



NORTH CAROLINA

STATE BOARD OF ELECTIONS

Mailing Address:
P.O. Box 27255,
Raleigh, NC 27611
(919) 814-0700 or
(866) 522-4723
Fax: (919) 715-0135

Counsel to Defending Digital Campaigns, Inc.

Michael E. Toner
Brandis L. Zehr
Hannah Bingham
Wiley Rein LLP
2050 M. Street NW
Washington, DC 20036

Ezra W. Reese
Jonathan A. Peterson
Elias Law Group LLP
250 Massachusetts Avenue NW, Suite 400
Washington, DC 2001

September 21, 2024

Re: Request for an advisory opinion under N.C.G.S. § 163-278.23 regarding contribution limits

Dear Counsel,

We have reviewed your correspondence on behalf of Defending Digital Campaigns, Inc. The following written opinion is provided in accordance with N.C.G.S. § 163-278.23.

In your letter, you shared that Defending Digital Campaigns, Inc (“DDC”) is seeking to expand its cybersecurity program to offer cybersecurity training, services and resources to North Carolina candidates committees and political parties. DDC proposes to make its services free to these entities on a nonpartisan basis.

According to your letter, DDC is an offshoot of the Defending Digital Democracy Project, an initiative of the Belfer Center for Science and International Affairs at Harvard University’s Kennedy School. Advisory Op. Request at 1. DDC is a Section 501(c)(4) nonprofit corporation organized under the provisions of the District of Columbia Business Organization Code. The Articles of Incorporation

make clear that the purpose of the corporation is “to provide education and research for civil 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” Advisory Op. Request Appendix A. While organized and operating as a nonprofit corporation described in Section 501(c)(4) of the Federal Internal Revenue Code, the Articles of Incorporation also state that “the Corporation 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 Code.” *Id.* This means DDC has elected to follow the strident prohibitions on political activity imposed on 501(c)(3) organizations.

DDC would like to offer a series of services to North Carolina candidate committees and political parties, including the following:

- Free or reduced-cost cybersecurity software and hardware through partner technology providers;
- Cybersecurity training covering core cybersecurity issues, and advanced cybersecurity training over time;
- On-site and remote onboarding and training to assist campaigns and political parties in getting cybersecurity products up and running;
- Cybersecurity incident response and monitoring services provided by digital security firms; and
- Information sharing systems allowing political organizations to share information on malicious email addresses, IP addresses, and other intelligence on cyber threats.

Advisory Op. Request at 3-4. To accomplish this, DDC intends to work directly with candidates and political parties to educate leadership and staff about cybersecurity and provide comprehensive cybersecurity training. DDC also works with select corporate partners to negotiate fee or reduced cost cybersecurity services and produces to be provided to campaigns and political parties who participate in DDC’s program.

DDC seeks guidance on whether it may provide these services: (1) to any party committee registered with the State Board of Elections, and (2) to candidates for state or local office who have qualified for the general election ballot in their respective races. DDC plans to proactively reach out to North Carolina campaigns and political parties in a consistent manner and offer the same suite of services to all such committees meeting the eligibility requirements. Advisory Op. Request at 5.

In 2018, DDC submitted a similar letter to the Federal Election Commission (“FEC”) to ask whether DDC may offer its services to eligible federal political committees. On May 21, 2019, the FEC approved DDC’s proposed activity

“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.” FEC, Advisory Op. 2018-12 at p 7. The FEC noted that the United States had experienced “actual and attempted foreign cyberattacks on party and candidate committees on an unprecedented scale” and that “DDC’s proposal is a unique response to such threats.” FEC, Advisory Op. 2018-12 at p 8.

The threat from foreign adversaries still exists today. *See An Update on Foreign Threats to the 2024 Elections: Hearing Before the S. Select Comm. on Intelligence*, 118th Cong. (2024) (Statement by Avril Haines, Director of National Intelligence), <https://www.intelligence.senate.gov/hearings/open-hearing-update-foreign-threats-2024-elections>. Like their federal counterparts, North Carolina political parties and candidates must remain vigilant in an increasingly complex cyber and security environment.

North Carolina law prohibits a candidate or political party from accepting any contribution made by any corporation, foreign or domestic, regardless of whether such corporation does business in the State of North Carolina, or made by any business entity, labor union, professional association, or insurance company. N.C.G.S. § 163-278.15(a).¹

A contribution is:

any advance, conveyance, deposit, distribution, transfer of funds, loan, payment, gift, pledge or subscription of money or anything of value whatsoever, made to, or in coordination with, a candidate to support or oppose the nomination or election of one or more clearly identified candidates, to a political committee, to a political party, to an affiliated party committee, or to a referendum committee, whether or not made in an election year, and any contract, agreement, or other obligation to make a contribution.

N.C.G.S. § 163-278.6(13). A contribution includes non-monetary transfers of goods or services, described as “in-kind contributions.” N.C. Campaign Finance Manual at p. 19 (issued Feb. 2022). In-kind contributions count towards contribution limits and the fair market value of the good or service must be disclosed on the appropriate disclosure report. *Id.* In general, the provision or discount of a service or the provision or discount of a product to a political committee is considered an in-kind contribution. *Id.* at p. 51.

The need for the services provided by the DDC is not driven by normal election activity. Political committees are in the business of “supporting or opposing the election of clearly identified candidates,” N.C.G.S. § 163-278.6(74), and nothing

¹ There is a limited exception for nonprofits that qualify under N.C.G.S. § 163-278.19(h). However, given the history of and potential for corporate contributions to DDC, it does not appear DDC would qualify.

inherent to the purpose of a political committee would typically require that committee to expend resources to defend against threats by malicious foreign actors. It is the current, heightened threat environment, and the fact that foreign actors have targeted political campaigns, that give us all an interest in ensuring political committee are safe from actors who have no role to play in U.S. elections.

In this specific instance, the purpose of DDC and the provision of its services is tailored to the unique and common threat faced by all candidates and parties, regardless of their affiliation. The services provided by DDC and DDC's corporate partners are not services that can be readily purchased on the market by candidates and political committees.

DDC and its corporate partners are offering services that are only relevant to, and only provided to, campaigns and committees – and are provided to all campaigns and committees for free – so there is no usual and normal charge for the services that are being forgone or waived. In short, DDC is making generally and publicly available a service for the purpose of ensuring the integrity of our electoral system, rather than providing free goods and services that would otherwise be paid for by campaigns and political parties.

Advisory Op. Request at p. 8. If anything, these services mirror some of the services the U.S. Cybersecurity and Infrastructure Security Agency (“CISA”) and the U.S. Department of Homeland Security provide to State agencies to make sure our critical election infrastructure is secure from attacks by the same foreign actors. Critically, these services do not serve to support or oppose the nomination or election of any candidate for public office or any political committee's electoral purpose. Instead, these services are designed to ward off illegal foreign intrusion into U.S. political campaigns.

As DDC suggests, what the organization is providing is akin to a publicly available service, and does not reflect something of value provided to a political committee under North Carolina law, so long as DDC adheres to its commitment to offer these services to all qualifying committees, regardless of partisan affiliation and ideology. In this regard, these services are no different from local law enforcement conducting routine patrols by the headquarters of a prominent political campaign to ward off illegal break-ins, vandalism, or other criminal activity. Those police officers in their squad cars are not contributing to that campaign, and neither would this organization when it is helping campaigns protect against malicious cyber activity.

In its opinion, the FEC was clear that the DDC may not defray expenses that committees would have incurred regardless of cybersecurity efforts. FEC, Advisory Op. 2018-12 at p. 9. For example, the DDC may not defray expenses for computers; the organization may only secure the computers against digital intrusion. FEC, Advisory Op. 2018-12 at p. 9. The same standard applies here in

North Carolina. Because many North Carolina campaigns may have smaller budgets than their federal counterparts, it's possible existing hardware and software purchased by the campaign pose security challenges. However, this opinion hinges on the unique nature of the cybersecurity services DDC's offers. While DDC may counsel candidates and party committees on the risk associated with use of certain hardware and software products, DDC's corporate partners cannot defray expenses for hardware or software the committee needs independent of any cybersecurity threat.

FEC approval was also conditioned upon DDC's public disclosure of all donations on the DDC's website. FEC, Advisory Op. 2018-12 at p. 8. As a result, DDC posts all new donors and related information on the first of the month following their contribution: <https://defendcampaigns.org/donors>. It is the State Board's expectation that donations to DDC to further efforts in North Carolina will also be displayed on this website.

The opinion will be filed with the Codifier of Rules to be published in the North Carolina Register.

Sincerely,

A handwritten signature in blue ink that reads "Karen Brinson Bell". The signature is fluid and cursive, with the first name "Karen" being the most prominent.

Karen Brinson Bell
Executive Director
State Board of Elections

Cc: Ashley B. Snyder, Codifier of Rules

December 19, 2023

VIA EMAIL

Karen Brinson Bell
Executive Director
North Carolina State Board of Elections
Dobbs Building, Third Floor
430 North Salisbury Street
Raleigh, NC 27603-1362
Karen.Bell@ncsbe.gov

Re: Advisory Opinion Request

Dear Executive Director Bell:

Defending Digital Campaigns, Inc. (“DDC”), through undersigned counsel, respectfully requests an advisory opinion from the North Carolina State Board of Elections (the “Board”) pursuant to N.C. Gen. Stat. § 163-278.23. DDC is a nonpartisan, Section 501(c)(4) social welfare organization whose mission is to secure our democratic process by providing campaigns and political parties with knowledge, training, and resources to defend themselves from foreign cyber threats. DDC has successfully helped federal campaigns and political parties bolster their cybersecurity since 2019, and seeks confirmation that it may expand its program to include North Carolina campaigns and political parties consistent with North Carolina campaign finance law.

BACKGROUND

I. History and Structure of DDC

DDC is an offshoot of the Defending Digital Democracy Project (“D3P”), an initiative of the Belfer Center for Science and International Affairs at Harvard Kennedy School. D3P, which was launched in the wake of the 2016 election, sought “to develop strategies, tools, and recommendations to protect democratic processes and systems from cyber and information attacks.”¹ Through this initiative, it became apparent to D3P’s founders—who included the former campaign managers for Hillary Clinton and Mitt Romney, as well as leading cybersecurity experts—that most campaigns do not have the expertise or resources to address cybersecurity threats and would benefit from direct, hands-on assistance. D3P’s founders formed DDC as a distinct nonpartisan, non-profit organization to fill this gap and directly engage with campaigns and political parties, providing them with the knowledge, training, and resources to defend themselves from unprecedented foreign cyber threats.²

¹ Harvard Kennedy School, Belfer Center for Science and International Affairs, Defending Digital Democracy Project, <https://www.belfercenter.org/project/defending-digital-democracy> (last visited Dec. 19, 2023).

² See FEC, Adv. Op. Request 2018-12 (Defending Digital Campaigns, Inc.) (attached as Exhibit A) (documenting the history and threat of foreign cyberattacks that political actors face).

Although organized as a Section 501(c)(4) social welfare organization under the Internal Revenue Code, DDC's governing documents demonstrate its nonpartisan focus and mandate that DDC adhere to the Internal Revenue Code's prohibitions on political campaign intervention that apply to Section 501(c)(3) charitable organizations.³ DDC is currently led by cybersecurity expert Michael Kaiser, who serves as President and C.E.O., and a balanced bipartisan board of directors comprised of veteran political operatives and cybersecurity professionals, including a former Director of Information Assurance at the National Security Agency, and former Department of Homeland Security Official.⁴

In 2019, DDC received an advisory opinion from the Federal Election Commission ("FEC") confirming that DDC may permissibly provide free or low-cost cybersecurity goods and services to federal campaigns and political parties without making a contribution or expenditure under federal campaign finance law.⁵ The FEC explained that "[f]oreign cyberattacks that entail disbursements by foreign nationals in connection with American elections are a violation of section 30121," but "present unique challenges to both criminal prosecution and civil enforcement" given that "attackers may not have any spending or physical presence in the United States."⁶ In approving DDC's program, the FEC opined that "[e]ffective enforcement of that provision to protect American elections from urgent cyberthreats also requires that countermeasures be taken within the United States," and "DDC's proposal is a unique response to such threats."⁷ Importantly, the FEC's approval was conditioned on DDC "mak[ing] its services available on a nonpartisan basis" and its commitment "not to benefit any one campaign or political party over another or to otherwise influence any federal election."⁸

DDC's program has been tremendously successful at the federal level. DDC has engaged with more than 500 federal campaigns and national and state political parties, with nearly 200 of those organizations choosing to accept DDC's free and reduced-cost cybersecurity services and products offered through corporate partners in 2020 and 2022. More importantly, however, DDC has helped build a culture of cybersecurity awareness among campaign professionals where best practices are the norm. Political campaigns face threats from nation-states, cybercriminals, and hacktivists making campaigns, and the people associated with them high-risk technology users when it comes to determining best practices for protecting them.

The threat of foreign cyberattacks on American political organizations has not subsided. In the fall of 2020, Microsoft noted that it "ha[d] detected cyberattacks targeting people and organizations involved in the upcoming presidential election, including unsuccessful attacks on people associated with both the Trump and Biden campaigns" and "that foreign activity groups [had] stepped up their efforts targeting the 2020 election as had been anticipated."⁹ Shortly

³ *Id.* at 5.

⁴ DDC, *Who We Are*, <https://defendcampaigns.org/team> (last visited Dec. 19, 2023).

⁵ FEC, Adv. Op. 2018-12 (Defending Digital Campaigns, Inc.) (attached as Exhibit B).

⁶ *Id.* at 8; *see also* 52 U.S.C. § 30121 (prohibiting foreign nationals from making contributions, expenditures, donations, or disbursements in connection with federal, state, and local elections).

⁷ FEC, Adv. Op. 2018-12 at 8.

⁸ *Id.*

⁹ Microsoft, *New Cyberattacks Targeting U.S. Elections* (Sept. 10, 2020), <https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden>.

before the 2020 general election, cybercriminals infiltrated the Republican Party of Wisconsin's email accounts and doctored invoices to facilitate stealing \$2.3 million.¹⁰ The state party's then-chairman noted that the hackers "exhibited a level of familiarity with state party operations at the end of the campaign to commit this crime."¹¹

Leading up to the 2022 general election, the FBI warned Democratic and Republican state political parties that "Chinese government hackers [were] scanning U.S. political party domains ahead of [the] midterm elections, looking for vulnerable systems as a potential precursor to hacking operations."¹² As one cybersecurity expert noted, "[p]olitical parties are excellent sources of intelligence on developing policy and they've been targeted for that purpose by cyberespionage actors for some time, but as foreign election interference has become commonplace, the risk is no longer just quiet spy work . . . intrusions like these can be leveraged in hack-and-leak activity designed to manipulate the democratic process."¹³ Candidates, even at the state level, are also targeted. Earlier this year, malicious actors hacked the Facebook page of a candidate for Kentucky Lieutenant Governor, took over the account, and used it to stream illegal content.¹⁴

In many ways, cyber threats are more acute for state political actors. State campaigns and political parties typically have fewer resources than federal committees and rely extensively on volunteers. State campaigns, particularly those not associated with statewide candidates, may not even have campaign email accounts or a secure way to save and share files. As the FBI observed in 2022, foreign adversaries are particularly interested in state-level politics and state political actors will continue to be targets.

II. DDC's Proposed Activities

Building off its success at the federal level, DDC now seeks to expand its cybersecurity program to the state level and initially plans to do so in ten states, including North Carolina. Specifically, DDC would like to offer its litany of cybersecurity training, services, and resources to campaigns and political parties in North Carolina, which include:

- Free or reduced-cost cybersecurity software and hardware through partner technology providers;
- Cybersecurity training covering core cybersecurity issues, and advanced cybersecurity training over time;

¹⁰ Raphael Satter, *Wisconsin Republican Party Says Hackers Stole \$2.3 Million*, Reuters (Oct. 29, 2020), <https://www.reuters.com/article/us-usa-election-wisconsin/wisconsin-republican-party-says-hackers-stole-2-3-million-idUSKBN27E2GU>.

¹¹ *Id.*

¹² Josh Dawsey, *et al.*, *Chinese Hackers are Scanning State Political Party Headquarters, FBI Says*, Wash. Post (Oct. 17, 2022), <https://www.washingtonpost.com/politics/2022/10/17/chinese-hackers-are-scanning-state-political-party-headquarters-fbi-says>.

¹³ *Id.*

¹⁴ Arianna Sergio, *Candidate for Kentucky Governor Says Running Mate's Facebook Was Hacked, FBI Investigating*, WHAS 11 (Feb. 3, 2023), <https://www.whas11.com/article/news/local/candidate-kentucky-governor-running-mates-facebook-hacked-fbi-investigating/417-6e91e8fa-21ec-4833-954c-a901955e34ad>.

- On-site and remote onboarding and training to assist campaigns and political parties in getting cybersecurity products up and running;
- Cybersecurity incident response and monitoring services provided by digital security firms; and
- Information sharing systems allowing political organizations to share information on malicious email addresses, IP addresses, and other intelligence on cyber threats.

DDC's cybersecurity program currently engages with federal campaigns and political parties in two ways, and DDC would like to expand its program to include North Carolina campaigns and political parties. *First*, DDC works directly with campaigns and political parties to educate leadership and staff about cybersecurity and provide comprehensive cybersecurity training. In 2021, DDC launched its national training program, "Protecting Democracy Through Cybersecurity," which provides an entry-level overview of cybersecurity best practices and advice on how to apply these best practices to political organizations. DDC offers the trainings at regular intervals throughout the election cycle and plans to begin the 2023-24 election cycle training program later this year. DDC staff offer customized onboarding support and cybersecurity trainings for campaigns and political parties, and engage with campaigns and political parties on an individualized basis when they need cybersecurity advice. DDC also facilitates cybersecurity information sharing among campaigns and political parties and with key technology companies.

Second, DDC works with select corporate partners to negotiate free or reduced cost cybersecurity services and products to be provided to campaigns and political parties who participate in DDC's program.¹⁵ For example, DDC currently partners with Google to provide free Titan Security Keys and Yubico to provide free YubiKeys, which are physical security keys used to provide the strongest multi-factor authentication for critical accounts (e.g., email, social media, banking, file sharing). DDC also partners with Cloudflare to provide "Cloudflare for Campaigns," which is a free service package tailored to help political organizations defend their websites from cyberattacks and unauthorized access. DDC also partners with LastPass to provide a password manager, and Amazon Web Services to provide security tools. In addition, DDC encourages campaigns and political parties to take advantage of additional account safeguards that major technology companies offer to high-profile users, such as Google's Advanced Protection Program,¹⁶ Meta's Facebook Protect,¹⁷ Microsoft 365 for Campaigns, and Account Guard.¹⁸

As with federal campaigns and political parties, DDC plans to make its services available to North Carolina campaigns and political parties on a nonpartisan basis and in a manner that would not support or oppose the nomination or election of specific North Carolina candidates. To do so, DDC plans to offer its services to any party committee registered with the State Board of

¹⁵ DDC, Partners, <https://defendcampaigns.org/partners#> (last visited Dec. 19, 2023).

¹⁶ Google, Advanced Protection Program, <https://landing.google.com/advancedprotection> (last visited Dec. 19, 2023).

¹⁷ Meta, Facebook Protect, <https://www.facebook.com/government-nonprofits/blog/facebook-protect> (last visited Dec. 19, 2023).

¹⁸ Microsoft, Microsoft 365 for Campaigns, <https://m365forcampaigns.microsoft.com> (last visited Dec. 19, 2023).

Elections (the “Board”), as well as any campaign committees registered with the Board that satisfy any of the following objective eligibility requirements:

- Candidates for local (municipal and county) office whose campaign committees have raised at least \$2,000 in receipts for the current election cycle;
- Candidates for state legislature whose campaign committees have raised at least \$5,000 in receipts for the current election cycle;
- Candidates for statewide office whose campaign committees have raised at least \$10,000 in receipts for the current election cycle; or
- Candidates for state or local office who have qualified for the general election ballot in their respective races.

DDC has selected these clear, nonpartisan criteria to ensure that campaigns and political parties have access to DDC’s services on a fair and equal basis. DDC also plans to proactively reach out to North Carolina campaigns and political parties in a consistent manner and offer the same suite of services to all such committees meeting the eligibility requirements.

QUESTION PRESENTED

May DDC provide its cybersecurity goods and services, including those offered through DDC’s corporate partners, at no cost or at reduced cost to North Carolina campaigns and political parties without making in-kind contributions to the participating campaigns and political parties?

LEGAL BACKGROUND AND ANALYSIS

As explained below, DDC believes that its proposed activities would not result in an in-kind contribution from DDC or its corporate partners to participating North Carolina campaigns and political parties, because the activities are not for the purpose of supporting or opposing the nomination or election of North Carolina candidates.

I. Legal Background

State law defines a “contribution,” in relevant part, as:

“[A]ny advance, conveyance, deposit, distribution, transfer of funds, loan, payment, gift, pledge or subscription of money or anything of value whatsoever, made to, or in coordination with, a candidate *to support or oppose the nomination or election of one or more clearly identified candidates*, to a political committee, to a political party, to an affiliated party committee, or to a referendum committee, whether or not made in an election year, and any contract, agreement, or other obligation to make a contribution.”¹⁹

¹⁹ N.C. Gen. State § 163-278.6(13) (emphasis added).

Similarly, an “expenditure” is defined to include:

“[A]ny purchase, advance, conveyance, deposit, distribution, transfer of funds, loan, payment, gift, pledge or subscription of money or anything of value whatsoever, whether or not made in an election year, and any contract, agreement, or other obligation to make an expenditure, *to support or oppose the nomination, election, or passage of one or more clearly identified candidates*, or ballot measure.”²⁰

Both of these definitions are contingent on a thing of value being used to support or oppose the nomination or election of North Carolina candidates.

The Board has also defined in-kind contributions to include “the provision or discount of a product to [a] committee,” advising that “[t]he contributor shall provide the committee with a statement setting forth the fair market value of the in-kind contribution.”²¹

Notably, the Board also acknowledged that activities which do not “support or oppose” a candidate and which are sponsored by an entity other than a political committee may be coordinated with candidates without resulting in a contribution, provided that they do not constitute electioneering communications and do not include any express advocacy.²² In a 2015 advisory opinion, the Board concluded that “[i]f an organization is not a North Carolina political committee and is not engaging in electioneering communications or communications that contain express advocacy, then communications made by those organizations are not subject to State Board of Elections regulation,” and similarly that “[i]f an organization that is not a North Carolina political committee coordinated issue advocacy communications with a Candidate and those issue advocacy communications do not constitute electioneering communications or contain express advocacy, payments for those communications cannot be deemed ‘coordinated expenditures’ or ‘contributions.’”²³

In a 2008 advisory opinion, the Board also addressed an analogous question regarding candidate attendance at a legislative conference. The Board noted that the funds raised to pay for the conference “will not be used to support or oppose any candidate, political party, or political committee,” that the conference host was a “nonpartisan organization,” that the funds would be used for activities “unrelated to any *given* legislator’s election or reelection” and that the funds in question were therefore not contributions.²⁴ The Board also observed that while contributions to specific candidates would generally constitute in-kind contributions, “[a]n individual legislator or other State official or candidate for legislative or other State office attending the...[c]onference, however, could accept a complimentary gift offered to every attendee without it constituting a contribution under the campaign finance statutes.”²⁵ Significantly, the Board applied this

²⁰ *Id.* § 163-278.6(51) (emphasis added).

²¹ N.C. State Board of Elections, Campaign Finance Manual at 51, 54 (Feb. 2022), https://s3.amazonaws.com/dl.ncsbe.gov/Campaign_Finance/Campaign-Finance-Manual.pdf.

²² See N.C. State Bd. of Elections Adv. Op. 2015-08-28 (Weisel).

²³ *Id.*

²⁴ N.C. State Bd. of Elections Adv. Op. 2008-04-21 (Speaker Hackney et al.) (emphasis added).

²⁵ *Id.*

analysis to *candidates*, not just incumbent officeholders; analysis was not contingent on incumbent officeholders attending the conference in an official capacity. The Board’s rationale was presumably that the conference costs were not contributions because they were not for the purpose of supporting or opposing candidates and because gifts would be given to all attendees, not merely candidates the organization wished to support; the reference to “any given legislator’s election or reelection” similarly suggests that a thing of value provided to all candidates, rather than only a specific subset of candidates, would not constitute a contribution.

II. Legal Analysis

The plain text of state law and relevant precedent support the conclusion that DDC’s proposed activities would not result in a contribution to North Carolina campaigns and political parties because, as described in more detail below, DDC’s proposed activities would not “support or oppose the nomination or election of one or more clearly identified candidates,” and DDC is not providing services to campaigns and parties at a discount relative to other recipients of the services.

First, the purpose of DDC’s proposed activities is to help secure the democratic process by providing all campaigns and political parties with the knowledge, training, and resources they need to defend themselves from foreign cyber threats — not to support or oppose the nomination or election of specific North Carolina candidates. Although individual campaigns and political parties will necessarily benefit from these activities by receiving information and resources that they would otherwise not have access to and/or could not afford, the ultimate beneficiaries will be the nation’s voters and our electoral system. Moreover, DDC has structured its internal governance and its proposed activities to operate in a nonpartisan, objective manner that does not favor any candidate or political party over another. Therefore, under the letter of the law, these services would not be supporting or opposing any specific candidates; rather, because they are available to *all* candidates and committees, the services do not influence the likelihood of election of any specific candidate. This approach is consistent with the Board’s approach in the 2008 advisory opinion described above, wherein the Board determined that a thing of value offered to all candidates, and not for the purpose of supporting or opposing their election, would not constitute a contribution to those candidates.

Second, in addition to being consistent with the text of the statute, DDC’s request is also consistent with the purpose of state campaign finance law, which is to regulate activities that support or oppose specific North Carolina candidates. Both the State Board of Elections and the courts have affirmed that state campaign finance law regulates only contributions and expenditures made to support and oppose North Carolina candidates. As one federal court has observed, “the determination as to whether an action is taken ‘to support or oppose ... a clearly identified candidate’ is thus one of the foundations of North Carolina’s campaign finance regulatory scheme.”²⁶ Here, the services in question are being provided to secure the integrity of elections by being made available on an equal basis to all candidates and parties, and *not* to

²⁶ N.C. Right to Life, Inc. v. Leake, 525 F.3d 274, 280 (4th Cir. 2008).

support or oppose specific candidates. In short, DDC's proposal is consistent with how the state has historically interpreted the scope of state campaign finance law.

Third, DDC's services are not being provided at a discount. The State Board of Elections has noted that the valuation of an in-kind contribution includes "the provision or discount of a product to [a] committee" and is based on "the fair market value of the in-kind contribution."²⁷ But in this case, there *is* no "fair market value" for the services in question. DDC and its corporate partners are not providing free services for which they — or any third party — would otherwise charge recipients a fee. Rather, DDC is a non-profit; its sole purpose is to provide these types of services to candidates and parties for free. Furthermore, both DDC and its corporate partners are offering services that are only relevant to, and only provided to, campaigns and committees — and are provided to *all* campaigns and committees for free — so there is no usual and normal charge for the services that are being foregone or waived. In short, DDC is making generally and publicly available a service for the purpose of ensuring the integrity of our electoral system, rather than providing free goods and services that would otherwise be paid for by campaigns and political parties.

Finally, in its advisory opinion approving the DDC program, the Federal Election Commission observed that the threat of foreign cyberattacks on American elections constituted "urgent circumstances" that posed "unique challenges," and that "this highly unusual and serious threat militates in favor of granting DDC's request."²⁸ The Commission — which has exclusive jurisdiction over enforcement of the prohibition on foreign contributions and other foreign participation in federal, state, and local elections²⁹ — therefore approved the request. The same circumstances that warranted approval of DDC's request before the Federal Election Commission exist here, and approval of this request would be consistent with the Board's stated mission of "ensuring the safety and security of all voters and the elections process," including with respect to cybersecurity threats.³⁰

CONCLUSION

For these reasons, we respectfully ask the State Board of Elections to confirm that DDC's provision of cybersecurity goods and services to North Carolina campaigns and political parties would not result in an in-kind contribution from DDC or its corporate partners to participating campaigns and political parties.

Thank you for your consideration of this advisory opinion request. Please do not hesitate to contact us if you have any questions or require additional information.

²⁷ N.C. State Board of Elections, Campaign Finance Manual at 51, 54 (Feb. 2022), https://s3.amazonaws.com/dl.ncsbe.gov/Campaign_Finance/Campaign-Finance-Manual.pdf.

²⁸ FEC, Adv. Op. 2018-12 at 8.

²⁹ 52 U.S.C. § 30106(b)(1).

³⁰ N.C. State Board of Elections, Election Security, <https://www.ncsbe.gov/election-security>.

Respectfully Submitted,

Ezra W. Reese

ereese@elias.law

Jonathan A. Peterson (NC Bar # 44698)

jpeterson@elias.law

ELIAS LAW GROUP LLP

250 Massachusetts Avenue NW

Suite 400

Washington, DC 20001

Michael E. Toner

mtoner@wiley.law

Brandis L. Zehr

bzehr@wiley.law

Hannah Bingham

hbingham@wiley.law

WILEY REIN LLP

2050 M Street NW

Washington, DC 20036

Counsel to Defending Digital Campaigns, Inc.

Exhibit A

Advisory Opinion Request 2018-12 (Defending Digital Campaigns, Inc.)

September 5, 2018

RECEIVED
FEC MAIL CENTER
2018 SEP -6 PM 1:02

2018 SEP -6 PM 2:35

OFFICE OF
GENERAL COUNSEL

BY HAND DELIVERY

Office of General Counsel
Attn: Lisa J. Stevenson, Acting General Counsel
Federal Election Commission
1025 First Street NE
Washington, DC 20463

Re: Advisory Opinion Request

Dear Ms. Stevenson:

Pursuant to 52 U.S.C. § 30108, we seek an advisory opinion on behalf of Defending Digital Campaigns, Inc., (“DDC” or the “Organization”), a nonprofit corporation formed under the provisions of the District of Columbia Nonprofit Corporation Act (D.C. Code, Title 29), seeking guidance on the permissibility of a number of proposed activities under the Federal Election Campaign Act of 1971, as amended (the “Act”), and Federal Election Commission (“FEC” or the “Commission”) regulations.

BACKGROUND

Ongoing attempts by foreign powers to undermine our democratic processes through cyber and information operations pose a novel and unprecedented threat to the integrity of our electoral system.¹ While this threat has many facets, the vulnerability of modern political committees to cyberattack and infiltration has been repeatedly exploited by foreign actors over the past several election cycles and arguably represents one of the most critical weaknesses in our collective defenses against this new form of warfare. This is particularly alarming given the amount of sensitive voter information and other data that campaigns regularly collect and share. And given the scale and interconnectedness of the modern American campaign landscape, shoring up this weakness will require both a widely distributed deployment of resources and expertise as well as a greater level of communication and nonpartisan cooperation among and between campaigns, political parties, and the cybersecurity community. We have also seen candidates personally targeted and imagine their families are vulnerable as well. The frailty of their personal online security can be a very tempting vector of attack for adversaries who wish to punish lawmakers or candidates they believe are acting counter to their interests.

¹ Press Release, Senate Intel Completes Review of Intelligence Community Assessment on Russian Activities in the 2016 U.S. Elections (May 16, 2018), <https://www.burr.senate.gov/press/releases/senate-intel-completes-review-of-intelligence-community-assessment-on-russian-activities-in-the-2016-us-elections>.

DDC intends to address this systemic vulnerability by facilitating the development and delivery of a set of campaign-tailored resources and training aimed at fortifying campaign committees and other political committees against these attacks, and by developing and maintaining channels for information sharing among committees, technology providers, and cybersecurity experts in the public and private sectors. In short, DDC intends to operate as an Information Sharing and Analysis Organization (“ISAO”) for the most vulnerable players in our electoral system: campaigns and political parties.

DDC seeks assurance from the Commission that engaging in these activities on a nonpartisan basis according to neutral, objective criteria will not result in DDC or its private sector sponsors and partners making “contributions” under the Act. Although these activities will necessarily entail the provision of resources to individual political committees, the purpose of these efforts is not to benefit any one campaign or political party over another or to otherwise influence any federal election. Rather, DDC plans to make resources available to all candidates who meet simple, objective criteria, regardless of party. The purpose is to help safeguard American elections from foreign interference by providing these defenses to a critical mass of those political committees most vulnerable to attack, and by fostering the development of an information sharing network that can detect and coordinate effective responses to new threats and outbreaks before they have a chance to negatively impact the integrity of our elections.

DDC’s proposal is ambitious and contemplates activities that the Commission has not had occasion to consider in the context of a threat to our democratic institutions as unique and unprecedented as the one we currently face. However, as “the agency of the United States Government charged with protecting our federal election financing system from foreign attack,”² the FEC has a unique responsibility to do all it can to facilitate nonpartisan efforts aimed at providing campaigns and political parties with the resources and information they need to defend themselves from these extraordinary attacks. In the face of this threat, “failure to act is no longer an option.”³

I. The Threat Facing Campaigns and Political Parties

While Russia’s activities in the 2016 elections exposed serious national security vulnerabilities in our election infrastructure, for several election cycles individual campaigns and political parties have proven to be particularly tempting targets for foreign powers and other malicious actors operating online. In 2008, Chinese hackers infiltrated the Obama and McCain campaigns, and stole large quantities of information from both. In 2012, the Obama and Romney campaigns each faced hacking attempts against their networks and websites. And in 2016, cyber operatives

² Statement of Commissioner Ellen L. Weintraub On the FEC’s Unanimous Bipartisan Decision to Address Internet Political Advertising Disclaimers (Nov. 16, 2017), <https://www.fec.gov/resources/cms-content/documents/ELW-statement-on-FECs-opening-of-a-disclaimer-rulemaking.pdf>.

³ *Id.*

believed to be sponsored by Russia stole and leaked tens of thousands of emails and documents from Democratic campaign staff.⁴

As campaigns and political parties have become increasingly digital, they have become increasingly vulnerable to cyberattacks. And Congressional campaigns—with less staff, resources, and institutional experience than presidential campaigns and national party committees—are even more vulnerable to cyberattacks and are likely to be increasingly targeted in future elections. Indeed, news reports of attempted or successful hacks of Congressional campaigns have become more and more common:

- In March 2018, the campaign of Tennessee Senate candidate Phil Bredesen contacted the FBI about a potential breach of its system.⁵
- Also in March, the campaign of a U.S. House candidate in California's 45th district discovered that its systems had been breached and reported the incident to the FBI. The campaign reportedly decided it could not afford the cost of a professional cybersecurity firm to investigate the attack, nor did it have the resources to replace infected computers.⁶
- A second candidate for U.S. House in California, Dr. Hans Keirstead, reported sophisticated phishing emails, which successfully gained credentials to access Dr. Keirstead's email, as well as repeated attempts to gain access to the campaign's website, including "130,000 attempts to gain administrator access through the cloud server that was used to house the site."⁷
- In July 2018, the campaign of Alabama congressional candidate Tabitha Isner announced that Russians had attempted to hack the campaign's website.⁸ Later that day, Microsoft announced that it had helped detect and block attempted hacks of three congressional campaigns so far in 2018.⁹

⁴ Defending Digital Democracy Project, *The Cybersecurity Campaign Playbook 5* (rev. May 3, 2018), https://www.belfercenter.org/sites/default/files/files/publication/CampaignPlaybook_0.pdf.

⁵ 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 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>.

⁷ Mark Morales, *Democrat Who Challenged GOP Congressman Said He Was Hacked*, CNN (Aug. 15, 2018), <https://www.cnn.com/2018/08/15/politics/dana-rohrbacher-opponent-cyberattack-hack/index.html>.

⁸ 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>.

⁹ 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>.

II. Establishment of the Defending Digital Democracy Project

In the wake of the 2016 elections, the Belfer Center for Science and International Affairs at Harvard Kennedy School launched a new, bipartisan initiative called the Defending Digital Democracy Project (“D3P”).¹⁰ Co-led by the former campaign managers for Hillary Clinton and Mitt Romney and experts from the national security and technology communities, the project aimed to identify and recommend strategies, tools, and technology to protect democratic processes and systems from cyber and information attacks by creating a unique and bipartisan team comprising political operatives and leaders in the cybersecurity and national security fields.

Recognizing the lack of resources available to campaigns struggling to deal with cybersecurity issues, D3P released “The Cybersecurity Campaign Playbook” (the “Playbook”) in November 2017.¹¹ The Playbook was designed to give campaigns of any size simple, actionable guidance to make their information more secure from adversaries trying to attack their organization.

It has, however, become increasingly apparent that campaigns are in need of more direct, hands-on assistance to address cybersecurity threats. As the Playbook explains:

Today’s campaigns are uniquely soft targets. They’re inherently temporary and transient. They don’t have the time or money to develop long-term, well-tested security strategies. Large numbers of new staff are often onboarded quickly without much time for training. They may bring their own hardware from home and the malware lurking on it. Events move quickly, the stakes are high, and people feel that they don’t have time to care about cybersecurity. There are a lot of opportunities for something to go wrong.

At the same time, campaigns rely more and more on proprietary information about voters, donors, and public opinion. They also store sensitive documents like opposition research, vulnerability studies, personnel vetting documents, first-draft policy papers, and emails on various servers. The risks of a potential attack are increasing and so are the consequences.

Unfortunately, the vast majority of campaigns simply do not have adequate resources to address these threats. Most campaigns do not have the resources to hire full-time, professional cybersecurity staff, and even basic cybersecurity consulting software and services can overextend the budget of most congressional campaigns. Even presidential campaigns and national party committees require expert guidance to know how to best allocate resources for cybersecurity.

¹⁰ Harvard Kennedy School, Belfer Center for Science and International Affairs, Defending Digital Democracy Project, <https://www.belfercenter.org/project/defending-digital-democracy> (last visited Sept. 5, 2018).

¹¹ *The Cybersecurity Campaign Playbook*, *supra* note 4.

Furthermore, outside actors like private sector digital platforms, cybersecurity providers, and government agencies don't have access to a nonpartisan medium trusted by campaign operatives to share information and coordinate action. This lack of information sharing leads to otherwise preventable breaches and makes it more difficult to detect and respond to threats before it's too late.

III. DDC's Structure and Activities

D3P's founding members formed DDC as a distinct nonprofit organization with the specific mission of directly engaging with national party committees and congressional and presidential campaigns. DDC's planned engagement has two overarching and interrelated aims: to provide campaigns and political parties with the specific knowledge, training, and resources they need to defend themselves from cyber threats; and to create secure, nonpartisan forums for information sharing among and between campaigns, political parties, technology providers, law enforcement, and other government agencies in order to detect new and emerging cyber threats and facilitate the development and deployment of effective responses to neutralize them.

DDC is structured to ensure it operates as a truly nonpartisan, not-for-profit organization. It was established as a District of Columbia nonprofit corporation and is organized as a social welfare organization under Section 501(c)(4) of the Internal Revenue Code.¹² To demonstrate DDC's truly nonpartisan focus, DDC's organizing documents require the Organization to adhere to the Internal Revenue Code's prohibitions on political campaign intervention that apply to Section 501(c)(3) organizations. Specifically, DDC's articles of incorporation and bylaws mandate that the Organization "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 Code."¹³ In addition, pursuant to DDC's organizing documents, and in accordance with IRS rules governing Section 501(c) organizations, DDC directors, officers, and staff are explicitly barred from personally profiting from the Organization's activities apart from board-approved reasonable compensation for officers and employees, which will be determined in accordance with recognized procedures and best practices for nonprofit salary determinations.¹⁴

The Organization's initial board of directors—consisting of Democrat Robby Mook, Republican Matt Rhoades, and Debora Plunkett, former Director of Information Assurance at the NSA and veteran of the National Security Council in both Democratic and Republican administrations—creates a well-rounded foundation for DDC's mission. Day-to-day operations of the Organization are managed by a nonpartisan President and staff. DDC's board of directors provides oversight

¹² See Articles of Incorporation of Defending Digital Campaigns, Inc. (Attached hereto as Appendix A).

¹³ See *id.*, Bylaws of Defending Digital Campaigns, Inc. (Attached hereto as Appendix B, Exhibit A).

¹⁴ See Defending Digital Campaigns, Inc., Compensation Review Policy (Attached hereto as Appendix B, Exhibit E).

and will be assisted by an advisory committee of veteran political operatives, cybersecurity professionals, and private sector digital platform providers.

IV. DDC's Proposed Eligibility Criteria

DDC plans to make its services available to each of the 11 active, federally-registered national party committees,¹⁵ and to federally-registered candidate committees satisfying any of the following objective eligibility requirements (collectively, "Eligible Committees" or "Committees"):

- 1) House candidates whose committees have raised at least \$50,000 in receipts for the current election cycle, and Senate candidates whose committees have raised at least \$100,000 in receipts for the current cycle;
- 2) House or Senate candidates who have qualified for the general election ballot in their respective races; or
- 3) Any presidential candidate who is polling above 5% nationally.

DDC has selected these clear, nonpartisan criteria to ensure that the national party committees and campaigns most likely to become targets of cyberattacks have access to DDC's services on a fair and equal basis. DDC will proactively reach out to Eligible Committees in a consistent manner and offer the same suite of services to all Eligible Committees in a given race.

DDC plans to eventually make a number of services available to Eligible Committees. However, DDC will phase in services as resources and time allow and will not provide a service unless it has the resources available to provide that service to all Eligible Committees in a given election cycle and/or race.

V. DDC's Proposed Activities

DDC's planned program of activities is still under development and will ultimately depend on several factors, including funding availability, the outcome of negotiations with potential corporate, institutional, and government partners, and the Commission's guidance on the permissibility of various activities under the Act and FEC regulations. However, DDC is interested in engaging in one or more the following activities.

¹⁵ It is our understanding that there are currently 11 active federally-registered national party committees: Republican National Committee (#C00003418); DNC services corp./Dem. Nat'l Committee (#C00010603); NRSC (#C00027466); DSCC (#C00042366); NRCC (#C00075820); DCCC (#C00000935); Socialist Workers National Campaign Committee (#C00111476); Socialist National Committee (#C00129668); Libertarian National Committee (#C00255695); Green Party of the United States (#C000370221); and the Green Senatorial Campaign Committee (#C00428664). Although DDC currently does not have the resources to engage with state political party committees, it may do so in future election cycles.

A. Information Sharing

As the Department of Homeland Security has recognized, “America’s cyber adversaries move with speed and stealth. To keep pace, all types of organizations . . . need to be able to share and respond to cyber risks in as close to real-time as possible.”¹⁶ Private sector entities, government agencies, campaigns, and political party committees receive information every day on malicious email addresses, IP addresses, and other intelligence on cyber threats targeting campaigns and elections. “Organizations engaged in information sharing related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States.”¹⁷ DDC would like to create information sharing systems—listservs, bulletins, etc.—to anonymously share such information and potentially collaborate with the Federal Bureau of Investigation, the Department of Homeland Security, and other law enforcement officials to further enhance this information. The private sector and many of the platform providers for campaigns and political parties, in particular, have a wealth of information on cyber threats targeting campaigns and elections. Currently, there is no streamlined, nonpartisan clearinghouse for these actors to share this information. DDC would like to fill this void by functioning as an ISAO focused on cyber threats targeting the political campaign community; there would be no charge for private sector entities, government agencies, or Eligible Committees to participate in DDC’s information-sharing activities.

A nonpartisan, independent entity is needed to play this role, since campaigns have proven reluctant to engage directly with the Federal Bureau of Investigation and Department of Homeland Security. A trusted, independent entity can be a place where government, the private sector, and campaigns could each pool and monitor intelligence about attacks on an anonymous basis.

Furthermore, a nonpartisan, independent entity can provide campaigns with advice and assistance accessing resources in the case of a suspected breach and could encourage or even help facilitate engagement with the government.

B. Cybersecurity Hotline

DDC would like to create and operate a cybersecurity “hotline” that Eligible Committees could call for advice or coaching on cybersecurity issues. This hotline would also serve to identify new and emerging cybersecurity threats in order to notify appropriate government agencies as necessary. There would be no fee for Eligible Committees to call the hotline.

¹⁶ U.S. Dep’t of Homeland Security, Information Sharing and Analysis Organizations (ISAOs), <https://www.dhs.gov/isao> (last visited Sept. 5, 2018).

¹⁷ *Id.*

C. Cybersecurity “Bootcamps,” Advanced Training, and Certification Courses

DDC would like to offer cybersecurity training opportunities or “bootcamps” for Eligible Committees’ leadership and IT staff on core campaign cybersecurity issues. DDC also would like to offer advanced cybersecurity training and certification courses for Eligible Committees’ IT staff. There would be no fee for Eligible Committees’ staff to attend any of these training opportunities. For efficiency purposes, DDC may consider hosting such trainings at central locations and providing free or discounted transportation and lodging for Eligible Committees’ staff to attend. DDC may recruit cybersecurity experts to speak at such trainings in a volunteer capacity and would likely contract with cybersecurity firms to provide the advanced training and certification courses.

D. On-Site Training and Assistance

As D3P recognized in the Playbook, “[c]ybersecurity is fundamentally a human problem, not a technical one. . . . Successful cybersecurity practices depend on creating a culture of cybersecurity awareness.” Although off-site training will help Eligible Committees’ IT staff learn core cybersecurity practices, it is vital for all employees of Eligible Committees to receive basic information security training. Moreover, Eligible Committees may need advice on how to implement cybersecurity practices into their own infrastructure. DDC would like to facilitate free on-site visits to Eligible Committee offices by cybersecurity professionals to provide information security training and/or general cybersecurity assistance. Under one option, cybersecurity professionals would provide these services in a volunteer capacity while on unpaid leave or while on paid leave accrued in accordance with their employers’ existing leave policies. Under a second option, DDC would establish partnerships with cybersecurity firms that would agree to provide paid leave to their employees to provide this on-site cybersecurity assistance.

E. Cybersecurity Incident Response and Monitoring Services

DDC would like to offer cybersecurity incident response services and brand monitoring services to Eligible Committees free of charge or at a reduced cost. To offer these services, DDC would enter into retainer agreements with one or more digital security vendors and brand protection services. It is often difficult and cost-prohibitive for campaigns and political parties to work with digital security vendors. DDC would like to retain a digital security firm providing incident response services and allow Eligible Committees to contact the retained firm in the event of a suspected phishing attack, to forward suspicious emails, etc. DDC may also enter into similar retainer agreements with one or more brand protection services—entities with the ability to provide monitoring and notification services that identify fake websites being set up to imitate legitimate campaigns or political parties. Such vendors would monitor the Internet for fraudulent or unauthorized activities purporting to be those of Eligible Committees and notify Eligible Committees of any such activities.

F. Free or Reduced-Cost Software

DDC would like to work with technology companies—such as platform providers like Google and Microsoft—to customize the companies’ existing software for campaigns and political parties, similar to the manner in which companies frequently customize their products and services for particular types of customers (e.g., students, small businesses, nonprofit organizations). DDC would also like to negotiate partnerships with these companies to secure free or discounted licenses for both customized and off-the-shelf software for Eligible Committees. These software license agreements would be entered into between the software providers and Eligible Committees, but DDC would act as an intermediary between the providers and Eligible Committees to ensure that licenses are provided on a fair and equal basis to all Eligible Committees. In addition, DDC staff would provide Eligible Committees with assistance installing the software and educating staff on proper use of the software.

G. Free or Reduced-Cost Hardware

Similarly, DDC would like to enter into partnerships with technology providers to provide Eligible Committees with free or reduced-cost hardware, such as Yubi-keys used to provide two-factor authentication for Eligible Committee computers. Again, DDC would not purchase the hardware itself, but would act as an intermediary between the providers and Eligible Committees to ensure that the hardware is provided on a fair and equal basis to all Eligible Committees, and to educate Eligible Committee staff on its proper use.

QUESTIONS PRESENTED

1. Whether DDC may 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, which Eligible Committees could call to ask basic cybersecurity questions or report cybersecurity incidents.
2. Whether DDC may provide cybersecurity bootcamps, advanced training sessions, and certification courses without charge to Eligible Committees without making in-kind contributions to such Eligible Committees.
3. Whether DDC may entirely or partially pay for the transportation and lodging expenses of Eligible Committees’ staff to attend DDC’s cybersecurity bootcamps, advanced training sessions, and/or certification courses without making in-kind contributions to such Eligible Committees.

4. Whether DDC may 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; and/or
 - b. Cybersecurity professionals who are acting in a volunteer capacity.
5. Whether DDC may 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. Whether DDC may facilitate the provision of free and/or discounted cybersecurity-related software licenses and/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 and/or hardware licenses.
7. Whether DDC may assist Eligible Committees with installing and using the software licenses and/or hardware referred to in Question 6 without making in-kind contributions to such Eligible Committees.

LEGAL ANALYSIS

- I. DDC's proposed activities are not for the purpose of influencing federal elections and, accordingly, DDC may undertake the activities described above to counter foreign interference in American elections without making prohibited corporate in-kind contributions under the Act.**

Because DDC's proposed activities are for the purpose of protecting U.S. elections from foreign interference—and not for the purpose of influencing the elections themselves—the proposed activities fall outside of the scope of the Act and would not result in prohibited corporate in-kind contributions to Eligible Committees.

The Act and Commission regulations prohibit a corporation from making any contribution to a candidate in connection with a federal election.¹⁸ The Act defines “contribution” to include anything of value “made by any person for the purpose of influencing any election for Federal office.”¹⁹ A contribution also includes “the payment by any person of compensation for the personal services of another person which are rendered to a political committee without charge

¹⁸ 52 U.S.C. § 30118(a), (b)(2); *see also* 11 C.F.R. § 114.2(b).

¹⁹ 52 U.S.C. § 30101(8)(A)(i).

for any purpose.”²⁰ Commission regulations further provide that “anything of value” includes in-kind contributions, such as the provision of goods or services “without charge or at a charge that is less than the usual and normal charge for such goods or services.”²¹

DDC’s proposed activities fall outside the scope of the Act and Commission regulations because they are not “for the purpose of influencing” any federal election. Rather, their purpose is to help protect our system of democratic governance by providing political party and campaign committees on a nonpartisan basis with the specifically tailored resources they need to participate in the electoral process free from interference by malicious actors attempting to undermine the integrity of American elections. Although individual campaigns and political parties will necessarily benefit from these activities by receiving resources and information that they would otherwise not have access to and/or could not afford, this assistance would be provided according to predetermined, nonpartisan, objective criteria, and would never favor one candidate or political party over another. Further, the ultimate beneficiary of these activities will be the nation’s voters and the electoral system itself, much the same way that an immunization program inoculates individuals for the ultimate purpose of safeguarding an entire community from a disease.

The Commission has on several occasions considered the applicability of the Act to nonpartisan activities that—while resulting in services or other direct or indirect benefits being provided to individual political committees—were found not to be for the purpose of influencing a federal election and concluded that such activities did not constitute contributions or expenditures for purposes of the Act.

For example, in Advisory Opinion 2000-16, the Commission approved another proposal intended to combat a threat to our democratic institutions, albeit one considerably less immediate and acute than foreign interference in our elections. In that opinion the Commission unanimously approved a proposal by a nonprofit organization to pay for the production and placement of several internet advertisements in support of various Presidential candidates in order to “examine and address the problem of young voter disengagement from the political process and the threat this disengagement poses to democracy at large.”²² Under the proposal, the advertisements would be viewed by approximately 36,000 individuals as part of a project designed to study political disengagement among young Americans.²³ The organization’s request to the Commission stressed that the company was nonpartisan in both its structure and its activities and, as a 501(c)(3) organization, it was prohibited from participating or intervening in any political campaign on behalf of or in opposition to any candidate for public office.²⁴ As explained to the Commission, the organization’s motivation for producing and placing the advertisements was to generate survey data that would aid in the evaluation of the organization’s

²⁰ *Id.* § 30101(8)(A)(ii); 11 C.F.R. § 100.54 (emphasis added).

²¹ 11 C.F.R. § 100.52(d)(l).

²² FEC Adv. Op. 2000-16 (Third Millennium).

²³ *Id.*

²⁴ See Request for an Advisory Opinion by Third Millennium (June 8, 2000).

hypothesis regarding why young Americans vote in such low numbers.²⁵ The Commission, accordingly, found that the proposal was permissible under the Act.²⁶

More recently, in Advisory Opinion 2015-14, the Commission determined that a university could provide a stipend and academic credit for a student's campaign internship without making a prohibited contribution under the Act. Although, as noted above, the definition of "contribution" expressly 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*,"²⁷ the Commission concluded that because the grant program stipends were being "provided to students for *bona fide* educational objectives, not for the provision of personal services to federal campaigns,"²⁸ they did not result in impermissible corporate contributions from the university.

As with the stipend approved by the Commission in Advisory Opinion 2015-14, 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. And just as the Commission nonetheless permitted the stipend because the underlying objective of the university's internship program was to provide students with educational opportunities, not to influence federal elections, so too should the Commission permit the payments proposed by DDC because their underlying objective is not to influence the outcome of any federal election but rather to provide the American public with elections free from foreign interference. And unlike the stipend—which subsidized a student's ability to engage in federal election-influencing activities that directly furthered a campaign's electoral objectives, and did not automatically trigger the provision of equal support to the opposing campaign—DDC's payments would only be used to protect campaigns and political parties from cybersecurity threats and would be proactively offered on an equal, nonpartisan basis to competing campaigns and parties.

Further support for the permissibility of DDC's proposed activities under the Act can be found in the group of statutory and regulatory exemptions to the corporate contribution ban for candidate-related activities by nonprofit organizations. These exemptions—which allow nonprofit organizations to prepare and distribute voter guides,²⁹ engage in nonpartisan activity designed to encourage individuals to vote or to register to vote,³⁰ stage candidate debates,³¹ engage in press activities, and host candidate appearances on their premises,³²—share a common theme of protecting and encouraging nonpartisan activities that are intended to foster civic engagement and facilitate the proper functioning of democratic processes. The fact that DDC's proposed

²⁵ See *id.*; FEC Adv. Op. 2000-16 (Third Millennium).

²⁶ FEC Adv. Op. 2000-16 (Third Millennium).

²⁷ 52 U.S.C. § 30101(8)(A)(ii); 11 C.F.R. § 100.54 (emphasis added).

²⁸ FEC Adv. Op. 2015-14 (Hillary for America II) at 4.

²⁹ 11 C.F.R. § 114.4(c)(5).

³⁰ 52 U.S.C. § 30101(9)(B)(ii).

³¹ 11 C.F.R. 110.13.

³² *Id.* § 114.4(c)(7).

activities do not fit squarely within any of these exemptions, but share elements with most of them, reflects the reality that the Act and Commission regulations simply did not envision the specter of foreign interference in the electoral process itself, the burden it would impose on the proper functioning of the electoral process, and the nonpartisan role that nonprofit organizations could play in addressing this issue.

However, the Commission has previously adapted and applied these exemptions to new circumstances and could appropriately do so here as well. In Advisory Opinion 2011-26, the Commission extended application of the exception to the definition of expenditure for nonpartisan activity designed to encourage individuals to vote or to register to vote to also cover raising and spending funds for the purposes of identifying citizens who do not possess photographic identification in states that require a citizen to present photographic identification to register to vote or to vote, and to assist those citizens in obtaining such photographic identification. The Commission found that these activities were connected because they were “intended to encourage or assist individuals to register to vote or to vote, by making it possible for them to satisfy State laws requiring photographic identification in order to register to vote or to vote.”³³

DDC’s proposed activities are also distinguishable from fact patterns under which the Commission has rejected proposals by corporations to provide free or discounted services to campaigns. For example, in Advisory Opinion 1996-2, the Commission held that CompuServe could not offer a product to campaigns free of charge when it typically charged other non-campaign users for the same service, rejecting CompuServe’s argument that the publicity it would receive from free users would heighten the company’s prestige and goodwill and encourage subscribers and, thus, was not a corporate contribution.³⁴ The Commission concluded that “substantial publicity, goodwill or other commercial benefit does not negate or reduce the corporate contribution” as “[s]uch publicity or benefit does not constitute consideration.”³⁵ Here, by contrast, DDC is not arguing that its proposed activities with the Eligible Committees represent a fair-market exchange of value or would otherwise provide DDC with any offsetting benefit other than helping to accomplish its core objective of protecting American elections from foreign interference.

II. The provision of free or discounted software and/or hardware to Eligible Committees by private sector entities, as described above and facilitated by DDC, would also not result in prohibited corporate in-kind contributions under the Act.

The conclusion above should likewise extend to the free or discounted software and/or hardware provided by private sector entities, so long as it is under the nonpartisan control and direction of DDC, and in accordance with the pre-determined neutral and objective criteria described above.

³³ FEC Adv. Op. 2011-26 (Martin H. Freeman).

³⁴ FEC Adv. Op. 1996-02 (CompuServe).

³⁵ *Id.*

Although the Commission has reviewed numerous proposed and actual relationships between corporate vendors and political campaigns to determine whether they would or did result in a prohibited in-kind contribution to the campaigns, to our knowledge the Commission has not grappled with this fact pattern. However, it has addressed an analogous situation, in which it permitted the use of corporate funding for debates staged by nonprofit organizations.³⁶

In *Becker v. FEC* the Court held that FEC debate regulations allowing corporate funding of certain debate staging organizations reflected a permissible construction of the Act and were not inconsistent with the definitions of "contribution" and "expenditure" provided by the Act.³⁷

Just as nonpartisan debate staging organizations are permitted to accept corporate funding and support, so too should DDC be permitted to accept the support and specialized expertise of corporate sponsors and other private-sectors entities needed to successfully engage in this critical, nonpartisan project.

CONCLUSION

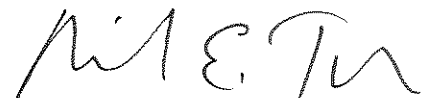
In conclusion, we respectfully submit that DDC's proposed activities fall outside the scope of the Act and, therefore, would not result in prohibited corporate in-kind contributions to Eligible Committees.

We would be happy to provide any additional information you may request. We look forward to your response.

Very truly yours,



Marc E. Elias
Perkins Coie LLP
700 13th Street NW, Suite 600
Washington, DC 20005
202.434.1609
MElias@perkinscoie.com



Michael E. Toner
Wiley Rein LLP
1776 K Street NW
Washington, DC 20006
202.719.7545
MToner@wileyrein.com

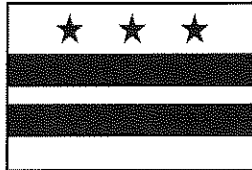
Counsel to Defending Digital Campaigns, Inc.

³⁶ See 11 C.F.R. § 110.13.

³⁷ *Becker v. Fed. Election Comm'n*, 230 F.3d 381, 394 (1st Cir. 2000), *cert. denied*, 532 U.S. 1007 (2001).

APPENDIX A

GOVERNMENT OF THE DISTRICT OF COLUMBIA
DEPARTMENT OF CONSUMER AND REGULATORY AFFAIRS
CORPORATIONS DIVISION



C E R T I F I C A T E

THIS IS TO CERTIFY that all applicable provisions of the District of Columbia Business Organizations Code have been complied with and accordingly, this ***CERTIFICATE OF INCORPORATION*** is hereby issued to:

Defending Digital Campaigns, Inc.

Effective Date: 7/31/2018

IN WITNESS WHEREOF I have hereunto set my hand and caused the seal of this office to be affixed as of 7/31/2018 2:40 PM



Business and Professional Licensing Administration

A handwritten signature in cursive script, reading 'Patricia E. Grays'.

PATRICIA E. GRAYS
Superintendent of Corporations
Corporations Division

Muriel Bowser
Mayor

Tracking #: 4ZPoZYHM

JUL 31 2018

File Copy File

ARTICLES OF INCORPORATION
of
DEFENDING DIGITAL CAMPAIGNS, INC.

TO: Department of Consumer and Regulatory Affairs
District of Columbia Government
Corporations Division

The undersigned, acting as the Incorporator of a nonprofit corporation under the provisions of the District of Columbia Business Organizations Code (D.C. Code, Title 29) (the "Act"), adopts the following Articles of Incorporation:

FIRST: The name of the Corporation is Defending Digital Campaigns, Inc. (the "Corporation").

SECOND: The Corporation is incorporated as a nonprofit corporation under D.C. Code, Title 29, Chapter 4.

THIRD: The period of the Corporation's duration is perpetual.

FOURTH: The Corporation is organized as a social welfare organization within the meaning of Section 501(c)(4) of the Internal Revenue Code of 1986, as now in effect or as hereafter may be amended (the "Code"). The purposes for which the Corporation is formed are 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, and to engage in any lawful act or activity for which corporations may be organized under the Act. In furtherance thereof, the Corporation shall have all the general powers enumerated in Section 29-403.02 of the Act as now in effect or as may hereafter be amended, together with the power to solicit grants and contributions for such purposes, except as the same may be limited by Section 501(c)(4) of the Code.

FIFTH: The Corporation is not authorized to issue shares of stock.

SIXTH: The Corporation shall have no members.

SEVENTH: The powers of the Corporation shall be exercised, and its affairs conducted, by a board of directors of the Corporation (the "Board of Directors") who shall be elected by the existing Board of Directors in the manner provided for from time to time in the Bylaws of the Corporation. The number of directors may be increased or decreased pursuant to the Bylaws of the Corporation, but shall not be less than the minimum number of directors required by law.

EIGHTH: Provisions for the regulation of the internal affairs of the Corporation, including provisions for distribution of assets on dissolution or final liquidation are as follows:

A. No part of the net earnings of the Corporation shall inure to the benefit of, or be distributable to, any director or officer of the Corporation or any other private individual, except that the Corporation shall be authorized and empowered to pay reasonable compensation for services rendered to or for the Corporation and to make payments and distributions in furtherance of its purposes as described herein.

B. Notwithstanding any other provisions of these Articles of Incorporation, the Corporation shall not directly or indirectly carry on any activity which would prevent it from obtaining exemption from Federal income taxation as a corporation described in Section 501(c)(4) of the Code, or cause it to lose such exempt status.

C. The Corporation 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 Code.

D. In the event of dissolution or final liquidation of the Corporation, the remaining assets of the Corporation shall, after paying or making provision for the payment of all of the liabilities and obligations of the Corporation, be distributed as the Board of Directors shall determine for one or more exempt purposes within the meaning of Section 501(c)(4) of the Code and in accordance with applicable law and regulations.

E. To the fullest extent permitted by the Act, as now in effect or as may hereafter be amended, no officer or director of the Corporation shall be personally liable to the Corporation for monetary damages for any breach of fiduciary duty as an officer or director of the Corporation; provided, however, that such relief from liability shall not apply in any instance where such relief is inconsistent with applicable law. Subject to the provisions of the Bylaws, the Corporation shall indemnify any officer, director, or agent of the Corporation to the fullest extent permitted by and in accordance with the Act.

NINTH: The address, including street and number, of the initial registered office of the Corporation is Corporation Service Company, and the name of its initial registered agent at such address is 1090 Vermont Avenue, N.W., Washington, DC 20005.

TENTH: The name and address of the incorporator are as follows:

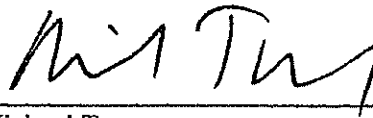
<i>Name</i>	<i>Address</i>
Michael Toner	Wiley Rein LLP 1776 K Street NW Washington, DC 20016

DATED: July 31, 2018

[SIGNATURE PAGE FOLLOWS]

**SIGNATURE PAGE TO
ARTICLES OF INCORPORATION
of
DEFENDING DIGITAL CAMPAIGNS, INC.**

IN WITNESS WHEREOF, the undersigned has executed these Articles of Incorporation
as of the date set forth above.

A handwritten signature in black ink, appearing to read "Michael Toner", written over a horizontal line.

Michael Toner
Incorporator

APPENDIX B

ORGANIZATIONAL ACTION TAKEN BY WRITTEN CONSENT
of
THE BOARD OF DIRECTORS
of
DEFENDING DIGITAL CAMPAIGNS, INC.

The undersigned, being and constituting all of the members of the Board of Directors of Defending Digital Campaigns, Inc. (the "Corporation"), a District of Columbia nonprofit corporation, for purposes of taking action in lieu of an organizational meeting of the Board of Directors, pursuant to Section 29-402.05 of the District of Columbia Nonprofit Corporation Act of 2010, hereby adopt the following resolutions and waive all requirements of notice.

Adoption of Bylaws

WHEREAS, the Articles of Incorporation of the Corporation were filed with the Department of Consumer and Regulatory Affairs of the District of Columbia as of July 31, 2018; and

WHEREAS, the Bylaws of the Corporation, attached hereto as Exhibit A, have been presented to the Board of Directors of the Corporation (the "Board"), it hereby is:

RESOLVED, that the Bylaws are adopted in their entirety and ordered to be made a permanent part of the records of the Corporation.

Election of Officers

WHEREAS, the election of officers of the Corporation is to be undertaken by the Board as specified in the Bylaws, it hereby is:

RESOLVED, that the following persons are elected to the office set forth opposite their names until their respective successors are elected, or until their prior resignation or removal:

<i>Name of Officer</i>	<i>Corporate Office</i>
Robert Mook	President
Matthew Rhoades	Treasurer

Adoption of Governance Policies

WHEREAS, the Board has determined it is in the best interests of the Corporation to adopt certain governance policies,

WHEREAS, the Conflict of Interest Policy, Whistleblower Policy, Document Retention Policy, and Compensation Review Policy attached hereto as Exhibits B, C, D, and E were presented to the Board, it hereby is:

RESOLVED, that each of the Conflict of Interest Policy, Whistleblower Policy, and Document Retention Policy is hereby approved and adopted in its entirety, and ordered to be inserted in the minute book of the Corporation.

Other Organizational Actions

WHEREAS, the following organizational actions of the Corporation have been reviewed by the Board, and the Board deems it is advisable and in the best interests of the Corporation to take the following actions, it hereby is:

RESOLVED, that the officers of the Corporation shall make such filings and take such actions as may be necessary to cause the Corporation to make an election to be exempt from tax pursuant to Section 501(c)(4) of the Internal Revenue Code of 1986, as amended; and it is

FURTHER RESOLVED, that the accounting and tax year of the Corporation shall be the calendar year, unless otherwise determined by resolution of the Board at a later date pursuant to the provisions of the Bylaws; and it is

FURTHER RESOLVED, that the officers of the Corporation are hereby authorized to pay all fees and expenses incident to and necessary for the organization of the Corporation; and it is

FURTHER RESOLVED, that the President and Treasurer of the Corporation be, and are hereby authorized to open such bank accounts in the name of the Corporation in such bank or banks such officers shall determine necessary for the deposit of funds belonging to the Corporation, such funds to be withdrawn only by check of the Corporation and other orders for the payment of money drawn in the name of the Corporation when signed by an officer of the Corporation; and it is

FURTHER RESOLVED, that the officers of the Corporation are hereby authorized to exercise all such powers of the Corporation and take all such lawful acts that they deem necessary to implement the foregoing resolutions of the Corporation that are not by law, by the Certificate of Incorporation, or by the Bylaws of the Corporation reserved or required to be exercised or done by the Board of Directors; and it is

FURTHER RESOLVED, that all activities and actions taken and documents executed heretofore by any incorporator, director or officer of the Corporation in connection with the organization and operation of the Corporation are hereby ratified, confirmed and approved in all respects.

This action by written consent may be signed in any number of counterparts, all of which when taken together will constitute one and the same document.

Dated: August 1, 2018

[SIGNATURE PAGE FOLLOWS]

**SIGNATURE PAGE TO
ORGANIZATIONAL ACTION TAKEN BY WRITTEN CONSENT
of
THE BOARD OF DIRECTORS
of
DEFENDING DIGITAL CAMPAIGNS, INC.**

IN WITNESS WHEREOF, the undersigned have executed this Written Consent,
effective as of the date set forth above.



Robert Mook
Director

Matthew Rhoades
Director

Debora Plunkett
Director

**SIGNATURE PAGE TO
ORGANIZATIONAL ACTION TAKEN BY WRITTEN CONSENT
of
THE BOARD OF DIRECTORS
of
DEFENDING DIGITAL CAMPAIGNS, INC.**

IN WITNESS WHEREOF, the undersigned have executed this Written Consent,
effective as of the date set forth above.

Robert Mook
Director



Matthew Rhodes
Director

Debora Plunkett
Director

**SIGNATURE PAGE TO
ORGANIZATIONAL ACTION TAKEN BY WRITTEN CONSENT
of
THE BOARD OF DIRECTORS
of
DEFENDING DIGITAL CAMPAIGNS, INC.**

IN WITNESS WHEREOF, the undersigned have executed this Written Consent,
effective as of the date set forth above.

Robert Mook
Director

Matthew Rhoades
Director

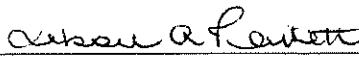

Debora Plunkett
Director

EXHIBIT INDEX

Exhibit A	Bylaws
Exhibit B	Conflict of Interest Policy
Exhibit C	Whistleblower Policy
Exhibit D	Document Retention Policy
Exhibit E	Compensation Review Policy

EXHIBIT A

Bylaws
(see attached)

BYLAWS
of
DEFENDING DIGITAL CAMPAIGNS, INC.

(formed under the District of Columbia
Nonprofit Corporation Act of 2010)

(adopted August 1, 2018)

ARTICLE I

Name and Location

Section 1.01 *Name*. The name of the corporation (the “Corporation”) is Defending Digital Campaigns, Inc.

Section 1.02 *Location*. The principal office of the Corporation shall be located at such location within or without the District of Columbia as the Board of Directors shall determine. The Corporation may maintain additional offices at such other places as the Board of Directors may determine from time to time.

Section 1.03 *Registered Office and Agent*. The Corporation shall continuously maintain a registered office and agent within the District of Columbia at such place as may be designated by the Board of Directors. The Corporation’s initial registered office and agent are set forth in the Articles of Incorporation.

ARTICLE II

Purposes

The Corporation is organized as a social welfare organization within the meaning of Section 501(c)(4) of the Internal Revenue Code of 1986, as now in effect or as hereafter may be amended. The purposes for which the Corporation is formed are 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. In addition to the foregoing, the Corporation may carry on any other social welfare (within the meaning of Internal Revenue Code Section 501(c)(4)) activity which is consistent with the other provisions of these Bylaws and which may be lawfully carried on by a corporation organized under the District of Columbia Nonprofit Corporation Act of 2010. The Corporation 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 Code.

ARTICLE III

Board of Directors

Section 3.01 *Power of Board of Directors and Qualifications of Directors.* The business and affairs of the Corporation shall be managed by the Board of Directors.

Section 3.02 *Number of Directors.* The number of directors constituting the Board of Directors shall be no less than three (3), and the initial Board of Directors consists of the directors named in the Action by the Sole Incorporator dated July 31, 2018. The number of directors may be increased or otherwise amended from time to time by the Board of Directors.

Section 3.03 *Election of Directors.* The initial directors named by the action of the incorporator shall hold office until the next election of directors. Thereafter, directors shall be elected by the Board of Directors at the Board of Directors annual meeting subject to the term described herein.

Section 3.04 *Term of Directors.* The term of a Director shall be one year. Notwithstanding the foregoing, the term of any director shall not end until the date the term begins for any directors elected in his or her stead (or until the Board of Directors expressly votes to eliminate such director position).

Anyone elected to fill a vacancy for a Director, from whatever cause arising, shall serve only for the remainder of the term of the Director whose death, removal or resignation created the vacancy. Any new Director elected or appointed pursuant to Section 3.03 (not to fill a vacancy) at a time other than a Board of Directors annual meeting shall serve a term of one year or less commensurate with the term of the other Directors then elected.

Section 3.05 *Removal and Resignations.* A director may be removed with or without cause at any time by a majority vote of the Board of Directors. Any director may resign at any time upon written notice to the Board of Directors.

Section 3.06 *Vacancies.* Any vacancy occurring in the Board of Directors for any reason may be filled by the Board of Directors as specified in Sections 3.03 and 3.04.

Section 3.07 *Quorum of Board of Directors and Action of the Board of Directors.* Unless a greater proportion is required by law, the presence of a majority of the directors shall constitute a quorum for the transaction of business and, except as otherwise provided by law or by the Articles of Incorporation or these Bylaws, the majority vote of the directors present at the meeting at which a quorum is present shall be the act of the Board of Directors.

Section 3.10 *Meetings of the Board of Directors.* Annual or other meetings of the Board of Directors may be held at any time upon call of a majority of all directors or at least three (3) directors, whichever is fewer. A meeting of the Board of Directors may be held at such time and place within or without the District of Columbia as may be determined by the Board of Directors and shall be set forth in the notice for such meeting. Notice of all meetings shall be delivered in writing to all directors at least one (1) business day before such meeting. Such notice requirement may be waived in writing before, at or after such meeting and the participation of any director in any meeting, other than an appearance solely to object to the lack or form of notice, shall be deemed such a waiver. Notice of any meeting may be delivered personally, by facsimile or by electronic or regular mail.

Section 3.11 *Informal Action by the Board of Directors; Meetings by Telephone Conference.* Any action required or permitted to be taken by the Board of Directors may be taken without a meeting if all directors consent in writing thereto. The resolution and the written consents thereto by the directors shall be filed with the minutes of proceedings of the Board of Directors. Any one or more directors may participate in a meeting of the Board of Directors by means of telephone conference or similar communications equipment by means of which all persons participating in the meeting can communicate with one another. Participation in a meeting by such means shall constitute presence in person at the meeting.

Section 3.12 *Compensation of Directors.* The Corporation may not pay any compensation to directors for their services rendered as directors, but the Corporation may reimburse directors for expenses incurred in the performance of their duties to the Corporation. Directors may receive reasonable compensation for serving the Corporation in any other capacity, including without limitation as an officer of the Corporation.

ARTICLE IV

Committees

Section 4.01 *Board Committees.* The Board of Directors, by resolution passed by a majority of the directors, may designate one or more committees, each of which shall consist of two or more directors only, which committees, to the extent provided in such resolution, shall have and may exercise the authority of the Board of Directors in the management of the Corporation. Each such committee and each member thereof shall serve at the pleasure of the Board of Directors. The designation of any such committee and the delegation thereto of authority shall not alone relieve any director of his duty under law to the Corporation. The proceedings and meetings of any such committee shall be governed by the rules for meetings of the Board of Directors.

Section 4.02 *Advisory Committee.* The Advisory Committee shall serve as an advisory body to the Board of Directors and the Corporation's officers, and shall be composed of persons who are knowledgeable about cybersecurity and election processes, and are supportive of the Corporation's mission and programs. The Advisory Committee is invited and encouraged to offer advice and guidance as to the policies and activities of the Corporation. The Advisory Committee shall not have or purport to exercise any powers of the Board of Directors nor shall it have the power to bind the Corporation in any manner. Members of the Advisory Committee shall be appointed by the Board of Directors.

ARTICLE V

Officers and Agents

Section 5.01 *Officers.* The Board of Directors shall elect a President and Treasurer, and it may also elect one or more other officers and may give any of them such further designation or alternate titles as it considers desirable. Any two or more offices may be held by the same person.

Section 5.02 *Election and Term of Office*. Each officer shall hold office for the term for which he is elected or appointed and until his successor is elected or appointed and qualified or until his earlier death, resignation or removal.

Section 5.03 *Removal and Resignations*. The Board of Directors may remove any officer at any time with or without cause. Any officer may resign at any time by giving written notice to the Board of Directors. Any resignation shall take effect at the time specified therein, and unless otherwise specified therein no acceptance of such resignation shall be necessary to make it effective.

Section 5.04 *Vacancies*. Any vacancy in any office may be filled by the Board of Directors. An officer appointed or elected to fill a vacancy shall hold office for the unexpired term of his predecessor in office, and until his successor is elected and qualified, or until his earlier death, resignation or removal.

Section 5.05 *Powers and Duties of Officers*. Subject to the control of the Board of Directors, all officers as between themselves and the Corporation shall have such authority and perform such duties in the management of the Corporation as may be provided by the Board of Directors and, to the extent not so provided, as generally pertain to their respective offices.

President. The President shall preside at meetings of the Board of Directors unless otherwise designated by the Board and shall serve as the chief executive officer of the Corporation. The President shall supervise and control all of the affairs of the Corporation in accordance with policies and directives approved by the Board of Directors. The President shall be a designated agent of the Corporation for the purpose of signing all Corporation documents. The President shall also be responsible for the keeping of an accurate record of the proceedings of all meetings of the Board of Directors, and shall give or cause to be given all notices in accordance with these Bylaws or as required by law.

Treasurer. The Treasurer shall have the custody of, and be responsible for, all funds and securities of the Corporation. The Treasurer shall keep or cause to be kept complete and accurate accounts of receipts and disbursements of the Corporation, and shall deposit all monies and other valuable property of the Corporation in the name and to the credit of the Corporation in such banks or depositories, as the Board of Directors may designate, within 10 days of receipt by the Corporation. Whenever required by the Board of Directors, the Treasurer shall render a statement of accounts. The Treasurer shall at all reasonable times exhibit the books and accounts to any officer or director of the Corporation, and shall perform all other duties incident to the office of Treasurer. The Treasurer shall be a designated agent of the Corporation for the purpose of signing all Corporation documents.

Section 5.06 *Agents and Employees*. The Board of Directors may appoint agents and employees who shall have such authority and perform such duties as may be prescribed by the Board of Directors. The Board of Directors may remove any agent or employee at any time with or without cause. Removal without cause shall be without prejudice to such person's contract rights, if any, and the appointment of such person shall not itself create contract rights.

Section 5.07 *Compensation of Officers, Agents, and Employees.* The Corporation may pay compensation to officers for services rendered to the Corporation in their capacity as officers, and officers may be reimbursed for expenses incurred in the performance of their duties to the Corporation, in reasonable amounts as approved by a majority of the Board of Directors. The Corporation may pay compensation in reasonable amounts to agents and employees for services rendered, such amounts to be fixed by the Board of Directors or, if the Board of Directors delegates power to any officer or officers, then by such officer or officers.

ARTICLE VI

Miscellaneous

Section 6.01 *Prohibited Activities.*

(a) *Actions Jeopardizing Tax Status.* This Corporation shall not carry on any activities not permitted to be carried on by an organization exempt from federal income taxes under Section 501(c)(4) of the Internal Revenue Code of 1986, as amended, or the corresponding provision of any future United State internal revenue law.

(b) *Private Inurement.* No part of the net income or net assets of the Corporation shall inure to the benefit of, or be distributable to, its directors, officers, members or other private persons. However, the Corporation is authorized to pay reasonable compensation for services actually rendered and to make payments and distributions in furtherance of its tax-exempt purposes

Section 6.02 *Fiscal Year.* The fiscal year of the Corporation shall be the calendar year, or such other period as may be fixed by the Board of Directors.

Section 6.03 *Checks, Notes, Contributions, Contracts.* The Board of Directors shall determine who shall be authorized from time to time on the Corporation's behalf to (a) sign checks, drafts, or other orders for payment of money; (b) to sign acceptances, notes, or other evidences of indebtedness; (c) to enter into contracts; or (d) to execute and deliver other documents and instruments.

Section 6.04 *Books and Records.* The Corporation shall keep correct and complete books and records of account, the activities and transactions of the Corporation, minutes of the proceedings of the Board of Directors and any committee of the Corporation, and a current list of the directors and officers of the Corporation.

Section 6.05 *Amendment of Articles of Incorporation and Bylaws.* The Articles of Incorporation and these Bylaws of the Corporation may be adopted, amended, or repealed in whole or in part by action of a majority of the Board of Directors.

Section 6.06 *Financial Statements and Reports.* An independent auditor appointed or approved by the Board shall at such times, if and as the Board determines, prepare for the Corporation as a whole a consolidated financial statement, including a statement of combined capital assets and liabilities, a statement of revenues, expenses and distributions, a list of projects and/or organizations to or for which funds were used or distributed, and such other additional reports or information as may be ordered from time to time by the Board. The auditor may also

prepare such financial data as may be necessary for returns or reports required by the state or federal government to be filed by the Corporation. The auditor's charges and expenses shall be proper expenses of administration.

Section 6.07 Indemnification and Insurance. The Corporation shall indemnify any director, officer, employee or agent, any former director, officer, employee or agent against expenses (including attorneys' fees), judgments, fines and amounts paid in settlement, actually and reasonably incurred by him in connection with any threatened, pending or completed action, suit or proceeding (whether civil, criminal, administrative, or investigative) to which he may be or is made a party by reason of being or having been such director, officer, employee or agent if he acted in good faith and in a manner he reasonably believed to be in or not opposed to the best interests of the Corporation. However, there shall be no indemnification in respect of any claim, issue or matter as to which he shall have been adjudged to be liable to the Corporation for damages arising out of his gross negligence or willful misconduct.

The Corporation may advance expenses to, or where appropriate may itself, at its expense, undertake the defense of, any director, officer, employee or agent; provided that such director, officer, employee or agent shall undertake to repay such expense if it should be ultimately determined that he is not entitled to indemnification under this Section.

The indemnification and advancement of expenses provided by this Section shall not be deemed exclusive of any other rights to which such director, officer, employee or agent may be entitled under any statute, Bylaw, agreement, vote of disinterested directors or otherwise, and shall not restrict the power of the Corporation to make any indemnification permitted by law.

The Board of Directors may authorize the purchase of insurance on behalf of any person who is or was a director, officer, employee, or agent of the Corporation, against any liability asserted against or incurred by him in any such capacity, or which arises out of such person's status as a director, officer, employee, or agent whether or not the Corporation would have the power to indemnify such person against that liability under law.

The rights to indemnification set forth in this Section are expressly conditioned upon such rights not violating the Corporation's status as a tax-exempt organization described in Section 501(c)(4) of the Internal Revenue Code of 1986, as amended.

If any part of this Section shall be found invalid or ineffective, the validity and effectiveness of the remaining parts shall not be affected thereby.

Section 6.08 Dissolution. The Corporation may be dissolved at any time by majority vote of the directors then in office. Upon the dissolution or winding up of the Corporation, or in the event it shall cease to engage in carrying out the purposes and goals set forth in these Bylaws, all of the business, properties, assets and income of the Corporation remaining after payment, or provision for payment, of all debts and liabilities of this Corporation, shall be distributed as the Board of Directors shall determine for one or more exempt purposes within the meaning of Sections 501(c)(4) of the Internal Revenue Code of 1986, as amended, and in accordance with applicable law and regulations

EXHIBIT B

Conflict of Interest Policy
(see attached)

DEFENDING DIGITAL CAMPAIGNS, INC.
(the “Organization”)

Conflict of Interest Policy

I. Purpose

The purpose of this conflict of interest policy is to protect the Organization’s interests as a tax-exempt, nonprofit and social welfare organization when it is contemplating entering into a transaction or arrangement that might benefit the private interest of an officer or director of the Organization or might possibly result in an excess benefit transaction. This policy is intended to supplement but not replace any applicable state and federal laws governing conflict of interest applicable to nonprofit organizations.

II. Definitions

- A. Interested Person** – Any director, principal officer, or member of a committee with board of directors delegated powers, who has a direct or indirect financial interest, as defined below, is an interested person.
- B. Financial Interest** – A person has a financial interest if the person has, directly or indirectly, through business, investment, or family:
 - 1. An ownership or investment interest in any entity with which the Organization has a transaction or arrangement;
 - 2. A compensation arrangement with the Organization or with any entity or individual with which the Organization has a transaction or arrangement; or
 - 3. A potential ownership or investment interest in, or compensation arrangement with, any entity or individual with which the Organization is negotiating a transaction or arrangement.

Compensation includes direct and indirect remuneration as well as gifts or favors that are not insubstantial. A financial interest is not necessarily a conflict of interest. Under Section III(B), a person who has a financial interest may have a conflict of interest only if the board of directors or committee with board of directors delegated powers decides that a conflict of interest exists.

III. Procedures

- A. Duty to Disclose** – In connection with any actual or possible conflict of interest, an interested person must disclose on an ongoing basis the existence of the financial interest and be given the opportunity to disclose all material facts to the directors and members of committees with board of directors delegated powers considering the proposed transaction or arrangement.

B. Determining Whether a Conflict of Interest Exists – After disclosure of the financial interest and all material facts, and after any discussion with the interested person, he/she shall leave the board of directors or committee with board of directors delegated powers meeting while the determination of a conflict of interest is discussed and voted upon. The remaining board or committee members shall decide if a conflict of interest exists.

C. Procedures for Addressing the Conflict of Interest

1. An interested person may make a presentation at the board of directors or committee with board of directors-delegated powers meeting, but after the presentation, he/she shall leave the meeting during the discussion of, and the vote on, the transaction or arrangement involving the possible conflict of interest.
2. The President of the Organization or chairperson of the committee with board of directors-delegated powers shall, if appropriate, appoint a disinterested person or committee to investigate alternatives to the proposed transaction or arrangement.
3. After exercising due diligence, the board of directors or committee with board of directors delegated powers shall determine whether the Organization can obtain with reasonable efforts a more advantageous transaction or arrangement from a person or entity that would not give rise to a conflict of interest.
4. If a more advantageous transaction or arrangement is not reasonably possible under circumstances not producing a conflict of interest, the board of directors or committee with board of directors delegated powers shall determine by a majority vote of the disinterested directors whether the transaction or arrangement is in the Organization's best interest, for its own benefit, and whether it is fair and reasonable. In conformity with the above determination it shall make its decision as to whether to enter into the transaction or arrangement.

D. Violations of the Conflict of Interest Policy

1. If the board of directors or committee with board of directors-delegated powers has reasonable cause to believe a member has failed to disclose an actual or possible conflict of interest, it shall inform the member of the basis for such belief and afford the member an opportunity to explain the alleged failure to disclose.
2. If, after hearing the member's response and after making further investigation as warranted by the circumstances, the board of directors or committee with board of directors delegated powers determines the

member has failed to disclose an actual or possible conflict of interest, it shall take appropriate disciplinary and corrective action.

IV. Records of Proceedings

The minutes of the board of directors and all committees with board of directors-delegated powers shall contain:

- A. The names of the persons who disclosed or otherwise were found to have a financial interest in connection with an actual or possible conflict of interest, the nature of the financial interest, any action taken to determine whether a conflict of interest was present, and the decision of the board of directors or committee with board of directors delegated powers as to whether a conflict of interest in fact existed; and
- B. The names of the persons who were present for discussions and votes relating to the transaction or arrangement, the content of the discussion (including any alternatives to the proposed transaction or arrangement), and a record of any votes taken in connection with the proceedings.

V. Compensation

- A. A director who receives compensation, directly or indirectly, from the Organization for services is precluded from voting on matters pertaining to that director's compensation.
- B. A voting member of any committee with board of directors-delegated powers whose jurisdiction includes compensation matters and who receives compensation, directly or indirectly, from the Organization for services is precluded from voting on matters pertaining to that member's compensation.
- C. No director or voting member of any committee with board of directors delegated-powers whose jurisdiction includes compensation matters and who receives compensation, directly or indirectly, from the Organization, either individually or collectively, is prohibited from providing information to any such committee regarding compensation.

VI. Annual Statements

Each director, principal officer, and member of a committee with board of directors-delegated powers shall annually sign a statement which affirms such person:

- A. Has received a copy of the conflict of interest policy;
- B. Has read and understands the policy;
- C. Has agreed to comply with the policy; and

- D.** Understands the Organization is a nonprofit, social welfare organization and in order to maintain its federal tax exemption it must engage primarily in activities which accomplish one or more of its tax-exempt purposes.

VII. Periodic Reviews

To ensure the Organization operates in a manner consistent with its social welfare purposes and does not engage in activities that could jeopardize its tax-exempt status, periodic reviews shall be conducted. The periodic reviews shall, at a minimum, include the following subjects:

- i.** Whether compensation arrangements and benefits are reasonable, based on competent survey information, and the result of arm's length bargaining; and
- ii.** Whether partnerships, joint ventures, and arrangements with management organizations conform to the Organization's written policies, are properly recorded, reflect reasonable investment or payments for goods and services, further the social welfare purposes of the Organization and do not result in inurement, impermissible private benefit or in an excess benefit transaction.

VIII. Use of Outside Experts

When conducting the periodic reviews pursuant to Section VII, the Organization may, but need not, use outside advisors. If outside experts are used, their use shall not relieve the board of directors of its responsibility for ensuring periodic reviews are conducted.

DEFENDING DIGITAL CAMPAIGNS, INC.

Annual Conflict of Interest Disclosure Statement

I hereby acknowledge that I have received a copy of Defending Digital Campaigns, Inc.'s Conflict of Interest Policy ("Policy") and that I have read and understand its terms. I understand that Defending Digital Campaigns, Inc. is a nonprofit, social welfare organization and in order to maintain its federal tax exemption it must engage primarily in activities which accomplish one or more of its tax-exempt purposes. To the best of my knowledge, except as disclosed below, I do not have a Conflict of Interest, as defined in the Policy, requiring disclosure under the Policy.

☐ Without exception

☐ Except as described below

Disclosure of Financial Interest that may give rise to a Conflict of Interest (a written statement may be attached if additional space is needed):

If any situation should arise in the future which I believe may or does pose a Conflict of Interest, I will promptly disclose the applicable Financial Interest in writing to the President.

By signing below I indicate my agreement to comply with the terms of the Policy and of this Disclosure Statement.

Signature: _____

Print Name: _____

Date: _____

EXHIBIT C

Whistleblower Policy
(see attached)

DEFENDING DIGITAL CAMPAIGNS, INC.

Whistleblower Policy

This Whistleblower Policy (1) encourages Defending Digital Campaigns, Inc. (the "Corporation") staff and volunteers to come forward with information on possible illegal practices or serious violations of adopted policies of the Corporation; (2) specifies that the Corporation will protect any such person from retaliation; and (3) identifies where and how such information can be reported.

- 1. Encouragement of Reporting.** The Corporation encourages complaints, reports, or inquiries about possible illegal practices or serious violations of the Corporation's policies, including illegal or improper conduct by the Corporation itself, by its leadership, or by others on its behalf. Appropriate subjects to raise under this policy would include financial improprieties, accounting or audit matters, ethical violations, or other similar illegal or improper practices.
- 2. Protection from Retaliation.** The Corporation prohibits retaliation by or on behalf of the organization against staff or volunteers who make good-faith complaints, reports, or inquiries under this policy or who participate in a review or investigation under this policy. This protection extends to those whose allegations are made in good faith but prove to be mistaken. The Corporation reserves the right to discipline persons who make bad faith, knowingly false, or vexatious complaints, reports, or inquiries or who otherwise abuse this policy.
- 3. Where to Report.** Complaints, reports, or inquiries may be made under this policy on a confidential or anonymous basis. Complaints should describe in detail the specific facts demonstrating the bases for the complaints, reports, or inquiries. Complaints may be directed to the Corporation's President; if this person is implicated in the complaint, report, or inquiry, then it should be directed to any other member of the Corporation's board of directors. The Corporation will conduct a prompt, discreet, and objective review or investigation. Staff or volunteers must recognize that the Corporation may be unable to fully evaluate a vague or general complaint, report, or inquiry that is made anonymously.

EXHIBIT D

Document Retention Policy
(see attached)

DEFENDING DIGITAL CAMPAIGNS, INC.

Document Retention and Destruction Policy

This Document Retention and Destruction Policy identifies the record retention responsibilities of directors, officers, staff, volunteers, and outside agents and vendors of Defending Digital Campaigns, Inc. (the "Corporation") for maintaining and documenting the storage and destruction of the Corporation's paper and electronic documents and records.

1. **Rules.** The Corporation's directors, officers, staff, consultants, vendors, and volunteers are required to honor the following rules:
 - a. All documents or records containing information concerning the Corporation should be closely guarded and considered as containing confidential information not to be disseminated or distributed outside of the Corporation.
 - b. No paper or electronic documents will be destroyed or deleted if pertinent to any ongoing or anticipated government investigation or proceeding or any civil or criminal judicial proceeding.
 - c. Paper or electronic documents listed for retention below will be transferred and maintained by the President or his designee.
 - d. All other paper documents that do not fall under the retention schedule below will be destroyed after three years.
 - e. All other electronic documents that are not currently being used and do not fall under the retention schedule below will be deleted from all individual computers, databases, networks, and back-up storage after one year.
2. **Retain Permanently**
 - a. **Governance records** – Articles of Incorporation and Bylaws, and any amendments thereto, other organizational documents, governing board and committee written consents and minutes.
 - b. **Tax records** – Filed federal and state tax returns/reports and supporting records, application for tax exemption, tax exemption determination letter and related correspondence, and any files related to tax audits.
 - c. **Intellectual property records** – Copyright and trademark registrations and samples of protected works.
 - d. **Audit and Financial Records** – Audited financial statements, attorney contingent liability letters.

- e. **Pension and benefit records** – Pension (ERISA) plan participant/beneficiary records, actuarial reports, related correspondence with government agencies, and supporting records.
- f. **Insurance records** – Expired insurance policies, insurance records, accident reports, claims, etc.

3. Retain for 10 Years

- a. **Government relations records** – Federal and state lobbying and political contribution reports and supporting records.

3. Retain for 7 Years

- a. **Employment Records/Personnel Files** – Employee names, addresses, social security numbers, dates of birth, INS Form 1-9, resume/application materials, job descriptions, dates of hire and termination/separation, employment agreements, evaluations, compensation information, promotions, transfers, disciplinary matters, time/payroll records, leave/comp time/FMLA, engagement and discharge correspondence, documentation of basis for independent contractor status, independent contractor agreements (retain for all current employees and independent contractors and for seven years after the departure of each individual).

4. Retain for 3 Years

- a. **Employment Applications** – Resume/application materials for individuals who did not become employees.
- b. **Lease, Contract, and License Records** – Software license agreements, vendor, hotel, and service agreements, consultant agreements, and all other agreements (retain during the term of the agreement and for three years after the termination, expiration, or non-renewal of each agreement).
- c. **Banking Records** – Bank reconciliations, bank statements, deposit slips, checks.

5. Retain for 1 Year

All other pertinent electronic records, documents, and files, such as correspondence files, publications, survey information.

6. Exceptions

Any exceptions to these rules and the terms for retention may be granted only by the Corporation's President or Board of Directors in writing.

EXHIBIT E

Compensation Review Policy
(see attached)

DEFENDING DIGITAL CAMPAIGNS, INC.
(the "Organization")

Compensation Review Policy

This Compensation Review Policy applies to the Organization's Chief Employed Executive, Officers, Key Employees, and Disqualified Persons. The purpose of this policy is to ensure the Organization does not engage in any "excess benefit transaction" as defined in Section 4958 of the Internal Revenue Code ("I.R.C.") and regulations promulgated thereunder.¹

1. Definitions

- a. **Chief Employed Executive** – The chief executive officer, executive director, or top management official (i.e., the employee who has ultimate responsibility for implementing the decisions of the Organization's governing body or for supervising the management, administration, or operations of the Organization).
- b. **Officer** – A person elected or appointed to manage the Organization's daily operations, such as a president, vice president, secretary, or treasurer. The officers of the Organization are determined by reference to its organizing document, bylaws, or resolutions of its governing body, or as otherwise designated consistent with state law, but at a minimum include those officers required by applicable law. The Organization's top management official and top financial official (the person who has ultimate responsibility for managing the Organization's finances) are included as officers.
- c. **Key Employee** – An employee of the Organization who meets all three of the following tests: (a) *\$100,000 Test* – receives reportable compensation from the Organization and all related organizations in excess of \$100,000 for the year; (b) *Responsibility Test* – the employee (i) has responsibility, powers, or influence over the Organization as a whole that is similar to those of officers, directors, or trustees, (ii) manages a discrete segment or activity of the Organization that represents 10% or more of its activities, assets, income, or expenses of the Organization, as compared to the Organization as a whole, or (iii) has or shares authority to control or determine 10% or more of the Organization's capital expenditures, operating budget, or compensation for employees; and (c) *Top 20 Test* – is one of the 20 employees (that satisfy the \$100,000 Test and Responsibility Test) with the highest reportable compensation from the Organization and related organizations for the year.
- d. **Disqualified Person** – Any person (including any management company or entity acting as a consultant or independent contractor) in a position to exercise substantial influence over the affairs of the organization. To be a disqualified person, it is not necessary that the person *actually* exercise substantial influence,

¹ See *An Introduction to I.R.C. 4958 (Intermediate Sanctions)* by Lawrence M. Brauer, Toussaint T. Tyson, Leonard J. Henzke and Debra J. Kawecki, (2002 EO CPE Text, page 259) (the "Introduction to I.R.C. 4958").

only that the person *be in a position to* exercise substantial influence. (See Treas. Reg. 53.4958-3T).

2. Compensation Review Process

- a. **Review and Approval.** The compensation of the Chief Employed Executive and each Officer, Key Employee or Disqualified Person shall be reviewed and approved by the board of directors or compensation committee of the Organization, provided that directors or other persons with conflicts of interest with respect to the compensation arrangement at issue shall not be involved in this review and approval.
- b. **Use of Comparable Compensation Data.** The compensation of the Chief Employed Executive and each Officer, Key Employee or Disqualified Person shall be reviewed and approved using data as to comparable compensation for similarly qualified persons in functionally comparable positions at similarly situated organizations.
- c. **Contemporaneous Documentation and Recordkeeping.** There shall be contemporaneous documentation and recordkeeping with respect to the deliberations and decisions regarding the compensation arrangement. The board of directors or compensation committee evaluating such compensation arrangement may, but shall not be required, to use the “Rebuttable Presumption Checklist” or other tools set forth in the Introduction to I.R.C. 4958.

Exhibit B

Advisory Opinion 2018-12 (Defending Digital Campaigns, Inc.)



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-rohrbacher-opponent-cyberattack-hack/index.html>; Holley Long, *Campaign: Russians Attempted to Hack AL Congressional Candidate’s Website*, WFSB-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. AOR005. 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 committees⁷ 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 through 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,

A handwritten signature in blue ink that reads "Ellen L. Weintraub". The signature is fluid and cursive, with a long horizontal flourish extending to the right.

Ellen L. Weintraub
Chair