsel