RECEIVED
By Office of the Commission Secretary at 5:17 pm, Oct 09, 2018

FEDERAL ELECTION COMMISSION
Washington, DC 20463

AGENDA DOCUMENT NO. 18-43-A
AGENDA ITEM
For meeting of October 11, 2018
SUBMITTED LATE

MEMORANDUM

TO: The Commission

FROM: Lisa J. Stevenson LJS
Acting General Counsel

Neven F. Stipanovic NFS
Acting Associate General Counsel

Robert M. Knop RMK by NFS
Assistant General Counsel

Joseph P. Wenzinger JPW
Attorney

Subject: AO 2018-12 (Defending Digital Campaigns, Inc.) Draft A

Attached is a proposed draft of the subject advisory opinion.

Members of the public may submit written comments on the draft advisory opinion. We are making this draft available for comment until 9:00 am (Eastern Time) on October 11, 2018.

Members of the public may also attend the Commission meeting at which the draft will be considered. The advisory opinion requestor may appear before the Commission at this meeting to answer questions.

For more information about how to submit comments or attend the Commission meeting, go to https://www.fec.gov/legal-resources/advisory-opinions-process/

Attachment

ADVISORY OPINION 2018-12

Marc E. Elias, Esq. **DRAFT A**
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 its proposal to provide or facilitate the provision of certain cybersecurity services, software, and hardware for free or at a reduced cost to federal candidate committees and national party committees (collectively, "federal candidates and parties") on a nonpartisan basis and according to pre-determined, objective criteria. Because the provision of the cybersecurity services, software, and hardware described in the request would not be made for the purpose of influencing or in connection with a federal election, the Commission concludes that DDC's proposal is permissible.

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.

---

[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).

Accordingly, you believe that "[o]ngoing 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." 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 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 cybersecurity services, software, and hardware 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[5] and active, registered federal candidate committees satisfying one of the following requirements (collectively, "Eligible Committees"):

- 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.*

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.

[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).

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.*[6] You state that DDC would operate as an ISAO, serving as a "streamlined, nonpartisan clearinghouse" to pool and monitor intelligence about cyber threats on 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.*

---

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

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.*

Questions Presented

1. *May DDC allow Eligible Committees to participate in the following DDC activities without making in-kind contributions to participating Eligible Committees:*

a. DDC's free cybersecurity information-sharing forums; and

b. DDC's free cybersecurity hotline?

2. May DDC provide cybersecurity bootcamps, advanced training sessions, and certification courses without charge to Eligible Committees without making in-kind contributions to such Eligible Committees?

3. May DDC entirely or partially pay for the transportation and lodging expenses of Eligible Committees' staff to attend DDC's cybersecurity bootcamps, advanced trainings, or certification courses without making in-kind contributions to such Eligible Committees?

4. May DDC coordinate on-site cybersecurity training and assistance for Eligible Committees without making in-kind contributions to Eligible Committees when such training and assistance is provided by:

a. Cybersecurity professionals employed by cybersecurity firms with whom DDC has a partnership and who have agreed to provide paid leave to employees to conduct such on-site training and assistance; or

b. Cybersecurity professionals who are acting in a volunteer capacity?

5. May DDC provide cybersecurity incident response services and brand monitoring services to Eligible Committees free of charge or at a reduced cost without making in-kind contributions to such Eligible Committees?

6. May DDC facilitate the provision of free or discounted cybersecurity-related software licenses or hardware from private sector companies to Eligible Committees without DDC

or the private sector companies making in-kind contributions to Eligible Committees receiving such software licenses or hardware?

7. *May DDC assist Eligible Committees with installing and using the software licenses or hardware without making in-kind contributions to such Eligible Committees?*

Legal Analysis and Conclusions

Yes, DDC may engage in the activities described in the request without making any in-kind contributions to the Eligible Committees, or facilitating the making of any such in-kind contributions by DDC's corporate sponsors or other partners in the private sector, because the provision of the cybersecurity services, software, and hardware would not be made for the purpose of influencing or in connection with a federal election.

The Act and Commission regulations prohibit corporations from making contributions, or facilitating the making of contributions, to federal candidates, political parties, and political committees that make contributions to federal candidates and political parties. 52 U.S.C. §§ 30118(a), (b)(2); 11 C.F.R. §§ 114.2(b), (f).[7] A "contribution" includes anything of value made for the purpose of influencing a federal election, and in the context of contributions by corporations also includes any "direct or indirect payment, distribution, loan, advance, deposit, or gift of money, or any services, or anything of value . . . in connection with any [federal] election . . . ." 52 U.S.C.§ 30118(b)(2); *see also id.* § 30101(8)(A)(i); 11 C.F.R. § 114.2(b).

[7] Corporations may, however, make contributions to nonconnected political committees that make only independent expenditures, *see, e.g.*, Advisory Opinion 2011-11 (Colbert); *Citizens United v. FEC*, 558 U.S. 310 (2010); *SpeechNow.org v. FEC*, 599 F.3d 686 (D.C. Cir. 2010) (*en banc*), and to non-contribution accounts of hybrid political committees, *see* Press Release, FEC Statement on *Carey v. FEC*: Reporting Guidance for Political Committees that Maintain a Non-Contribution Account (Oct. 5, 2011), https://www fec.gov/updates/fec-statement-on-carey-v-fec/.

"Anything of value" includes all in-kind contributions, such as the provision of goods and services without charge or at a charge that is less than the usual and normal charge. *See* 11 C.F.R. § 100.52(d)(1).

In Advisory Opinion 2000-16 (Third Millennium), the Commission approved a proposal by a nonprofit corporation to pay for several internet advertisements supporting various presidential candidates for the purpose of gathering survey data to enable it to determine how to "encourage participation in the electoral and legislative processes by younger Americans." *See* Advisory Opinion 2000-16 (Third Millennium) at 1, 5. The stated purpose of the corporation was to "examine and address the problem of young voter disengagement from the political process and the threat this disengagement poses to democracy at large." *Id*. at 1-2. Four Commissioners concluded that the corporation's proposed activities would not be for the purpose of influencing an election and therefore did not constitute a contribution.[8] In separate statements, all six Commissioners also found significant the nonpartisan nature of the organization and its proposed activities, and the fact that the organization was exempt from federal income tax under Section 501(c)(3) of the Internal Revenue Code, which "prohibited [it] from participating or intervening in any political campaign on behalf of or in opposition to any candidate for public office." *Id*. at 1.[9]

[8] Concurrence in Advisory Opinion 2000-16, Commissioner Sandstrom at 2-3, Advisory Opinion 2000-16 (Third Millennium) (Dec. 15, 2000); Concurrence in Advisory Opinion 2000-16, Chairman Wold and Commissioners Mason and Smith at 3-4, Advisory Opinion 2000-16 (Third Millennium) (Aug. 24, 2000). Two Commissioners concluded that, the proposed activities were for the purpose of influencing a federal election, but that they satisfied the exception for nonpartisan activity designed to encourage individuals to vote or register to vote under 52 U.S.C. § 30101(9)(B)(ii). Concurrence in Advisory Opinion 2000-16, Commissioners McDonald and Thomas at 2, Advisory Opinion 2000-16 (Third Millennium) (Aug. 25, 2000).

[9] *See* Concurrence in Advisory Opinion 2000-16, Chairman Wold and Commissioners Mason and Smith at 4, Advisory Opinion 2000-16 (Third Millennium) (Aug. 24, 2000) (stressing the "nonpartisan" purposes of the

More recently, the Commission has concluded that, under certain circumstances, a for-profit technology corporation may provide free cybersecurity services to its "election-sensitive customers," including political committees, on a nonpartisan basis to protect their accounts against security breaches. *See* Advisory Opinion 2018-11 (Microsoft). The Commission reasoned that the provision of such services would not constitute a prohibited corporate contribution because the services would be provided based on commercial and not political considerations, "most notably to protect [the company's] brand reputation, which would be at risk of severe and long-term damage if the accounts of its election-sensitive customers were hacked" given the public scrutiny regarding foreign attempts to influence elections. *Id*. at 2, 4.

Here, DDC was established for the purpose of providing education and research on cybersecurity issues and helping to protect "civic institutions" against "hostile cyber acts targeting the domestic democratic process." AOR017 (articles of incorporation), AOR028 (bylaws). Consistent with this stated purpose, DDC proposes to train the staff of Eligible Committees on "core cybersecurity practices," share information with them on the latest cyber threats uncovered by federal law enforcement agencies and private sector entities, and equip the Eligible Committees with cybersecurity software and hardware in order to protect them against cyberattacks.[10] AOR006-AOR009. DDC would provide these services to all Eligible

proposed activities, "rather than [providing] an opportunity for the candidates to refine, target, or otherwise convey their messages to the electorate"); Concurrence in Advisory Opinion 2000-16, Commissioners McDonald and Thomas at 2, Advisory Opinion 2000-16 (Third Millennium) (Aug. 25, 2000) (applying exemption for nonpartisan activity designed to encourage individuals to vote or register to vote under 52 U.S.C. § 30101(9)(B)(ii)); Concurrence in Advisory Opinion 2000-16, Commissioner Sandstrom at 2, Advisory Opinion 2000-16 (Third Millennium) (Dec. 15, 2000) (concluding that "[n]on-partisan activity — designed to influence the level of participation in an election, rather than its outcome — is . . . not 'for the purpose of influencing any election for [f]ederal office'").

[10] The Commission presumes that any cybersecurity services, software, or hardware DDC provided at a

Committees, according to pre-determined, objective criteria, and not for the benefit of any one campaign or political party over another. AOR006.

Significantly, DDC's organizational structure is designed to ensure its activities remain nonpartisan. Its articles of incorporation and bylaws expressly prohibit DDC from participating in, or intervening in, any political campaign within the meaning of Section 501(c)(3) of the Internal Revenue Code. AOR005, AOR018 (articles of incorporation), AOR028 (bylaws). The current composition of DDC's board of directors, with equal representation of Democratic and Republican members, is carefully balanced to avoid the appearance of partisanship. And further indicative of its nonpartisan structure is the fact that DDC would have to establish an advisory committee composed of experts in cybersecurity that would advise and guide the board on DDC's policies and activities. *See* AOR030 (bylaws).

The Act and Commission regulations recognize that corporations may engage in certain nonpartisan activities without making prohibited in-kind contributions to federal candidates or parties. *See, e.g.*, 52 U.S.C. § 30101(9)(B)(ii) (permitting nonpartisan activity designed to encourage individuals to vote or to register to vote without limitation); 11 C.F.R. §§ 114.4(c)(2) (permitting corporations to make voter registration and get-out-the-vote communications), 114.4(c)(3) (permitting corporations to distribute registration or voting information); 114.4(c)(4) (permitting corporations to distribute voting records), 114.4(c)(5) (permitting corporations to prepare and distribute voter guides), 114.4(c)(6) (permitting corporations to endorse candidates), 114.4(c)(7) (permitting corporations to host candidates for appearances on their premises), 114.4(d) (permitting corporations to make disbursements for voter registration and get-out-the-

reduced cost to Eligible Committees would be provided on the same terms to all Eligible Committees.

vote drives). Notably, Commission regulations expressly permit certain nonprofit organizations under Sections 501(c)(3) and 501(c)(4) of the Internal Revenue Code to stage candidate debates, as long as such organizations do not endorse, support, or oppose political candidates or political parties, and use pre-established objective criteria to determine which candidates may participate in the debate. 11 C.F.R. § 110.13; *see also* Funding and Sponsorship of Federal Candidate Debates, 44 Fed. Reg. 76734, 76735 (Dec. 27, 1979) (concluding that a "debate is nonpartisan if it is for the purpose of educating and informing the voters, provides fair and impartial treatment of candidates, and does not promote or advance one candidate over another"). Although none of these provisions squarely applies here, DDC's purpose and activities are similarly offered on an objective, nonpartisan basis and intended to facilitate the proper functioning of electoral processes rather than to support or oppose any candidate or party.

Finally, as noted above, DDC proposes to make its cybersecurity services, software, and hardware available to federal candidates and parties based on a pre-determined set of criteria including their registration status with the Commission, whether the candidate has qualified for the general election ballot, the level of fundraising activity, or, for presidential candidates, their status in national polls. AOR006. These criteria resemble those that the Commission has determined to be objective, easily determined, and outside of the providing organization's discretion or control, and thus not subject to the Act and Commission regulations. *See* Advisory Opinion 1999-25 (Democracy Network) at 2 (concluding that ballot qualification constitutes an objective criterion for purposes of whether to apply exception to definition of "expenditure" for nonpartisan activities designed to encourage individuals to vote or to register to vote under 52

U.S.C. § 30101(9)(B)(ii)); 11 C.F.R. § 110.13(c) (permitting nonprofit organizations to stage candidate debates based on "pre-established objective criteria").

In sum, the proposed activities would be conducted for the stated purpose of protecting all eligible federal candidates and parties against cyber threats, on a nonpartisan basis and according to pre-determined, objective criteria. Accordingly, the Commission concludes that the proposed activities would not be made for the purpose of influencing or in connection with any federal election. Thus, DDC may engage in the activities described in the request without making any in-kind contribution to the Eligible Committees, and without facilitating the making of any in-kind contribution to Eligible Committees from DDC's corporate sponsors or other private sector partners.[11]

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

[11] You state that "DDC's proposed payments of compensation to staff and fees to third-party cybersecurity professionals and firms would enable the provision of personal services to campaigns and political parties." AOR012. Under 52 U.S.C. § 30101(8)(A)(ii), the definition of "contribution" includes the payment by any person of compensation for the personal services of another person which are rendered to a political committee without charge for any purpose. However, in Advisory Opinion 2015-14 (Hillary for America), the Commission permitted an incorporated university to compensate a student — under a program where the university provided stipends to students to help with their summer internships — whose summer internship involved, among other things, preparing a federal campaign committee's reports to the Commission. *See* Advisory Opinion 2015-14 (Hillary for America) at 3. According to the Commission, the payments of compensation were not for personal services to the political committee but for the purpose of assisting students with an educational experience. *Id*. Here, too, any payments of compensation made by DDC would not be for the personal services offered to campaigns, but to exercise its mission to protect federal elections from foreign interference. Thus, the payments of compensation would not constitute a contribution under 52 U.S.C. § 30101(8)(A)(ii).

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.

On behalf of the Commission,

Caroline C. Hunter
Chair