



*U.S. ELECTION ASSISTANCE COMMISSION  
633 3rd St. NW, Suite 200  
Washington, DC 20001*

**RECEIVED**

By OGC/CELA at 4:27 pm, Feb 02, 2022

February 2, 2022

Federal Election Commission  
Office of Complaints Examination  
& Legal Administration  
Attn: Trace Keeyes, Paralegal  
1050 First Street, NE  
Washington, DC 20463

***RE: MUR 7946***

Dear Ms. Keeyes,

This response is submitted by the undersigned counsel on behalf of the U.S. Election Assistance Commission (EAC), Mona Harrington, in her official capacity as Executive Director of the EAC, and Paul Repak, in his official capacity as Finance Director of the EAC, (collectively, "Respondents") in connection with MUR 7946.

Complainant has presented no credible facts nor made any specific allegations against Respondents of a violation of law within the jurisdiction of the Federal Election Commission (Commission). Nevertheless, based on our understanding of the wide-ranging allegations, which rely on conjecture while ignoring evidence available in the public record, the Complaint appears to allege that 1) Respondents made, and failed to report, contributions to unspecified candidates and candidate committees through a third-party contractor using public funds; 2) CTCL made coordinated expenditures on behalf of unspecified candidates with funding from a private, third party because Respondents failed to properly exercise their oversight role; and 3) the EAC exceeded its statutory authority to serve as a national clearinghouse on election administration.

Based on the Response below, the Commission should find no reason to believe that Respondents violated the Act. First, Respondents hired a contractor, the Center for Tech & Civic Life (CTCL), for the sole purpose of designing a cybersecurity training module for state and local election officials to use as a resource in planning the 2020 elections.

Separately, in early 2020, Congress appropriated \$400 million and designated the EAC to distribute and account for these funds to state and local authorities to conduct safe and secure elections during the COVID pandemic. In Fiscal Year 2020, Congress also appropriated \$425 million in election grant funding for states to strengthen their cybersecurity posture in the upcoming election year.

Second, the Complaint misapplies the coordination provisions of the Commission's regulations, and nevertheless fails to specify a violation. Finally, the agency's development and distribution of election resources, which proved crucial to a successful 2020 election, falls under its statutory clearinghouse function.

## **I. Factual Background**

### **A. EAC, CTCL, and Statement of Work**

Under the Help America Vote Act of 2002 (HAVA),<sup>1</sup> Congress established the EAC as an independent, bipartisan commission charged with developing guidance to meet HAVA requirements, adopting voluntary voting system guidelines,<sup>2</sup> and serving as a national clearinghouse of information on election administration.<sup>3</sup> EAC also accredits testing laboratories and certifies voting systems,<sup>4</sup> as well as audits the use of HAVA funds.<sup>5</sup>

CTCL is a 501(c)(3) charitable organization based in Chicago, Ill.<sup>6</sup> Its mission is “to increase civic participation by modernizing engagement between local government and the people they serve . . . by (1) educating the public about government and democracy in the United States and (2) educating local government agencies about . . . the skills, strategies, and tools to engage their citizens.”<sup>7</sup>

On May 8, 2020, EAC and CTCL signed a Statement of Work for CTCL to provide “election specific customized online cyber security training to State and local election officials throughout the country.”<sup>8</sup> The scope of the training generally sought to assist election officials ensure federal compliance of existing and new systems and technologies and to analyze security systems and operations.<sup>9</sup>

Continuing throughout FY 2021, the EAC offered online cybersecurity training developed specifically for election officials at no cost through this partnership with CTCL. The online training consisted of both video and written materials separated into three modules.<sup>10</sup> It provided foundational knowledge on cybersecurity terminology, best practices in election offices, practical application, and communication. EAC extended the course offering for six months until November 8, 2021.<sup>11</sup> During this time, a total of 1111 participants from forty-five states, Washington D.C., and three territories (U.S. Virgin Islands, Northern Mariana Islands, and American Samoa) took part in the training.<sup>12</sup>

---

<sup>1</sup> 52 U.S.C. § 20921 (2018).

<sup>2</sup> *Id.* §§ 21101, 21102.

<sup>3</sup> *Id.* § 20922.

<sup>4</sup> *Id.* § 20971(a), (b).

<sup>5</sup> *Id.* § 21025.

<sup>6</sup> CTR. FOR TECH. AND CIVIC LIFE, FORM 990 (2020), <https://www.techandcivicliflife.org/2020covidsupport/>.

<sup>7</sup> *Id.* at 2.

<sup>8</sup> See Resp. Ex. A, Statement of Work 1 (May 8, 2020).

<sup>9</sup> See *id.* (listing ten ways the training would assist election officials).

<sup>10</sup> See CTR. FOR TECH AND CIVIC LIFE, LIBRARY, <https://learn.techandcivicliflife.org/library/?category=Cybersecurity>.

<sup>11</sup> See Resp. Ex. B, Miscellaneous Obligation Request (May 17, 2021).

<sup>12</sup> See ELECTION ASSISTANCE COMM’N, 2021 ANNUAL REPORT 47 (2022).

## **B. CARES Act Funding**

On March 27, 2020, the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) was signed into law.<sup>13</sup> The Act included \$400 million in new HAVA emergency funds, made available to states to prevent, prepare for, and respond to the coronavirus for the 2020 federal election cycle.<sup>14</sup> This supplemental appropriation funding, awarded by the EAC within thirty days pursuant to the Act,<sup>15</sup> provided states with additional resources to protect the 2020 elections from the effects of the novel coronavirus.

The CARES Act provided the funds to the EAC under HAVA Section 101, which authorizes the EAC to provide funds to states to improve the administration of federal elections.<sup>16</sup> In allocating these funds, the EAC followed the requirements of Section 101, and disbursed \$397,205,287 (99.30%) of the obligated \$400,000,000 based on the requests for those funds by the states.<sup>17</sup> Some states requested less than their full allocation due to concerns over meeting the required twenty percent match.<sup>18</sup>

The funds could only be used for costs associated with the pandemic during the 2020 election season, including Presidential and Congressional primaries that took place in advance of the general election.<sup>19</sup> States must report to the EAC on how they used the funds within 20 days of each primary and after the general election.<sup>20</sup> The Commission made all funding request letters public for the election community and the American people to have the particulars on how the states and territories were planning on using their funds.<sup>21</sup>

## **C. Election Security Grants**

In Fiscal Year 2020, Congress appropriated operating funds for the agency alongside election security grants totaling \$425 million.<sup>22</sup> In their federal financial reports submitted in December 2020, states reported using these funds to respond to the pandemic, replace voting equipment, secure and modernize voter registration databases, conduct cybersecurity vulnerability assessments, implement cybersecurity best practices, and pilot and conduct postelection audits, among other uses.<sup>23</sup>

<sup>13</sup> Pub. L. No. 136-116, 134 Stat. 281 (2020).

<sup>14</sup> § 6002, 134 Stat. 530.

<sup>15</sup> § 6002, 134 Stat. 531.

<sup>16</sup> 52 U.S.C. §20901 (2018).

<sup>17</sup> See ELECTION ASSISTANCE COMM'N, 2020 ANNUAL REPORT 29 (2021); see also ELECTION ASSISTANCE COMM'N, CARES ACT QUARTERLY REPORTS TO THE PANDEMIC RESPONSE ACCOUNTABILITY COMMITTEE (Jan. 2022), [https://www.eac.gov/sites/default/files/paymentgrants/cares/PRAC%20Reports/15011\\_Quarterly\\_Report\\_on\\_CARE\\_S\\_Funding\\_January%202022.pdf](https://www.eac.gov/sites/default/files/paymentgrants/cares/PRAC%20Reports/15011_Quarterly_Report_on_CARE_S_Funding_January%202022.pdf).

<sup>18</sup> *Id.*

<sup>19</sup> Pub. L. No. 136-116, 134 Stat. 530, 531 (2020) (requiring states to return any funds that remain unobligated on December 31, 2020, to the Treasury).

<sup>20</sup> § 6022, 134 Stat. at 530.

<sup>21</sup> ELECTION ASSISTANCE COMM'N, 2020 CARES ACT GRANTS, <https://www.eac.gov/payments-and-grants/2020-cares-act-grants>.

<sup>22</sup> Consolidated Appropriations Act, 2020, Pub. L. No. 116-93, 133 Stat. 2461 (2020).

<sup>23</sup> See 2020 ANNUAL REPORT, *supra* note 17, at 25; see also ELECTION ASSISTANCE COMM'N, ELECTION SECURITY FUNDS, <https://www.eac.gov/payments-and-grants/election-security-funds>.

## II. Legal Analysis

### A. Prohibited Contributions

#### 1. Legal Background

As summarized above, the Complaint appears to allege that Respondents made, and failed to report, contributions to unspecified candidates and candidate committees through a third-party contractor using public funds. This is based on various paragraphs in the Complaint<sup>24</sup> that together, appear to claim that that Respondents made contributions in the name of another to unspecified “political candidates and campaigns”<sup>25</sup> of “one political party and its candidate(s) for U.S. President,”<sup>26</sup> with “funds from United States taxpayers.”<sup>27</sup>

The Act defines, “contribution,” as “any gift, subscription, loan, advance, or deposit of money or anything of value made by any person for the purpose of influencing any election for Federal office.”<sup>28</sup> Under the Act, “person” includes, “an individual, partnership, committee, association, corporation, labor organization, or any other organization or group of persons . . .”<sup>29</sup> Significantly, the term, “person,” excludes “the Federal Government or any authority of the Federal Government.”<sup>30</sup> Finally, the Act prohibits a person from making “a contribution in the name of another person,” or to “knowingly permit his name to be used to effect such a contribution.”<sup>31</sup>

#### 2. The EAC Did Not Make Contributions in the Name of Another Through its Partnership with CTCL

The Commission should find no reason to believe EAC violated the Act by making contributions in the name of another. First, the Act expressly excludes “the Federal Government or any authority of the Federal Government” from the definition of “person.”<sup>32</sup> Therefore, the Respondents are not “person[s]” capable of making contributions under the Act.

Second, Complainant’s allegations that the agency used an unspecified amount of public funds to contribute to candidates and committees of one political party are based on conjecture and do not identify contributions in any amounts to specific recipients. Indeed, as detailed above, Congress duly appropriated all public funds that the EAC distributed during the 2020 election,

---

<sup>24</sup> See, e.g., Compl. at 10 ¶¶ 47-53, 70-71, 77-79 (citing the Act’s prohibition of contributions by federal contractors under 52 U.S.C. § 30119, 11 C.F.R. § 115.2 and its prohibition of contributions in the name of another under 52 U.S.C. § 30122, 11 C.F.R. § 110.4).

<sup>25</sup> Compl. at 2 ¶¶ 5-6.

<sup>26</sup> *Id.* at 2 ¶ 6.

<sup>27</sup> *Id.* at 3 ¶ 7.

<sup>28</sup> 52 U.S.C. § 30101(8)(A) (2018).

<sup>29</sup> *Id.* § 30101(11).

<sup>30</sup> *Id.*

<sup>31</sup> *Id.* § 30122, 11 C.F.R. § 110.4.

<sup>32</sup> *Id.* § 30101(11).

and EAC properly exercised its oversight role through mandatory reporting.<sup>33</sup> As the publicly filed reports indicate, the Congressional appropriations are all accounted for, and none were used to make contributions through CTCL to candidates or committees.<sup>34</sup>

Finally, as detailed above, the Statement of Work clearly reflects that EAC hired CTCL to design a cybersecurity training module for state and local election officials to use as a resource in planning the 2020 elections.<sup>35</sup> Their collaboration over the next eighteen months was entirely transparent, which even the Complaint acknowledges.<sup>36</sup>

Accordingly, the Commission should find no reason to believe that Respondents used public funds to make contributions in the name of another through CTCL.

## **B. Coordination**

### **1. Legal Background**

Commission regulations define, “coordinated,” as “made in cooperation, consultation or concert with, or at the request or suggestion of, a candidate, a candidate’s authorized committee, or a political party committee.”<sup>37</sup> The regulation further establishes, “[a]ny expenditure that is coordinated . . . but that is not made for a coordinated communication . . . or a party coordinated communication . . .” is an in-kind contribution.<sup>38</sup>

### **2. Complainant Fails to Support Allegations of Coordinated Expenditures Resulting in Excessive Contributions and Reporting Violations**

The Complaint appears to allege that CTCL made coordinated expenditures on behalf of unspecified candidates with funding from a private, third party, and that Respondents’ failure to properly exercise the agency’s oversight role “has caused a single, financially powerful individual to contribute excessive amounts of political contributions. . .”<sup>39</sup>

First, the Complainant fails to identify with which candidates or committees CTCL coordinated its expenditures. Instead, the Complaint speculates that “the close associations between CTCL officers and staff to partisan politics”<sup>40</sup> provides a basis to investigate. Without this information, there is no basis to establish coordination resulting in in-kind contributions that trigger reporting obligations under the Act. Second, the Complaint fails to indicate how the EAC and its officers connect to the alleged coordination scheme, pointing only to the general “failure”

---

<sup>33</sup> See *supra* Part I.B.

<sup>34</sup> See *id.*

<sup>35</sup> See *supra* Part I.A; see also Ex. A.

<sup>36</sup> See Compl. at 11 ¶¶ 52-53 (stating “This freshly formed public-private partnership was conspicuously advertised to the public at-large on the main page of the EAC’s website throughout the federal election cycle . . .”).

<sup>37</sup> 11 C.F.R. § 109.20(a).

<sup>38</sup> *Id.* § 109.20(b).

<sup>39</sup> Compl. at 3 ¶ 10.

<sup>40</sup> *Id.* at 17 ¶ 75.

of government oversight.<sup>41</sup> Finally, even if Complainant establishes this connection, Respondents are government entities who do not constitute “person[s]” under the Act and cannot therefore make “contributions” as defined by the Act.<sup>42</sup>

Ultimately, in the absence of more credible evidence, the allegations do not warrant an investigation and the Commission should find no reason to believe Respondents made coordinated expenditures.

### **C. EAC’s Clearinghouse Mandate**

#### **1. Legal Background**

Under HAVA, the EAC “shall serve as a national clearinghouse and resource for the compilation of information and review of procedures with respect to the administration of Federal elections. . .”<sup>43</sup> related to the voluntary voting system guidelines, testing and certification of voting systems, research, information, and training on grants management.<sup>44</sup>

#### **2. The EAC’s Clearinghouse Resources Fall Within Its Statutory Mandate**

The last allegation we can discern from the Complaint appears to claim that the EAC exceeded its statutory mandate to serve as a clearinghouse of information on election administration practices.<sup>45</sup> Specifically, the Complaint identifies the EAC’s July 2020 document, “Cyber Crisis Management for Elections Officials,” as an example of the agency’s “*ultra vires*” acts outside of that agency’s authority under its enabling statute.” However, the Complaint fails to explain how preparing this guidance falls outside the scope of the EAC’s clearinghouse function, instead suggesting only that “CTLC” [sic] prepared the report in violation of HAVA.<sup>46</sup>

To be sure, HAVA provides wide discretion for the agency’s clearinghouse function. It consists of guidance documents that range from election security to election worker best practices, voting accessibility, and disaster preparedness.<sup>47</sup>

Coupled with the Complaint’s failure to establish a violation of the Act, the Commission should find no reason to believe Respondents violated the Act by preparing resources for election officials.

---

<sup>41</sup> See *id.* at 3-4 ¶¶ 10-11, 13 ¶ 11.

<sup>42</sup> See *supra* Part II.A.2.

<sup>43</sup> 52 U.S.C. § 20922 (2018).

<sup>44</sup> *Id.*

<sup>45</sup> See Compl. at 11 ¶¶ 54-57.

<sup>46</sup> See *id.* at 12 ¶¶ 56-57.

<sup>47</sup> See ELECTION ASSISTANCE COMM’N, ELECTION MANAGEMENT RESOURCES, <https://www.eac.gov/election-officials>.

MUR 7946  
Response  
Page 7 of 7

### **III. Conclusion**

Based on the foregoing, the Commission should find no reason to believe Respondents, U.S. Election Assistance Commission, Mona Harrington, in her official capacity as Executive Director of the EAC, and Paul Repak, in his official capacity as Finance Director of the EAC, 1) made, and failed to report, contributions to unspecified candidates and candidate committees through a third-party contractor using public funds; 2) CTCL made coordinated expenditures on behalf of unspecified candidates with funding from a private, third party because Respondents failed to properly exercise their oversight role; and 3) the EAC exceeded its statutory authority to serve as a national clearinghouse on election administration.


Sincerely,



Amanda Joiner  
Associate Counsel



Kevin Rayburn  
General Counsel



administrative resource center

Click here to view instructions for completing this form

**Note on Citibank Purchase Card obligations:**

(Please see CitiDirect example tab in this workbook.)

> The vendor must be **Citibank USA NA** with Supplier number **045256872**

> The invoice Approver needs to be the Approving Official (AO) designated in CitiDirect as the Cardholder's AO.

> The Cardholder's name needs to be in the description field and it is helpful to add the merchant in the description field.

Section A - Miscellaneous Obligation Request

Type of Request

☐ New Request

☒ Mod Adjustment

☐ Deobligation (Optional)

Customer NameEAC

Obligating Document #EAC-20-0049

Period of Performance

5/8/2020

-

5/8/2021

Total Amount Obligated/Adjusted

\$

345,000.00

Vendor Name/Trading PartnerCenter for Technology and Civic Life

Vendor Duns # / Supplier #050750358

Primary Invoice Approver/COR:

Robin Sargent

Phone #/Email Address

rsargent@eac.gov/ (202)360-2144

Alternate Invoice Approver/COR:

Ashley Williams

Phone #/Email Address

awilliams@eac.gov/ (202) 860-0846

Description of goods/services to be provided: (Include account # if obligation is for a utility.)

Election cybersecurity training: 3 course series for election offices

Section B - Accounting Flexfield Information

Section C - Customer Agency Authorized Requestor

(In accordance with GAO Title 7, proper documentation will be maintained by customer.)

Approved By: (print name) Mona Harrington

Approved By: (provide signature if faxing form, otherwise print name) Mona Harrington, Acting Executive

Date Approved: 5/8/20

Mona Harrington

5/8/2020

Section D - ARC Accounting Office only

Oracle Obligation #



## STATEMENT OF WORK

### OVERVIEW/BACKGROUND

**The (EAC) is an independent agency of the United States government created by the Help America Vote Act of 2002 (HAVA). The Commission serves as a national clearinghouse and resource of information regarding election administration.** Through HAVA, the EAC works to help implement sweeping election reforms, assist states in certifying voting systems, advance voting accessibility, and serve as a clearinghouse of election information and that includes training resources in the areas of both election administration and cyber security.

The EAC seeks to procure a vendor to provide its stakeholders with online training platform of best practices related to cyber security training.

The purpose of this Order is to obtain contractor training services to expeditiously provide specific election specific customized online cyber security training to State and local election officials throughout the country.

### SCOPE

This task area supports EAC's Strategic Goal 2, and 3: Build and distribute election official cyber security training materials.

As the agency moves forward in assisting election officials with cyber security training, meeting industry best practices, security mandates required by federal laws, standards, and guidance, a more advanced conceptual and continuous approach to security will be required to ensure the safeguarding of information entrusted to the election community. This Comprehensive and Robust Cyber Security Training will assist election officials with: (1) continuing to implement and update NIST-compliant policies, and procedures, (2) engineering and implementing solutions to new requirements that arise both from advances in technology and from new regulations and directives and (3) maintaining IT system resiliency with effective contingency planning, evaluation, and testing. (4) In performing gap analysis on current security infrastructure (5) ensuring consistent application of information security standards across all election information systems. (6) Integration of these regulations and standards into a fully implementable security program. (7) Ensuring preparation for internal and external audits through management of all infrastructure. (8) Ensuring all new information technology (IT) projects meet or integrate security standards into their development. (9) Develop a culture of security-minded professionals across the community. (10) Ensure information system survivability and integrity and optimize processes to meet IT security-related goals and strategies.

The EAC requires this training immediately, for election officials. We believe it is very important to offer this training now as we navigate this challenging time as election officials are responding to COVID 19 and facing unique challenges. Cyber security is of paramount importance leading to the 2020 election as election officials are working remotely and cyber threats are more prevalent in this new environment than ever before.

This cyber security training is specific to elections and is proprietary. We seek to sole source to the Center for Tech and Civic Life as the product already exists and has been evaluated by the State of Virginia and the EAC and meets all criteria listed herein.

The Center for Tech and Civic Life (CTCL) is a civic tech 501(c)(3) nonprofit that connects

Americans with the information they need to become and remain civically engaged, and helps ensure elections are professional, inclusive, and secure. With this in mind, CTCL supports election departments with industry best practices, free tech tools, and professional development courses of CTCL's core programs is delivering low-cost, online training courses to election officials across the country on a range of topics that meet the most pressing needs facing the field of election administration. In response to election cyber incidents in 2016, CTCL partnered with the Center for Democracy and Technology in 2018 to develop election cybersecurity training courses for local election departments.

CTCL's 3-course election cybersecurity curriculum is the only training content that is tailored to local U.S. election offices, especially those with limited tech resources. The courses, which took 6 months to develop, have been iterated since 2018. The content and platform is tested, effective, and ready to deploy nationwide with 1-week notice.

Election cybersecurity training overview

CTCL's election cybersecurity training is a 3-course series that empowers election offices to manage cyber threats and communicate with the public about cybersecurity. Each course covers unique content and takes about 90-minutes to complete.

#### **CYBERSECURITY 101: INTRODUCTION**

1. Understand complex cybersecurity terminology
2. Identify different types of cyber threats and responses
3. Create stronger login practices

#### **CYBERSECURITY 201: INTERMEDIATE**

1. Safeguard your election data
2. Apply National Institute of Standards and Technology cybersecurity framework to election systems
3. Develop partnerships to overcome security challenges

#### **CYBERSECURITY 301: COMMUNICATIONS**

1. Inform the public about your election office's cybersecurity leadership
2. Make a cyber incident response plan
3. Build media allies

Training costs

The **total cost for 3 courses is \$345,000** and includes

- 1 year of unlimited access to 3 courses

- 1 year of maintenance of course content
- Access to pre-course and post-course evaluation responses via cloud storage
- Daily or weekly progress reports that can be accessed via cloud storage
- Monthly check-in meetings with CTCL staff Whitney May, Dylan Lynch, and Keegan Hughes

#### Training delivery, technical support, and maintenance

CTCL is responsible for managing the enterprise commercial platform that hosts the training courses. This includes all training documents, videos, captions, and surveys.

CTCL is responsible for supporting users with technical issues on the platform and all training materials. CTCL will respond to technical support emails within 24 hours during regular business days and within 72 hours over federal holidays and weekends.

CTCL is responsible for maintaining all training content. Staff will do weekly sweeps of content to update links, sources, and language as needed.

#### Election cybersecurity training development process

Since developing the content in 2018, CTCL has delivered the training series via live webinars in 3 instances (July 2018, August 2018, February 2019). Then in July of 2019, CTCL launched the election cybersecurity series as 3 self-paced courses.

Across these iterations CTCL has adapted and updated the courses to reflect feedback from participants and changes to resources. For example, the self-paced courses were updated to reference the new Cybersecurity and Infrastructure Security Agency (CISA) services and removed the Department of Homeland Security (DHS) catalog that was included in previous versions.

To date 1,129 election officials from 22 states have completed CTCL's cybersecurity training. CTCL most recently partnered with the Virginia Department of Elections (ELECT) to deliver one of ELECT's most successful training opportunities that generated participation from more than 400 of Virginia's election officials. And in 2020 CTCL is poised to deliver cybersecurity training to every election department in the U.S.

**PLACE OF PERFORMANCE**

The Contractor shall perform the work off-site with Contracting Officer's Representative (COR) approval.

**PERIOD OF PERFORMANCE**

The period of performance shall be for one year from date of purchase, unless otherwise modified by the Contracting Officer.

**ACQUISITION TYPE**

The Government intends on awarding a single award with a firm-fixed price.

**REQUIREMENTS**

The specific work to be performed under these task areas include, but not limited to, the following:

**Reports** – The Contractor shall electronically submit a Report or provide access for the EAC to access electronic reports to the COR or POC at EAC with election official log in information showing who has utilized the training and provide survey results from the participants that attended the training.

**CONTRACTOR MINIMUM QUALIFICATIONS**

The Contractor and/or their partnering organization collectively (i.e. Teaming Partner(s), Subcontractors) shall have:

- a. Already established election specific cyber security related training that is available for immediate deployment, within a 1 week timeframe
- b. Have specific knowledge in the development and deployment election specific cyber training to states
- c. knowledge of back office election administration
- d. ability to provide training on a secure online platform in the cloud with redundancy to ensure 99.999 % uptime
- e. ability to track users that utilize the training in an automated report
- f. have an automated mechanism to collect feedback
- g. ability to update the training on a quarterly basis based on emerging security trends
- h. provide technical support to stakeholders and EAC in a timely manner





## Table of Contents

Qualifications for Center for Tech and Civic Life .....	1
Election cybersecurity training overview .....	2
<i>Cybersecurity 101: Introduction</i> .....	2
<i>Cybersecurity 201: Intermediate</i> .....	2
<i>Cybersecurity 301: Communications</i> .....	2
Training costs .....	2
Training delivery, technical support, and maintenance .....	3
Election cybersecurity training development process .....	3
Feedback from training participants .....	4
References .....	4
Staff .....	4
Federal contracting information .....	5

## Qualifications for Center for Tech and Civic Life

The Center for Tech and Civic Life (CTCL) is a civic tech 501(c)(3) nonprofit that connects Americans with the information they need to become and remain civically engaged, and helps ensure elections are professional, inclusive, and secure. With this in mind, CTCL supports election departments with industry best practices, free tech tools, and professional development courses.

One of CTCL's core programs is delivering low-cost, online training courses to election officials across the country on a range of topics that meet the most pressing needs facing the field of election administration. In response to election cyber incidents in 2016, CTCL partnered with the Center for Democracy and Technology in 2018 to develop election cybersecurity training courses for local election departments.

CTCL's 3-course election cybersecurity curriculum is the only training content that is tailored to local U.S. election offices, especially those with limited tech resources. The courses, which took 6 months to develop, have been iterated since 2018. The content and platform is tested, effective, and ready to deploy nationwide with 1-week notice.

## Election cybersecurity training overview

CTCL's election cybersecurity training is a 3-course series that empowers election offices to manage cyber threats and communicate with the public about cybersecurity. Each course covers unique content and takes about 90-minutes to complete.

### **CYBERSECURITY 101: INTRODUCTION**

1. Understand complex cybersecurity terminology
2. Identify different types of cyber threats and responses
3. Create stronger login practices

### **CYBERSECURITY 201: INTERMEDIATE**

1. Safeguard your election data
2. Apply National Institute of Standards and Technology cybersecurity framework to election systems
3. Develop partnerships to overcome security challenges

### **CYBERSECURITY 301: COMMUNICATIONS**

1. Inform the public about your election office's cybersecurity leadership
2. Make a cyber incident response plan
3. Build media allies

## Training costs

The **total cost for 3 courses is \$345,000** and includes:



- 1 year of unlimited access to 3 courses
- 1 year of maintenance of course content
- Access to pre-course and post-course evaluation responses via cloud storage
- Daily or weekly progress reports that can be accessed via cloud storage
- Monthly check-in meetings with CTCL staff Whitney May, Dylan Lynch, and Keegan Hughes

## Training delivery, technical support, and maintenance

CTCL is responsible for managing the enterprise commercial platform that hosts the training courses. This includes all training documents, videos, captions, and surveys.

CTCL is responsible for supporting users with technical issues on the platform and all training materials. CTCL will respond to technical support emails within 24 hours during regular business days and within 72 hours over federal holidays and weekends.

CTCL is responsible for maintaining all training content. Staff will do weekly sweeps of content to update links, sources, and language as needed.

## Election cybersecurity training development process

Since developing the content in 2018, CTCL has delivered the training series via live webinars in 3 instances (July 2018, August 2018, February 2019). Then in July of 2019, CTCL launched the election cybersecurity series as 3 self-paced courses.

Across these iterations CTCL has adapted and updated the courses to reflect feedback from participants and changes to resources. For example, the self-paced courses were updated to reference the new Cybersecurity and Infrastructure Security Agency (CISA) services and removed the Department of Homeland Security (DHS) catalog that was included in previous versions.

To date 1,129 election officials from 22 states have completed CTCL's cybersecurity training. CTCL most recently partnered with the Virginia Department of Elections (ELECT) to deliver one of ELECT's most successful training opportunities that generated participation from more than 400 of Virginia's election officials. And in 2020 CTCL is poised to deliver cybersecurity training to every election department in the U.S.





## Feedback from training participants

*"I want to thank you all for developing this training! It has been clear and simple enough for those of us who are not IT gurus. For example, some of the EI-ISAC info I receive is way over my head."*

*"We have been flooded with Cybersecurity Information since June. These courses should have been given FIRST and then we would have better understanding of the information we have been receiving from the state."*

*"I think this course is good for elected officials and staff outside of the IT Department and would recommend it to others. I believe a course like this helps bridge a knowledge gap between IT and end users which helps enable useful dialogue."*

## References

Daniel Persico  
Chief Information Officer  
Virginia Department of Elections  
daniel.persico@elections.virginia.gov  
(540) 903-0701

Penny Limburg  
Director of Elections & General Registrar  
City of Bristol, VA  
plimburg@bristolva.org  
(276) 645-7318

## Staff

Whitney May is Co-founder and Director of Government Services with the Center for Tech and Civic Life. She leads a team that's building the best professional development network for election officials who want to learn about new ways to engage the public and keep up with changing technology. Prior to founding CTCL, Whitney served the Durham County Board of Elections in North Carolina from 2007 to 2012 then joined the New Organizing Institute to work on the Voting Information Project. Whitney holds a BA in Business Administration from Belmont University.



Dylan Lynch is a Training Associate at the Center for Tech and Civic Life. He helps develop and deliver training courses that advance the tech and communication skills of election officials. Prior to joining CTCL, Dylan worked for the National Conference of State Legislatures (NCSL) as an elections policy specialist. Dylan earned his Master of Public Administration, focusing on public policy, from Drake University.

Keegan Hughes is the Senior Associate at the Center for Tech and Civic Life. She previously worked on the Elections Team at the Democracy Fund with a focus on modernizing voter registration. She previously spent an election cycle campaigning with Let America Vote. Before her career in elections, Keegan was a digital humanist working at the intersection between programming and literature, including projects for Oxford and Cambridge. She holds a BA in English Literature from Washington University in St. Louis.

## Federal contracting information

Center for Technology and Civic Life DUNS: 050750358

Center for Technology and Civic Life SAM/CAGE: 8JAM4

.





Click here to view instructions  
for completing this form

## Miscellaneous Obligation Request

### Section A - Miscellaneous Obligation Request

Type of Request	<input type="radio"/> New Request <input checked="" type="radio"/> Mod Adjustment <input type="radio"/> Deobligation		IPP Mandate	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Customer Name	EAC				
Obligating Document #	EAC-20-0049		PIID / PAID (Procurement ID / Parent ID)		
Period of Performance	5/9/2021	-	11/9/2021	Payment Terms	Net 30 Prompt Pay
Total Amount Obligated/Adjusted	\$		375,000.00		
Vendor Name/Trading Partner	Center for technology and Civic Life			ALC	
Vendor Duns # / Supplier #	050750358	TAS		BETC	DISB
Primary Invoice Approver/COR:	Robin Sargent				
Phone # /Email Address	(202) 360-2144/rsargent@eac.gov				
Alternate Invoice Approver/COR:	Ashley Williams				
Phone #/Email Address	(202) 870-0846/awilliams@eac.gov				

Description of goods/services to be provided: (Include account # if obligation is for a utility.)

Election cybersecurity training: 3 course series for election offices- 6month w/cost extension Only obligating FY21 FUNDS for \$30K

### Section B - Accounting Flexfield Information

Line	Shipment	Distribution	Fund	BFY	USSGL	BOC	Internal Org	Cost Pool	CAM1	Cat B	Program	Cohort	CAM2	CAM3	Trading Partner (TP) TAS	TP BETC	Amount
1	1	1	FSA0520DB1919XX	2019	61000001	252004	FSA6100000000	XXXXXXXXXX	XXXXXXXXXXXXXX	XXXXXX	XXXXXXXXXX	XXXX	XXXXXXXXXXXXXX	XXXXXXXXXXXXXX	020X4560010	COLL	50,000.00
Line Period of Performance:						Line Description:											
2	1	1	EAC1650DB2121XX	2021	61000001	252004	EAC1201000000										\$ 30,000.00
Line Period of Performance:			5/9/2021	-	11/9/2021	Line Description:			election cybersecurity training								
1	1	1	EAC16502020XX	2020	61000001	252004	EAC1201000000										\$345,000
Line Period of Performance:			5/8/2020	-	5/8/2021	Line Description:			election cybersecurity training								
Line Period of Performance:				-		Line Description:											
Line Period of Performance:				-		Line Description:											

Click here to create additional funding lines

### Section C - Customer Agency Authorized Requestor (In accordance with GAO Title 7, proper documentation will be maintained by customer.)

Approved By: (print name)	Mona Harrington
Approved By: (provide signature if faxing form, otherwise print name)	<i>Mona Harrington</i>
Date Approved:	5/17/2021

### Section D - ARC Accounting Office only

Oracle Obligation #	
---------------------	--