April 5, 2019

Neven F. Stipanovic, Esq.
Acting Associate General Counsel
1050 First Street, NE
Washington DC 20463

RE: Comment on Advisory Opinion Request 2018-12 (Defending Digital Campaigns), Draft A

Dear Mr. Stipanovic,

In Campaign Legal Center's comment on Advisory Opinion Request 2018-11 (Microsoft) (Sep. 6, 2018), CLC addressed the issue of campaign cybersecurity:

> Given the Commission's broad mandate to prevent foreign interference in elections, the most appropriate method of addressing [cybersecurity services] might be for the Commission to consider whether FECA provides it the authority to adopt regulations specifically addressing campaigns' receipt of services necessary to defend against foreign attacks.
>
> If the Commission nonetheless adopts an advisory opinion approving [the services], rather than by engaging in a tortured effort to justify the provision of such services for commercial purposes, *the Commission should transparently and forthrightly state that it is doing so to implement FECA's ban on foreign participation in elections, 52 U.S.C. § 30121, and that the opinion is limited only to services that are necessary to directly further that ban*.

See also Advisory Opinion Request 2018-12 (Defending Digital Campaigns), Comment of Campaign Legal Center (Oct. 11, 2018) (citing comment on AOR 2018-11).

This issue is once again before the Commission. Accordingly, CLC respectfully submits the attached proposed response to Advisory Opinion Request 2018-12 (Defending Digital Campaigns). This response would analyze DDC's planned activity under section 30121.

CLC has conferred with counsel for DDC, who have asked us to inform the Commission that DDC supports adoption of this response.

Sincerely,

/s/ Adav Noti
Adav Noti
Senior Director, Trial Litigation

/s/ Brendan Fischer
Brendan Fischer
Director, Federal Reform Program

We are responding to your advisory opinion request on behalf of Defending Digital Campaigns, Inc. ("DDC"), concerning the application of the Federal Election Campaign Act, 52 U.S.C. §§ 30101-45 (the "Act"), and Commission regulations to DDC's proposal to provide cybersecurity to federal candidate committees and national party committees. Because of the demonstrated, currently enhanced threat of foreign cyberattacks against party and candidate committees, the Commission concludes that DDC's proposal as described in the request would be a lawful means of ensuring compliance with the Act's prohibition on spending by foreign nationals in connection with elections, 52 U.S.C. § 30121.

Background

The facts presented in this advisory opinion are based on your letter received on September 6, 2018.

DDC is recognized as a nonprofit corporation under Washington, D.C. law and is exempt from federal income tax under Section 501(c)(4) of the Internal Revenue Code. Advisory Opinion Request at AOR005, AOR017. According to its articles of incorporation, DDC's purpose is "to provide education and research for civic institutions on cybersecurity best practices and assist them in implementing technologies, processes, resources, and solutions for enhancing cybersecurity and resilience to hostile cyber acts targeting the domestic democratic process." AOR017. Consistent with this purpose, DDC proposes to provide federal candidates and parties with a "set of campaign-tailored resources and training" necessary to combat these cyberattacks, and to develop "channels for information sharing among committees, technology providers, and cybersecurity experts in the public and private sectors." AOR002. DDC intends to do so on a nonpartisan basis according to neutral, objective criteria, as described below, and "not to benefit any one campaign or political party over another or to otherwise influence any federal election," but to further its mission to "help safeguard American elections from foreign interference." *Id*.

I. Threat to Campaigns and Political Parties

You note that, in 2008, hackers "stole large quantities of information" from both then-Senator Obama's and then-Senator McCain's presidential campaigns, and in 2012 the networks and websites of both then-President Obama's and Mitt Romney's presidential campaigns were hacked. AOR002.[1] In 2016, hackers infiltrated the email accounts of Democratic campaign staff, stealing and leaking tens of thousands of emails. AOR002-AOR003.[2] Similar threats have been reported in the current campaign cycle; for example, you state that this year at least four

[1] *See also* Michael Isikoff, *Chinese Hacked Obama, McCain Campaigns, Took Internal Documents, Officials Say*, NBC News (June 10, 2013), http://investigations.nbcnews.com/_news/2013/06/06/18807056-chinese-hacked-obama-mccain-campaigns-took-internal-documents-officials-say.

[2] *See also* Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, Jan. 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

congressional candidates have reported hacking attempts,[3] and Microsoft has indicated that it has detected and blocked hacking attempts against three congressional campaigns. AOR003.[4]

According to your request, federal candidates and parties are singularly ill-equipped to counteract these threats. AOR004. You state that there is no "streamlined, nonpartisan clearinghouse" to help such committees detect and coordinate responses to new threats and outbreaks. AOR002, AOR007. Moreover, you state that presidential campaign committees and national party committees require expert guidance on cybersecurity and you contend that the "vast majority of campaigns" cannot afford full-time cybersecurity staff and that "even basic cybersecurity consulting software and services" can overextend the budgets of most congressional campaigns. AOR004. For instance, you note that a congressional candidate in California reported a breach to the Federal Bureau of Investigation ("FBI") in March of this year but did not have the resources to hire a professional cybersecurity firm to investigate the attack, or to replace infected computers. AOR003.

Accordingly, you believe that "[o]ngoing attempts by foreign powers to undermine our democratic process through cyber and information operations pose a novel and unprecedented threat to the integrity of our electoral system." AOR001.

II. Development and Structure of DDC

Following the 2016 elections, the Belfer Center for Science and International Affairs at Harvard Kennedy School instituted the Defending Digital Democracy Project, co-led by former campaign managers of Republican and Democratic presidential campaigns and cyber and national security experts to "recommend strategies, tools, and technology to protect democratic processes and systems from cyber and information attacks." AOR004. The bipartisan group produced a report, "The Cybersecurity Campaign Playbook," designed to provide campaigns with simple, actionable guidance to secure their systems. *Id*. That report noted many limitations in providing campaigns adequate support — campaigns are inherently temporary and transient, and lack the time and money to develop long-term, well-tested security strategies, to train large numbers of new staff, and to buy non-personal hardware and malware. *Id*. Thus, according to

---

[3] *See also* Joel Schectman & Christopher Bing, *Exclusive: FBI Probing Cyber Attack on Congressional Campaign in California*, Reuters (Aug. 17, 2018), https://www.reuters.com/article/us-usa-election-hacking-exclusive/exclusive-fbi-probing-cyber-attack-on-congressional-campaign-in-california-sources-idUSKBN1L22BZ; Mark Morales, *Democrat Who Challenged GOP Congressman Said He Was Hacked*, CNN (Aug. 15, 2018), https://www.cnn.com/2018/08/15/politics/dana-rohrabacher-opponent-cyberattack-hack/index.html; Holley Long, *Campaign: Russians Attempted to Hack AL Congressional Candidate's Website*, WFSA-12 (July 19, 2018), http://www.wsfa.com/story/38688628/campaign-russians-attempted-to-hack-al-congressional-candidates-website/; Miles Parks, *Senate Campaign in Tennessee Fears Hack After Impostor's Emails Request Money*, NPR (Mar. 8, 2018), https://www.npr.org/2018/03/08/592028416/senate-campaign-in-tennessee-fears-hack-after-imposter-emails-request-money.

[4] *See also* Eric Geller, *Microsoft Reveals First Known Midterm Campaign Hacking Attempts*, Politico (July 19, 2018), https://www.politico.com/story/2018/07/19/midterm-campaign-hacking-microsoft-733256; Advisory Opinion 2018-11 (Microsoft) (concluding that Microsoft may offer enhanced security services to election-sensitive clients under certain circumstances).

the request, "campaigns are in need of more direct, hands-on assistance to address cybersecurity threats." *Id*.

To that end, Defending Digital Democracy Project's founding members formed DDC with two aims in mind: to create secure, nonpartisan forums for sharing information among and between campaigns, political parties, technology providers, law enforcement, and other government agencies to detect cyber threats and facilitate effective responses to those threats; and to provide campaigns and political parties with knowledge, training, and resources to defend themselves from cyber threats. AOOR005. You describe DDC as "truly nonpartisan." *Id*. DDC's articles of incorporation vest the powers of the corporation in a board of directors — initially comprising Democrat Robby Mook, Republican Matt Rhoades, and Deborah Plunkett, the former Director of Information Assurance at the National Security Administration and member of the National Security Council in both Democratic and Republican Administrations — who must be elected from time to time in the manner prescribed in DDC's bylaws. AOR005, AOR017 (articles of incorporation), AOR028 (bylaws). The bylaws provide that the board of directors must be advised by a committee of professionals who are knowledgeable about cybersecurity and election processes, and must elect a president and treasurer to manage day-to-day operations of the corporation. AOR030.

Though DDC is recognized as a social welfare organization under Section 501(c)(4) of the Internal Revenue Code, its articles of incorporation and bylaws provide that DDC "shall not participate in, or intervene in (including the publishing or distribution of statements concerning), any political campaign on behalf of (or in opposition to) any candidate for public office within the meaning of Section 501(c)(3) of the [Internal Revenue] Code." AOR005, AOR018 (articles of incorporation), AOR028 (bylaws). The articles of incorporation and bylaws also provide that DDC's directors, officers, and staff may not personally profit from DDC's activities except for board-approved reasonable compensation for officers and employees, determined by recognized procedures and best practices of similarly situated organizations. AOR005, AOR018 (articles of incorporation), AOR030 (bylaws), AOR046-47 (compensation review policy).

III. DDC's Proposal

DDC proposes to offer free or reduced-cost cybersecurity, as described in the request, to federal candidates and parties according to a pre-determined set of criteria. DDC proposes to make that cybersecurity available to all active, registered national party committees[5] and active, registered federal candidate committees satisfying one of the following requirements:

[5] Currently, there are 11 national party committees registered with the Commission: the Constitution Party National Committee (C00279802), DNC Services Corp./Democratic National Committee (C00010603), DCCC (C00000935), DSCC (C00042366), Green Party of the United States (C00370221), Green Senatorial Campaign Committee (C00428664), Libertarian National Committee, Inc. (C00255695), Libertarian National Congressional Committee Inc. (C00418103), Republican National Committee (C00003418), NRCC (C00075820), and NRSC (C00027466).

- A House candidate's committee that has at least $50,000 in receipts for the current election cycle, and a Senate candidate's committee that has at least $100,000 in receipts for the current election cycle;
- A House or Senate candidate's committee for candidates who have qualified for the general election ballot in their respective elections; or
- Any presidential candidate's committee whose candidate is polling above five percent in national polls. AOR006.

You state that DDC has chosen these criteria to ensure that the federal candidates and parties most likely to be targeted for cyberattacks have access to DDC's services "on a fair and equal basis." *Id*. DDC "will proactively reach out to the Eligible Committees in a consistent manner and offer the same suite of services to all Eligible Committees in a given race." *Id*.

Question Presented

Would DDC's proposed activity be consistent with the Act and Commission regulations?

Legal Analysis and Conclusions

Yes, in light of the demonstrated, currently enhanced threat of foreign cyberattacks against party and candidate committees, DDC's proposed activity would be a lawful means of ensuring compliance with 52 U.S.C. § 30121.

The Act and Commission regulations prohibit foreign nationals from making donations or disbursements in connection with federal, state, and local elections. *See* 52 U.S.C. § 30121(a)(1); 11 C.F.R. § 110.20. This prohibition is intended to "exclude foreign citizens from activities intimately related to the process of democratic self-government." *See Bluman v. FEC*, 800 F. Supp. 2d 281, 287 (D.D.C. 2011) (internal quotations omitted), *aff'd mem.*, 132 S. Ct. 1087 (2012). Such exclusion "is part of the sovereign's *obligation* to preserve the basic conception of a political community." *Id*. (emphasis added).

As the request correctly notes, recent election cycles have seen actual and attempted foreign cyberattacks on party and candidate committees on an unprecedented scale.[6] All of these foreign cyberattacks necessarily entail disbursements by foreign nationals in connection with

[6] *See* Eric Lipton, David E. Sanger, & Scott Shane, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html; OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT U.S. ELECTIONS 5 (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf; Eric Lipton & Scott Shane, *Democratic House Candidates Were Also Targets of Russian Hacking*, N.Y. TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/us/politics/house-democrats-hacking-dccc.html; Nicole Perlroth, *DNC Says It Was Targeted Again by Russian Hackers After '18 Election*, N.Y. TIMES (Jan. 18, 2019), https://www.nytimes.com/2019/01/18/technology/dnc-russian-hacking.html; Ellen Nakashima & Shane Harris, *National Republican Congressional Committee says it was hacked during this year's election cycle*, N.Y. TIMES (Dec. 4, 2018), https://www.washingtonpost.com/world/national-security/national-republican-congressional-committee-says-it-was-hacked-during-this-years-election-cycle/2018/12/04/58136c7a-f7e9-11e8-8d64-4e79db33382f_story.html; AOR001 ("Ongoing attempts by foreign powers to undermine our democratic processes though cyber and information operations pose a novel and unprecedented threat to the integrity of our electoral system.").

American elections, and they are therefore by definition violations of section 30121. But the nature of the cyberattacks — i.e., foreign government agents acting abroad, sometimes without any spending or physical presence in the United States — presents unique challenges to prosecution of the violators under the Commission's enforcement procedures.[7] Thus, the Commission recognizes that fulfilling its "obligation to preserve the basic conception of a political community" under section 30121 cannot hinge solely on prosecution of foreign violators abroad. Effective enforcement of that provision to protect American elections from urgent cyberthreats also requires measures that relate to conduct within the United States.

In other contexts, the Commission has noted that certain carefully defined and limited actions can lawfully be taken under the Act to address urgent circumstances presenting a verified, heightened risk of physical or malicious digital harm. *See* Advisory Opinion 2018-15 (Wyden); Advisory Opinion 2017-07 (Sergeant at Arms).

Here, the Commission concludes that the confluence of these two highly unusual circumstances — i.e., the combination of foreign activity that violates section 30121 but is not realistically subject to direct Commission enforcement, along with the demonstrated, currently enhanced threat of such activity targeting party and candidate committees — renders DDC's proposed activity a lawful means of implementing and enforcing section 30121.

The Commission emphasizes that, to fall within the reasoning and scope of this opinion, the activities conducted must also conform to all of the conditions set forth in the request, including the eligibility criteria (AOR006), and those activities must consist solely and exclusively of cybersecurity. For example, although the request refers to "cybersecurity-*related*" software, hardware, and services, only software, hardware, and services that directly provide cybersecurity, or which are inextricably related to cybersecurity (e.g., office suites, secure messaging platforms) are within the scope of this opinion — not software, hardware, and services that are merely "related" to cybersecurity. Similarly, DDC may not defray expenses that committees would have incurred regardless of cybersecurity efforts, such as expenses for computers; only the securing of such computers against digital intrusion is within the scope of this opinion.

Finally, the Commission notes that any material change to the external threat environment as judged by national security experts would affect the continuing applicability of this opinion. *See* 52 U.S.C. § 30108. That environment includes but is not limited to: (1) the demonstrated, enhanced threat of foreign cyberattacks against party and candidate committees; and (2) the widespread technical inability of candidate committees to protect themselves against foreign cyberattacks. In particular, if Congress were to amend the Act to address the provision of cybersecurity to party or candidate committees by government or non-government entities,

---

[7] *See, e.g.*, Indictment, *United States v. Netyksho*, Crim. No. 18-215 (D.D.C. Jul. 13, 2018), https://www.justice.gov/file/1080281/download (indicting Russian agents in absentia for, among other things, hacking party and campaign committees); *see also* Mark Mazetti & Katie Benner, *12 Russian Agents Indicted in Mueller Investigation*, N.Y. TIMES (Jul. 13, 2018), https://www.nytimes.com/2018/07/13/us/politics/mueller-indictment-russian-intelligence-hacking.html. This activity therefore differs from foreign national activity that involves disbursements to or through U.S. entities and so might realistically be subject to enforcement.

this opinion would not apply to cybersecurity that committees are able to obtain in practice from those government or non-government entities pursuant to such legislation.

The Commission expresses no view as to the applicability of the Internal Revenue Code to the activity described in the request.

This response constitutes an advisory opinion concerning the application of the Act and Commission regulations to the specific transaction or activity set forth in your request. *See* 52 U.S.C. § 30108. The Commission emphasizes that, if there is a change in any of the facts or assumptions presented, and such facts or assumptions are material to a conclusion presented in this advisory opinion, then the requestor may not rely on that conclusion as support for its proposed activity. Any person involved in any specific transaction or activity which is indistinguishable in all its material aspects from the transaction or activity with respect to which this advisory opinion is rendered may rely on this advisory opinion. *See* 52 U.S.C. § 30108(c)(1)(B). Please note that the analysis or conclusions in this advisory opinion may be affected by subsequent developments in the law including, but not limited to, statutes, regulations, advisory opinions, and case law. Any advisory opinions cited herein are available on the Commission's website.