FEDERAL ELECTION COMMISSION
Washington, DC 20463

May 21, 2019

CERTIFIED MAIL
RETURN RECEIPT REQUESTED

ADVISORY OPINION 2018-12

Marc E. Elias, Esq.
Perkins Coie LLP
700 13th Street, NW, #600
Washington, DC 20005

Michael E. Toner, Esq.
Wiley Rein LLP
1776 K Street, NW
Washington, DC 20006

Dear Messrs. Elias and Toner:

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. Under the unusual and exigent circumstances presented by your request and because of the demonstrated, currently enhanced threat of foreign cyberattacks against party and candidate committees, the Commission concludes that DDC may provide the services described in the request, in its comment, and at the Commission meeting of April 11, 2019, to eligible committees free of charge or at reduced charge, subject to the restrictions below.

Background

The facts presented in this advisory opinion are based on your letter received on September 6, 2018, discussions between FEC staff and counsel to DDC, your comment dated April 5, 2019, and information conveyed at the Commission meeting of April 11, 2019.

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*. DDC also plans to offer its services to "think tanks" and other public policy-focused non-governmental organizations ("NGOs"), such as the Truman Center for National Policy and the Hudson Institute. DDC Comment (April 5, 2019) at 3.

In a public meeting of the Commission on April 11, 2019, counsel for and principals of DDC represented that the only donors they have considered so far to fund this project with monetary donations are individuals (except foreign nationals) and foundations. In a subsequent comment, DDC's counsel indicated that DDC may, at some future point, consider accepting monetary donations from sources other than individuals and foundations.[1] DDC plans to disclose its donors with respect to the proposed activities.[2]

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.[3] In 2016, hackers infiltrated the email accounts of Democratic campaign staff, stealing and leaking tens of thousands of emails. AOR002-AOR003.[4] Similar threats have continued since the 2016 elections; for example, you state that at least four congressional

---

[1] *See* Comment from Requestor (May 6, 2019), https://www.fec.gov/files/legal/aos/2018-12/201812C_4.pdf. Requestor's counsel also pointed out that, as explained further below, DDC's proposed cybersecurity activities necessarily involve working with business entities, and thus DDC will be accepting in-kind contributions from such business entities. *Id*.

[2] *See id*.

[3] *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.

[4] *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.

candidates have reported hacking attempts,[5] and Microsoft has indicated that it has detected and blocked hacking attempts against three congressional campaigns. AOR003.[6]

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

---

[5] *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.

[6] *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 services, including facilitating the provision of free or reduced-cost cybersecurity software and hardware from technology corporations, to federal candidates and parties according to a pre-determined set of criteria.

A. Proposed Eligibility Criteria

DDC proposes to make its services available to all active, registered national party committees[7] and active, registered federal candidate committees satisfying one of the following requirements (collectively, "Eligible Committees"):

[7] 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

- 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*. DDC also plans to work with public-policy focused NGOs that "play an important role in our democratic process because they often shape the public policy discussion among candidates and political parties at all levels of government." DDC Comment (April 5, 2019) at 3.

B. Proposed Activities

You state that DDC's potential offerings are under development and will depend on funding, negotiations, and the Commission's guidance, but that DDC proposes to engage in a variety of activities, as explained below.

i. Information Sharing

DDC proposes to create "information sharing systems," such as listservs and bulletins, to allow campaigns, political parties, government agencies, and private sector entities to anonymously share information on malicious email addresses, IP addresses, and other intelligence on cyber threats targeting campaigns and elections. AOR007. DDC may also collaborate with the FBI, Department of Homeland Security ("DHS"), and other law enforcement agencies in this effort. *Id*. As you explain in the request, DHS has expressly identified the need for what it refers to as "Information Sharing and Analysis Organizations (ISAOs)" to allow organizations "to be able to share and respond to cyber risks in as close to real-time as possible." *Id*.[8] You state that DDC would operate as an ISAO, serving as a "streamlined, nonpartisan clearinghouse" to pool and monitor intelligence about cyber threats on

Committee (C00428664), Libertarian National Committee, Inc. (C00255695), Libertarian National Congressional Committee Inc. (C00418103), Republican National Committee (C00003418), NRCC (C00075820), and NRSC (C00027466).

[8] *See* U.S Dep't of Homeland Security, Information Sharing and Analysis Organizations (ISAOs), https://www.dhs.gov/isao.

an anonymous basis, facilitate cooperation with the appropriate government agencies, and provide advice and assistance in the case of a breach. *Id*.

For this service, DDC would not charge the private sector entities, government agencies, or Eligible Committees. AOR007.

ii. Cybersecurity Hotline

DDC also intends to operate a cybersecurity hotline, at no charge, for Eligible Committees. AOR007. The hotline would allow Eligible Committees to receive advice or coaching, and to identify new and emergency cybersecurity threats in order to notify the proper government agencies if necessary. *Id*.

iii. Cybersecurity "Bootcamps," Advanced Training, and Certification Courses

DDC plans to offer free cybersecurity "bootcamps" — trainings covering core cybersecurity issues — as well as free "advanced cybersecurity training and certification courses" to Eligible Committees' leadership and information technology staff. AOR008. DDC may host these programs at central locations and provide free or discounted transportation and lodging for Eligible Committees' staff to attend. *Id*. Moreover, DDC may recruit cybersecurity professionals to speak at such trainings as volunteers, and contract with cybersecurity firms to provide advanced training and certification courses. *Id*

iv. On-Site Training and Assistance

In addition to the above training for Eligible Committees' leadership and information technology staff, DDC believes it "vital" to ensure that all employees receive basic cybersecurity training, and notes that Eligible Committees may need advice on implementing cybersecurity practices into their unique infrastructure. AOR008. Thus, DDC would like to "facilitate" free on-site visits to Eligible Committees by cybersecurity professionals who would provide basic training or general assistance. *Id*. Under one option, cybersecurity professionals would provide such training and assistance as volunteers while on unpaid leave or while on paid leave under their employers' existing policies. *Id*. Under another option, DDC would "establish partnerships" with cybersecurity firms that would agree to provide paid leave to their employees for the on-site training and assistance. *Id*.

v. Cybersecurity Incident Response and Monitoring Services

DDC also plans to form retainer agreements with digital security vendors to provide free or reduced-cost incident response services by digital security firms, allowing the Eligible Committees to contact such vendors during threatening cyber events, including phishing attacks and the receipt of suspicious emails. AOR008. DDC would also like to form similar agreements with brand monitoring services, which identify fake websites that imitate legitimate federal

candidates or parties, monitor the internet for fraudulent or unauthorized committees posing as Eligible Committees, and notify the Eligible Committees in the event of harmful behavior. *Id*.

vi. Free or Reduced-Cost Cybersecurity-related Software and Hardware

Under another proposed service, DDC would partner with technology companies (such as Google and Microsoft) to customize those companies' existing software for federal candidates and parties in order to enhance their cybersecurity, and also "negotiate partnerships" with those companies to secure free or discounted licenses for both customized and non-customized cybersecurity-related software for Eligible Committees. AOR009. DDC would "act as an intermediary" between the software providers and Eligible Committees "to ensure that licenses are provided on a fair and equal basis to all Eligible Committees," but the actual software license agreements would be between the providers and the Eligible Committees. *Id*. DDC staff would assist Eligible Committees in installing the software and educating staff on the proper use of the software. *Id*. Likewise, DDC would provide similar services acting as an intermediary in contracts between providers and Eligible Committees for cybersecurity-related hardware. *Id*.

Question Presented

May DDC provide the described services to Eligible Committees free of charge or at reduced charge?

Legal Analysis and Conclusions

Under the unusual and exigent circumstances presented by your request and in light of the demonstrated, currently enhanced threat of foreign cyberattacks against party and candidate committees, the Commission approves DDC's proposed activity.

The Act and Commission regulations prohibit foreign nationals from making contributions, expenditures, 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.*, 565 U.S. 1104 (2012). Such exclusion "is part of the sovereign's *obligation* to preserve the basic conception of a political community." *Id*. (emphasis added).

The Commission has approved certain advisory opinion requests to take particular, carefully defined, and limited actions 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, we have such circumstances. The Commission concludes that the current threat of foreign cyberattacks presents unique challenges to Commission enforcement of section 30121, and that this highly unusual and serious threat militates in favor of granting DDC's request.

The request notes that recent election cycles have seen actual and attempted foreign cyberattacks on party and candidate committees on an unprecedented scale.[9] Foreign cyberattacks that entail disbursements by foreign nationals in connection with American elections are violations of section 30121. But foreign cyberattacks, in which the attackers may not have any spending or physical presence in the United States, may present unique challenges to both criminal prosecution and civil enforcement.[10] 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 that countermeasures be taken within the United States.

DDC's proposal is a unique response to such threats. DDC proposes to offer free or reduced-cost cybersecurity services, including facilitating the provision of free or reduced-cost cybersecurity software and hardware from technology corporations, to federal candidates and parties according to a pre-determined set of criteria. DDC is formed in a bi-partisan fashion, co-led by former campaign managers of Republican and Democratic presidential campaigns. AOR004. DDC proposes to make its services available on a nonpartisan basis and "not to benefit any one campaign or political party over another or to otherwise influence any federal election." AOR002. DDC plans to offer its services not only to political committees, but also to "think tanks" and other public policy-focused NGOs. DDC Comment (April 5, 2019) at 3. DDC, a 501(c)(4) organization which its counsels represented will operate like a 501(c)(3), would not be prevented from accepting donations from foreign nationals because of its tax status. However, because this advisory opinion is premised on the threat of foreign cyberattacks against party and candidate committees and the implications those attacks have on Commission enforcement of section 30121, the Commission's approval is conditioned on DDC's commitment not to accept any donations from foreign nationals, and its adherence to the representations described above.

Approval is conditioned on DDC's public disclosure of all donations and, going forward, disclosure of new donations by the first day of the month following when they were received;[11]

---

[9] 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; 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.").

[10] *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.

[11] These disclosures shall appear prominently on DDC's website and shall include: (a) the true source of the funds as required of contributions by 11 C.F.R. §110.4, and (b) the categories of information required for contributions to authorized committees of candidates for Federal office found in 11 C.F.R. §104.3(a)(3).

and its commitment to accept donations only from individuals, foundations, and entities that have elected C corporation status for federal income-tax purposes.[12]

This opinion is limited to the circumstances presented in the request, including the eligibility criteria (AOR006), and extends solely to the described cybersecurity activities. 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 decline in the external threat environment — as judged, for example, by the U.S. Intelligence Community or U.S. national security officials — 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, 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,

[12] Vice Chairman Petersen and Commissioner Hunter approve this Advisory Opinion, but do not condition their approval on these disclosure requirements and funding restrictions.

regulations, advisory opinions, and case law. Any advisory opinions cited herein are available on the Commission's website.

On behalf of the Commission,

Ellen L. Weintraub
Chair