Microsoft

Microsoft

Research Faculty Summit 2012

ADVANCING THE STATE OF THE ART

ATTACKING THE WASHINGTON, D.C. INTERNET VOTING SYSTEM

J. Alex Halderman
The University of Michigan

MichiganEngineering

Who am I?
J. Alex Halderman

CS Prof.
University of Michigan

Security and Privacy

Tech Policy

Technology for Democracy

Selected Projects

2012	Widespread Weak Keys in Network Devices
2011	Telex: Anticensorship in the network infrastructure
2010	Hacking Washington D.C.’s Internet voting
2010	Vulnerabilities in India’s e-voting machines
2010	Reshaping developers’ security incentives
2009	Analysis of China’s Green Dam censorware
2009	Fingerprinting paper with desktop scanners
2008	Cold-boot attacks on encryption keys
2007	California’s “Top-to-Bottom” e-voting review
2007	Machine-assisted election auditing
2006	The Sony rootkit: DRM’s harmful side-effects

DISTRICT OF COLUMBIA
BOARD OF ELECTIONS AND ETHICS
WASHINGTON, D.C. 20001-2745

MEDIA RELEASE D.C. BOARD OF ELECTIONS AND ETHICS
September 21, 2010

Contact: Alysoun McLaughlin, amclaughlin@dcboee.org
202-727-2511 (direct)/202-441-1121 (cell)

Board Announces Public Test of Digital Vote by Mail Service

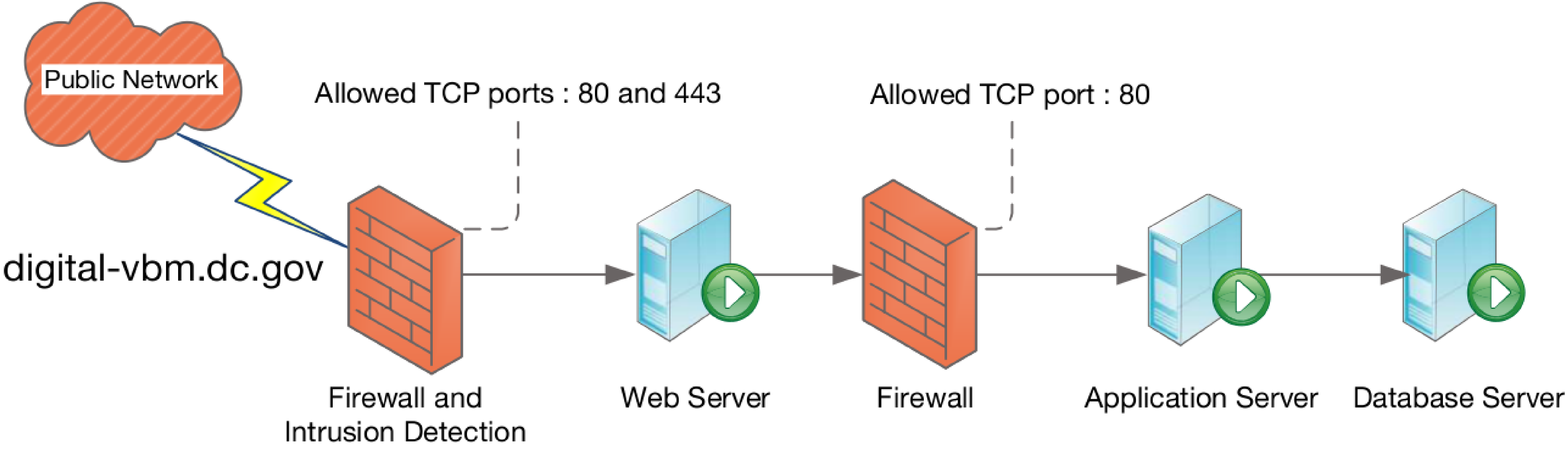
Open Source Solution Provides Secure Alternative for Overseas Voters Who Are Underserved by Traditional Vote by Mail

WASHINGTON, D.C. —The Board of Elections and Ethics today announced that the public examination phase of the Digital Vote by Mail pilot project for overseas voters will begin on Friday, September 24.

Digital Vote by Mail is a first-in-the-nation use of open source technology to provide a secure means for overseas voters to obtain, print and mail their ballot – and, if the voter chooses, also digitally mark and return their ballot. After testing is completed, the service will be made available to overseas voters, who often do not have enough time to receive and return their ballot by mail in the few weeks between the September primary and the November general election. Prior to Digital Vote by Mail, the only option for these voters was to sacrifice the secrecy of their ballot by using e-mail or fax.

During the test period, which will continue through Thursday, September 30, individuals who wish test and comment on the technology and usability of the application will be granted access to the application, a complete system architectural diagram, and access to the underlying source code.

A limited number of test credentials will be available on a first-come, first-served basis beginning on Friday morning. Using these test credentials, a tester may log in as a fictitious District voter and request, complete and submit an absentee ballot. The Board will compile all test ballots and test the decoding software and back office processes needed to accept and process digitally transmitted ballots. The Board asks testers to thoroughly test the system and disclose any security, programmatic, usability or other functional or design issues they discover in the testing process. All data, hardware and software are logically and physically segregated from all other Board systems. Users will not be held liable for damage resulting from good faith efforts at testing system integrity.



Public Network

digital-vbm.dc.gov

Allowed TCP ports : 80 and 443

Allowed TCP port : 80

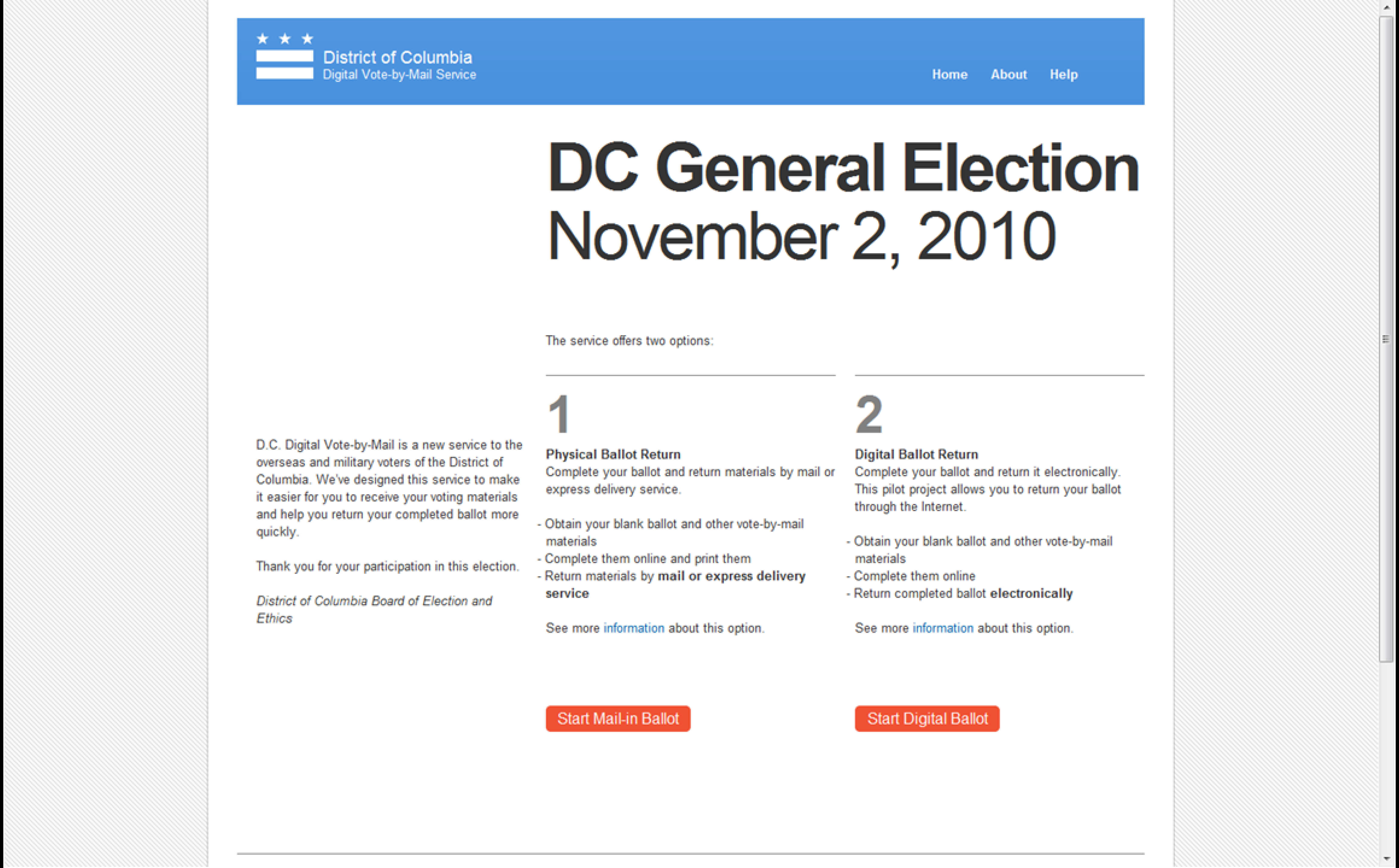
Firewall and Intrusion Detection

Web Server

Firewall

Application Server

Database Server



DC General Election
November 2, 2010

D.C. Digital Vote-by-Mail is a new service to the overseas and military voters of the District of Columbia. We've designed this service to make it easier for you to receive your voting materials and help you return your completed ballot more quickly.

Thank you for your participation in this election.

District of Columbia Board of Election and Ethics

The service offers two options:

1

Physical Ballot Return
Complete your ballot and return materials by mail or express delivery service.

- Obtain your blank ballot and other vote-by-mail materials
- Complete them online and print them
- Return materials by **mail or express delivery service**

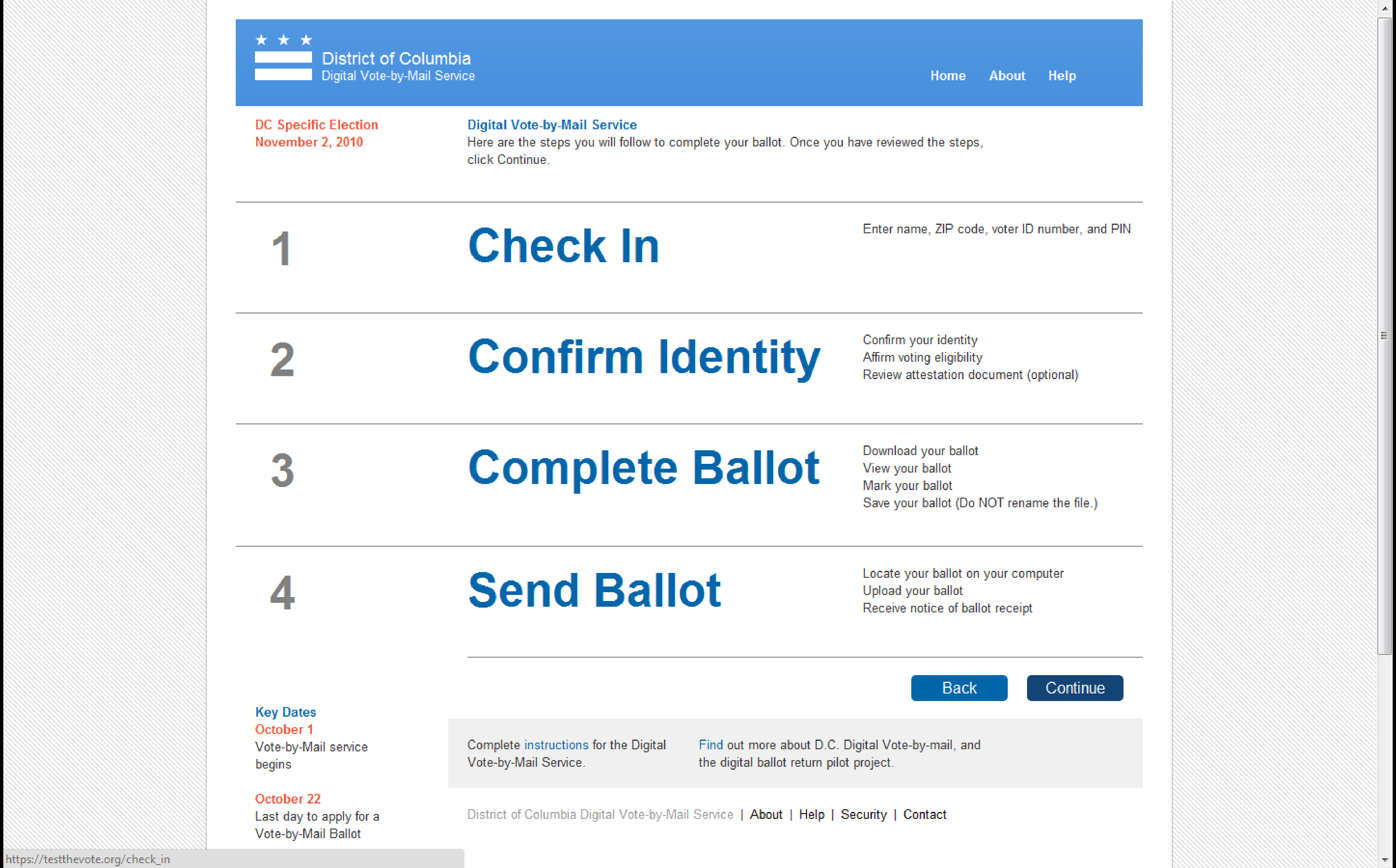
See more information about this option.

2

Digital Ballot Return
Complete your ballot and return it electronically. This pilot project allows you to return your ballot through the Internet.

- Obtain your blank ballot and other vote-by-mail materials
- Complete them online
- Return completed ballot **electronically**

See more information about this option.


District of Columbia
Digital Vote-by-Mail Service
Home
About
Help
Back
Continue
https://testthevote.org/check_in

DC Specific Election
November 2, 2010

Digital Vote-by-Mail Service
Here are the steps you will follow to complete your ballot. Once you have reviewed the steps, click Continue.

1	**Check In**	Enter name, ZIP code, voter ID number, and PIN
2	**Confirm Identity**	Confirm your identity Affirm voting eligibility Review attestation document (optional)
3	**Complete Ballot**	Download your ballot View your ballot Mark your ballot Save your ballot (Do NOT rename the file.)
4	**Send Ballot**	Locate your ballot on your computer Upload your ballot Receive notice of ballot receipt

Key Dates

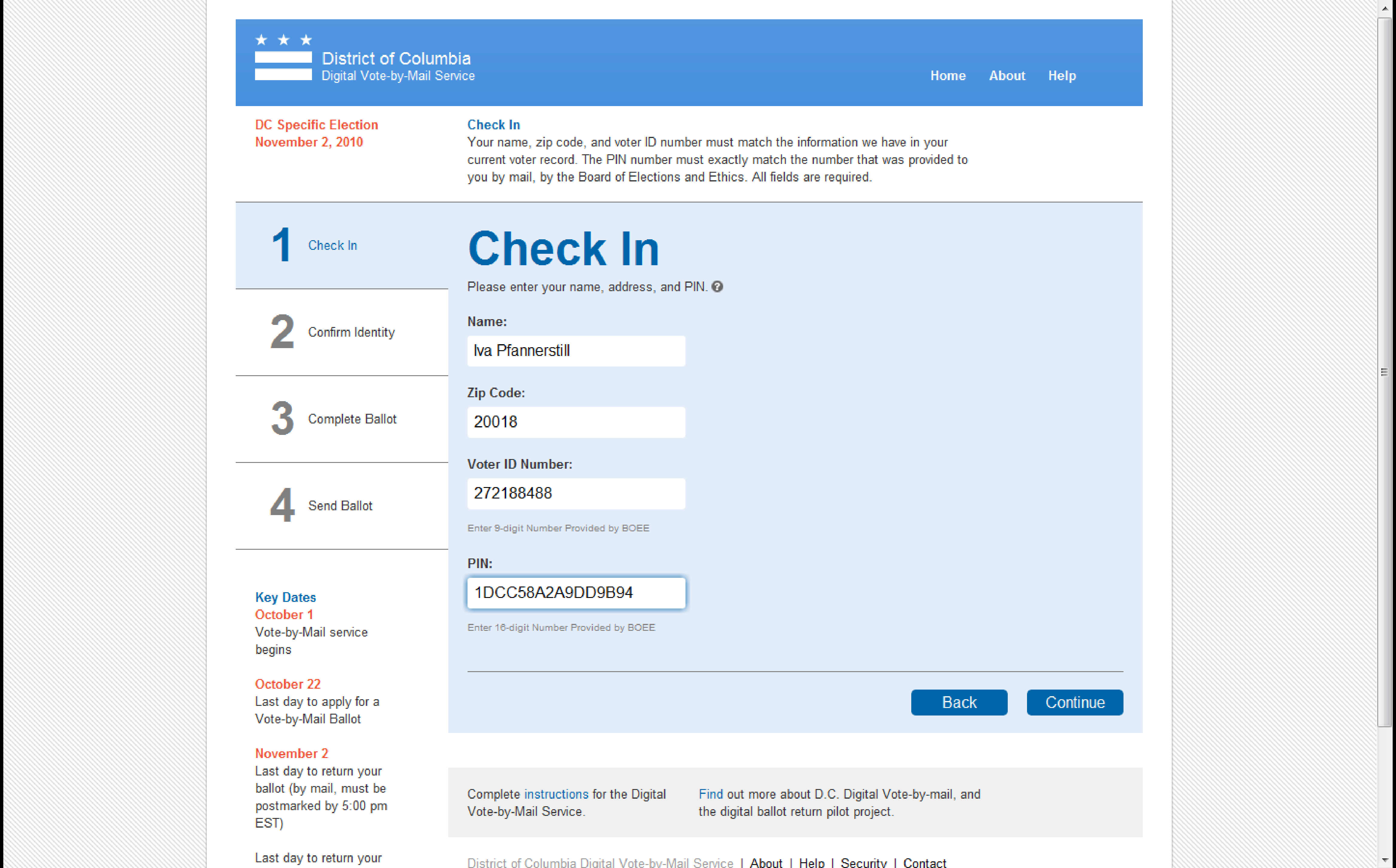
October 1
Vote-by-Mail service begins

October 22
Last day to apply for a Vote-by-Mail Ballot

Complete instructions for the Digital Vote-by-Mail Service.

Find out more about D.C. Digital Vote-by-mail, and the digital ballot return pilot project.

District of Columbia Digital Vote-by-Mail Service | About | Help | Security | Contact



District of Columbia
Digital Vote-by-Mail Service

DC Specific Election
November 2, 2010

Check In
Your name, zip code, and voter ID number must match the information we have in your current voter record. The PIN number must exactly match the number that was provided to you by mail, by the Board of Elections and Ethics. All fields are required.

1 Check In

2 Confirm Identity

3 Complete Ballot

4 Send Ballot

Check In

Please enter your name, address, and PIN. ?

Name:
Iva Pfannerstill

Zip Code:
20018

Voter ID Number:
272188488

Enter 9-digit Number Provided by BOEE

PIN:
1DCC58A2A9DD9B94

Enter 16-digit Number Provided by BOEE

Key Dates
October 1
Vote-by-Mail service begins

October 22
Last day to apply for a Vote-by-Mail Ballot

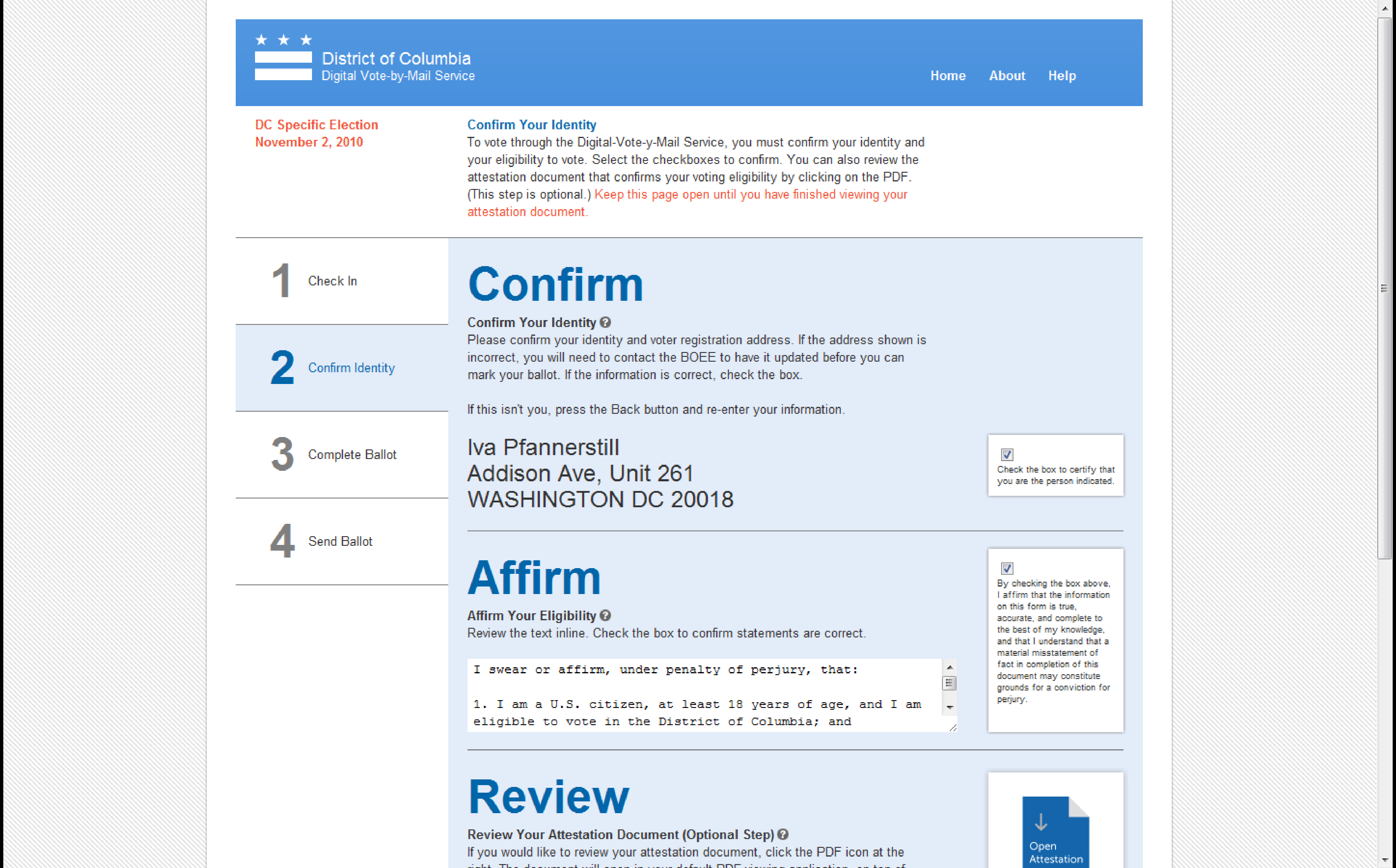
November 2
Last day to return your ballot (by mail, must be postmarked by 5:00 pm EST)

Last day to return your

Complete instructions for the Digital Vote-by-Mail Service.

Find out more about D.C. Digital Vote-by-mail, and the digital ballot return pilot project.

District of Columbia Digital Vote-by-Mail Service | About | Help | Security | Contact



District of Columbia
Digital Vote-by-Mail Service

DC Specific Election
November 2, 2010

Confirm Your Identity

To vote through the Digital-Vote-y-Mail Service, you must confirm your identity and your eligibility to vote. Select the checkboxes to confirm. You can also review the attestation document that confirms your voting eligibility by clicking on the PDF. (This step is optional.) Keep this page open until you have finished viewing your attestation document.

1 Check In

2 Confirm Identity

3 Complete Ballot

4 Send Ballot

Confirm

Confirm Your Identity ?

Please confirm your identity and voter registration address. If the address shown is incorrect, you will need to contact the BOEE to have it updated before you can mark your ballot. If the information is correct, check the box.

If this isn't you, press the Back button and re-enter your information.

Iva Pfannerstill
Addison Ave, Unit 261
WASHINGTON DC 20018

☑ Check the box to certify that you are the person indicated.

Affirm

Affirm Your Eligibility ?

Review the text inline. Check the box to confirm statements are correct.

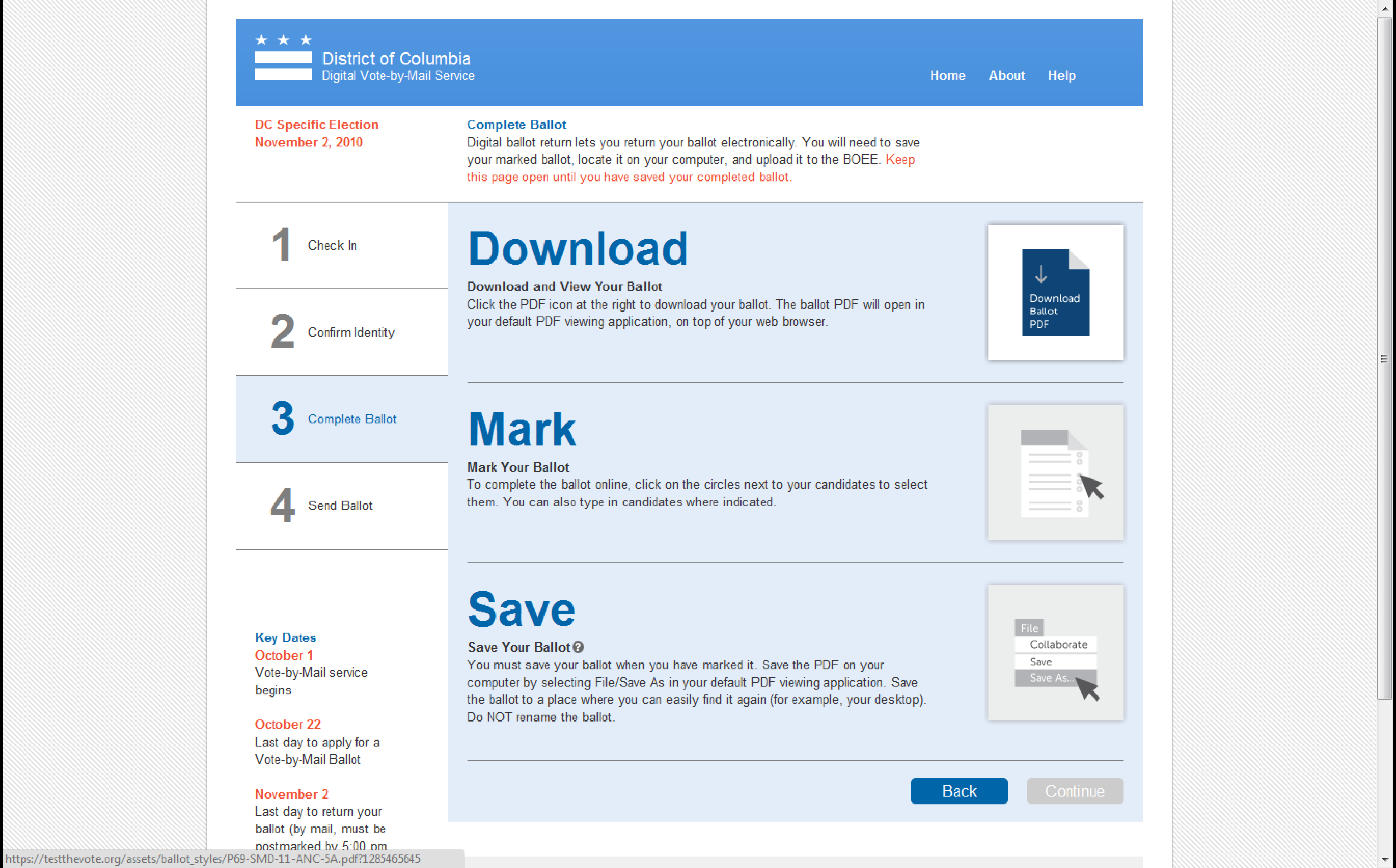
```
I swear or affirm, under penalty of perjury, that:

1. I am a U.S. citizen, at least 18 years of age, and I am
eligible to vote in the District of Columbia; and
```

☑ By checking the box above, I affirm that the information on this form is true, accurate, and complete to the best of my knowledge, and that I understand that a material misstatement of fact in completion of this document may constitute grounds for a conviction for perjury.

Review

Review Your Attestation Document (Optional Step) ?

If you would like to review your attestation document, click the PDF icon at the right. The document will open in your default PDF viewing application, on top of



District of Columbia
Digital Vote-by-Mail Service

Home About Help

DC Specific Election
November 2, 2010

Complete Ballot

Digital ballot return lets you return your ballot electronically. You will need to save your marked ballot, locate it on your computer, and upload it to the BOEE. Keep this page open until you have saved your completed ballot.

1 Check In

2 Confirm Identity

3 Complete Ballot

4 Send Ballot

Download

Download and View Your Ballot

Click the PDF icon at the right to download your ballot. The ballot PDF will open in your default PDF viewing application, on top of your web browser.

Mark

Mark Your Ballot

To complete the ballot online, click on the circles next to your candidates to select them. You can also type in candidates where indicated.

Save

Save Your Ballot ?

You must save your ballot when you have marked it. Save the PDF on your computer by selecting File/Save As in your default PDF viewing application. Save the ballot to a place where you can easily find it again (for example, your desktop). Do NOT rename the ballot.

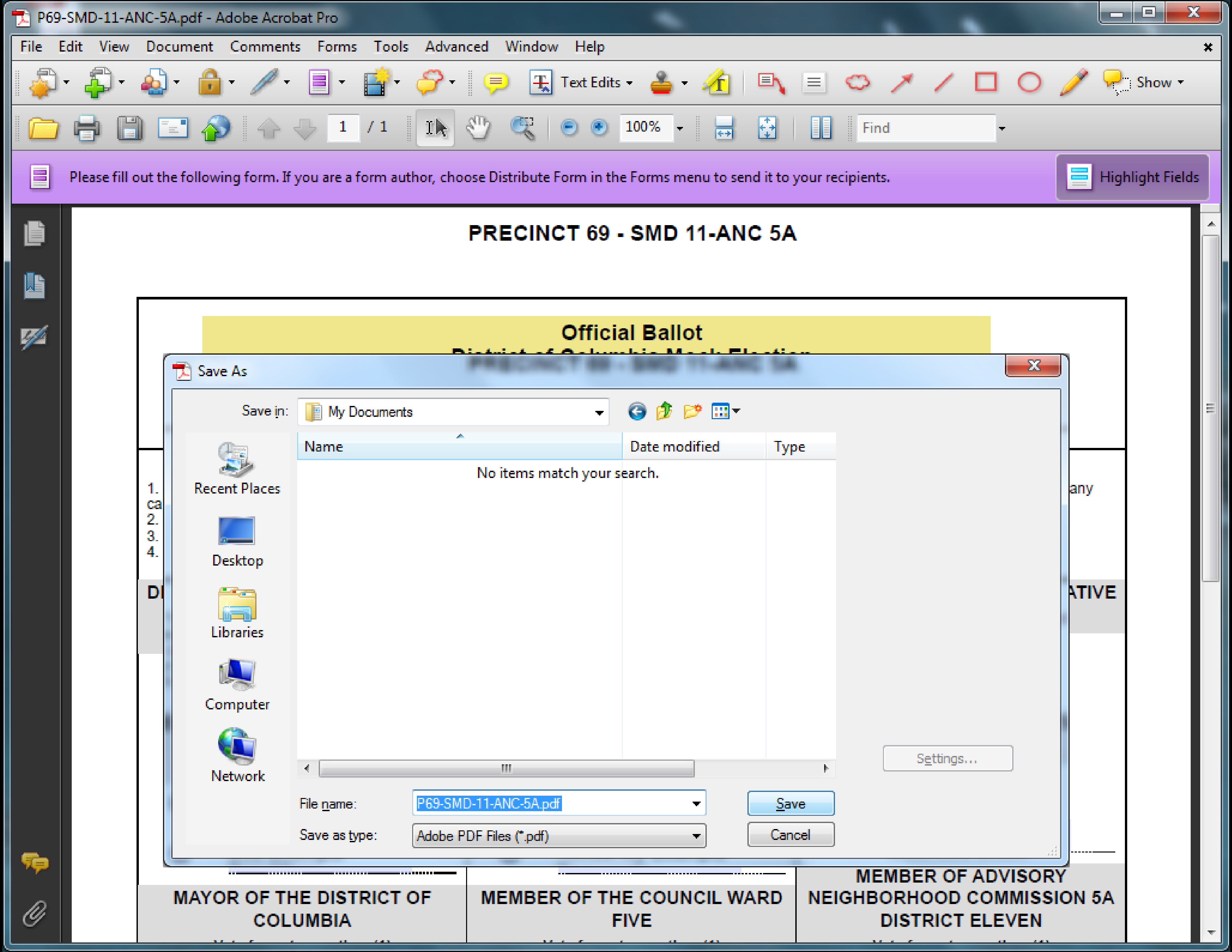
Key Dates

October 1
Vote-by-Mail service begins

October 22
Last day to apply for a Vote-by-Mail Ballot

November 2
Last day to return your ballot (by mail, must be postmarked by 5:00 pm

https://testthevote.org/assets/ballot_styles/P69-SMD-11-ANC-5A.pdf?1285465645



Please fill out the following form. If you are a form author, choose Distribute Form in the Forms menu to send it to your recipients.

PRECINCT 69 - SMD 11-ANC 5A

Official Ballot

Save in: My Documents

No items match your search.

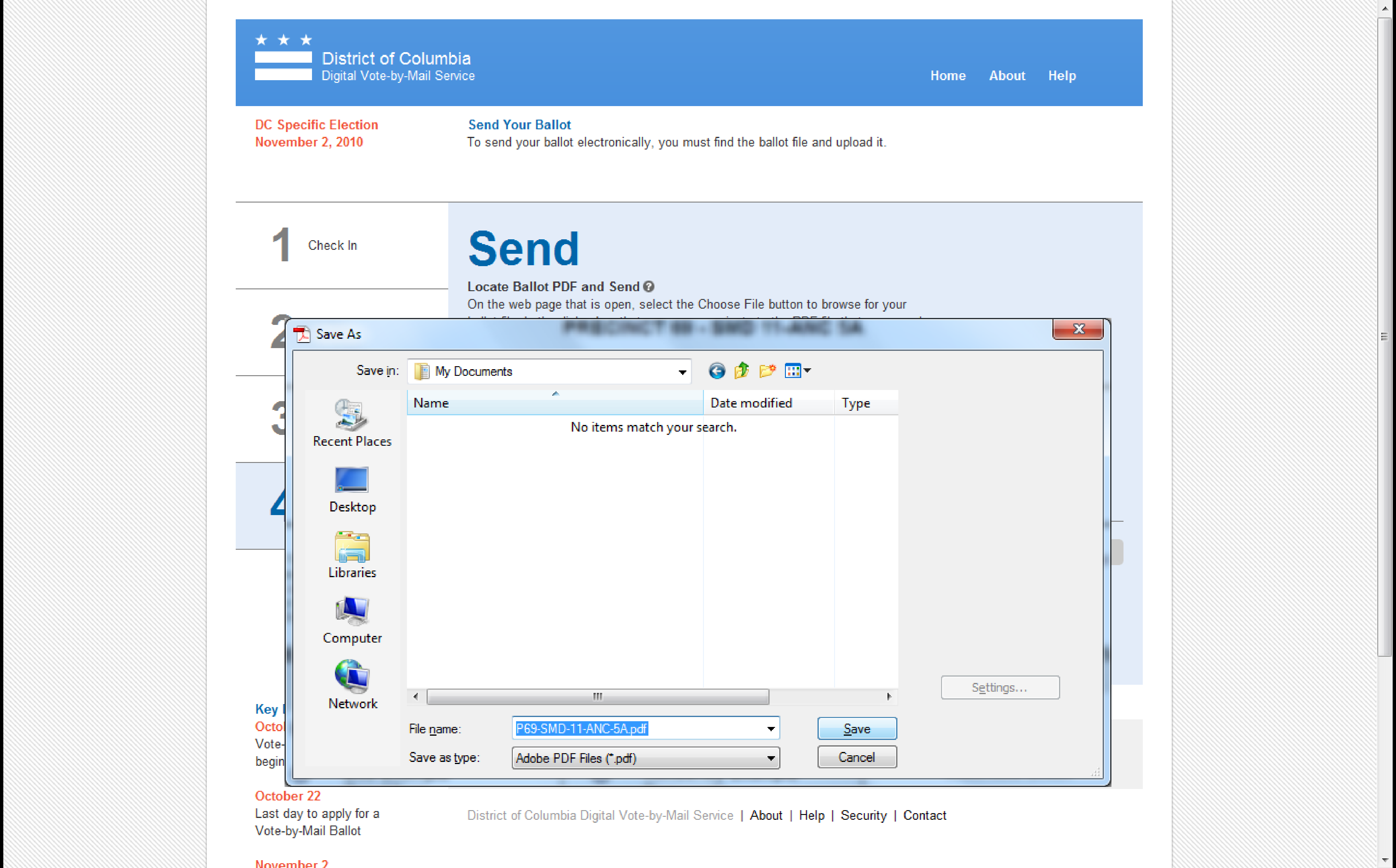
File name: P69-SMD-11-ANC-5A.pdf

Save as type: Adobe PDF Files (*.pdf)

MAYOR OF THE DISTRICT OF COLUMBIA

MEMBER OF THE COUNCIL WARD FIVE

MEMBER OF ADVISORY NEIGHBORHOOD COMMISSION 5A DISTRICT ELEVEN



DC Specific Election
November 2, 2010

Send Your Ballot

To send your ballot electronically, you must find the ballot file and upload it.

Send

Locate Ballot PDF and Send

On the web page that is open, select the Choose File button to browse for your

Save As [redacted]

Save in: My Documents

Name	Date modified	Type
No items match your search.		

File name: P69-SMD-11-ANC-5A.pdf

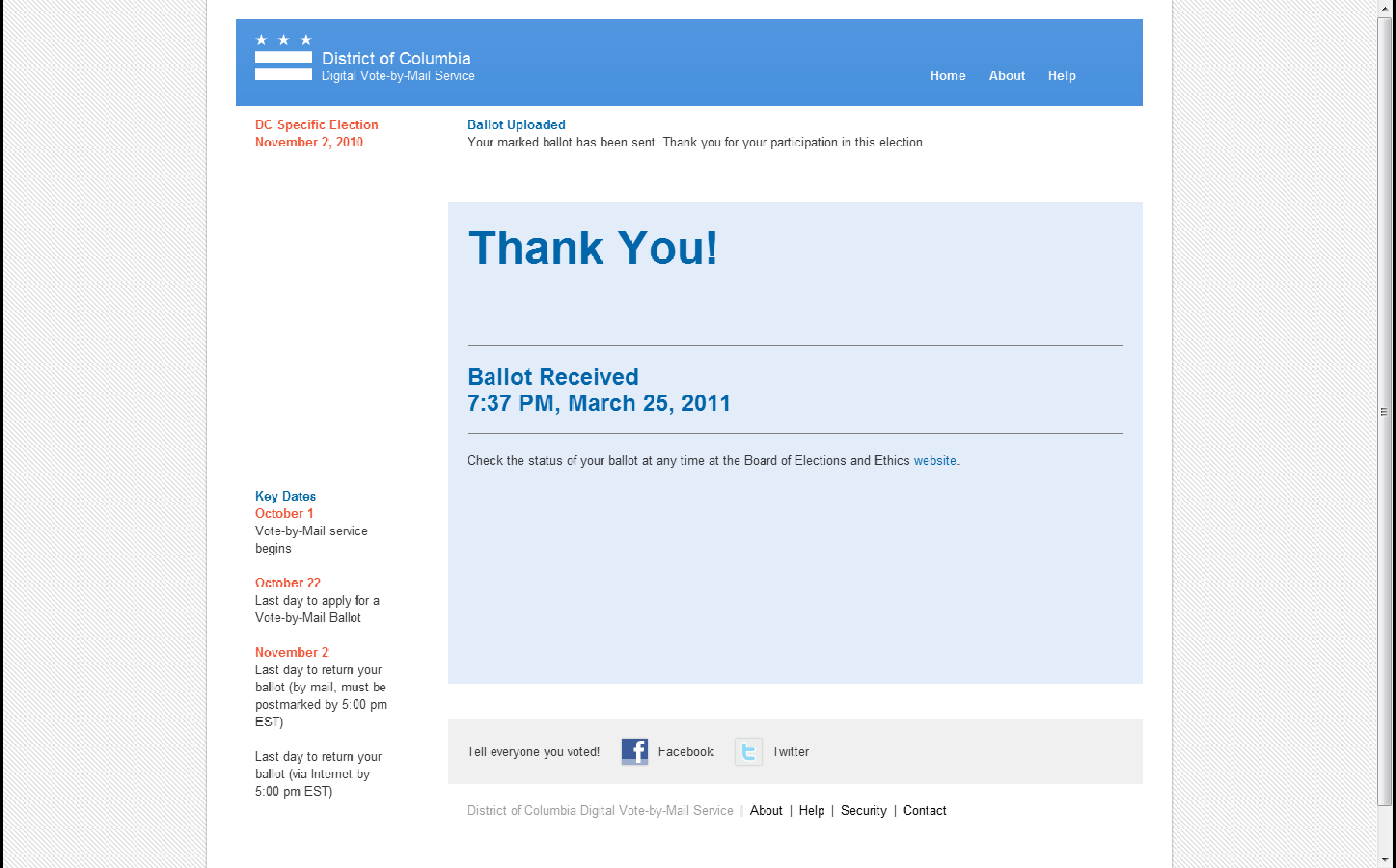
Save as type: Adobe PDF Files (*.pdf)

Key
Octo
Vote-
begin

October 22
Last day to apply for a Vote-by-Mail Ballot

November 2

District of Columbia Digital Vote-by-Mail Service | About | Help | Security | Contact



District of Columbia
Digital Vote-by-Mail Service

DC Specific Election
November 2, 2010

Ballot Uploaded
Your marked ballot has been sent. Thank you for your participation in this election.

Thank You!

Ballot Received
7:37 PM, March 25, 2011

Check the status of your ballot at any time at the Board of Elections and Ethics website.

Key Dates

October 1
Vote-by-Mail service begins

October 22
Last day to apply for a Vote-by-Mail Ballot

November 2
Last day to return your ballot (by mail, must be postmarked by 5:00 pm EST)

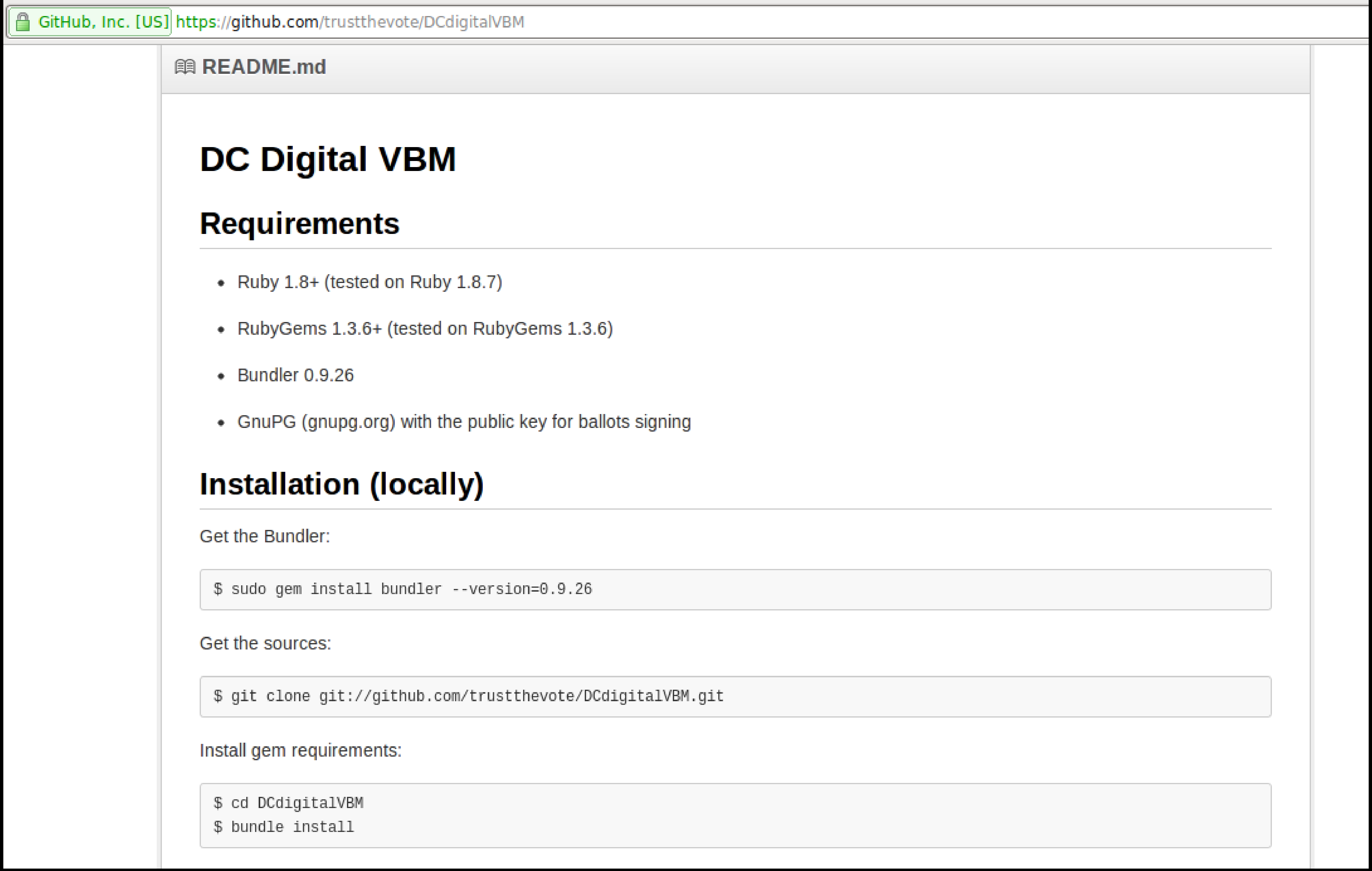
Last day to return your ballot (via Internet by 5:00 pm EST)

Tell everyone you voted! Facebook Twitter

District of Columbia Digital Vote-by-Mail Service | About | Help | Security | Contact

RECRUIT

✓ 1. collect info (remember
✓ 2. establish level of control
✓ 3. clear track
✓ 4. install attacks
~~- replace old ballots~~
~~- steal tmp ballots~~
~~- rig to replace new ballots~~
~~- rig to steal new ballots~~
get ROOT?
~~defacement~~
~~SSL cert?~~
SSL backdoor?
1. Ches
Telex
Mouse
MICHIGA
CAMP CAEN 200


GitHub, Inc. [US] https://github.com/trustthevote/DCdigitalVBM
README.md

DC Digital VBM

Requirements

- Ruby 1.8+ (tested on Ruby 1.8.7)
- RubyGems 1.3.6+ (tested on RubyGems 1.3.6)
- Bundler 0.9.26
- GnuPG (gnupg.org) with the public key for ballots signing

Installation (locally)

Get the Bundler:

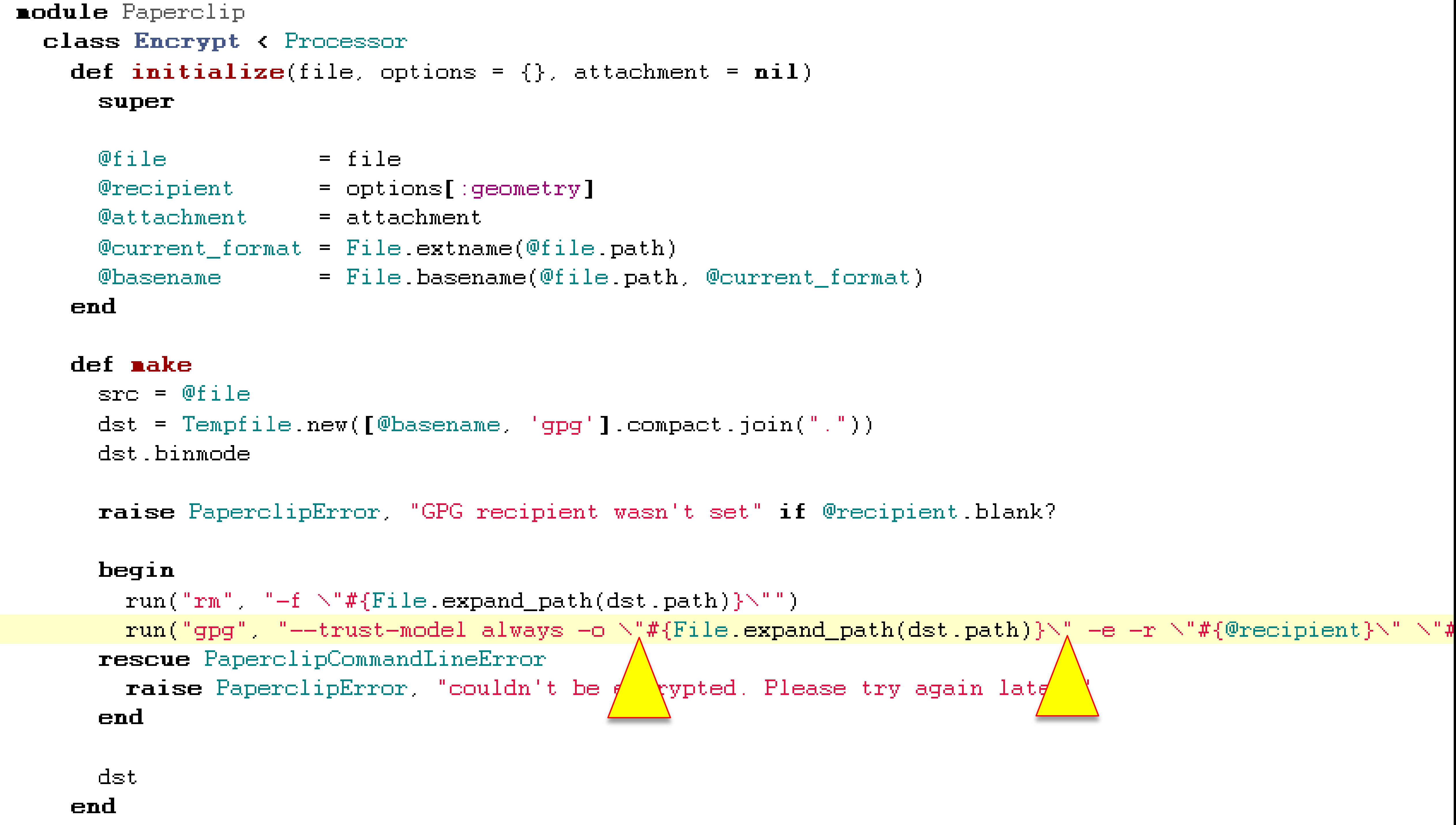
```
$ sudo gem install bundler --version=0.9.26
```

Get the sources:

```
$ git clone git://github.com/trustthevote/DCdigitalVBM.git
```

Install gem requirements:

```
$ cd DCdigitalVBM
$ bundle install
```



```
module Paperclip
  class Encrypt < Processor
    def initialize(file, options = {}, attachment = nil)
      super

      @file           = file
      @recipient      = options[:geometry]
      @attachment     = attachment
      @current_format = File.extname(@file.path)
      @basename       = File.basename(@file.path, @current_format)
    end

    def make
      src = @file
      dst = Tempfile.new([@basename, 'gpg'].compact.join("."))
      dst.binmode

      raise PaperclipError, "GPG recipient wasn't set" if @recipient.blank?

      begin
        run("rm", "-f \"#{File.expand_path(dst.path)}\"")
        run("gpg", "--trust-model always -o \"#{File.expand_path(dst.path)}\" -e -r \"#{@recipient}\" \"#
      rescue PaperclipCommandLineError
        raise PaperclipError, "couldn't be encrypted. Please try again later."
      end

      dst
    end
```

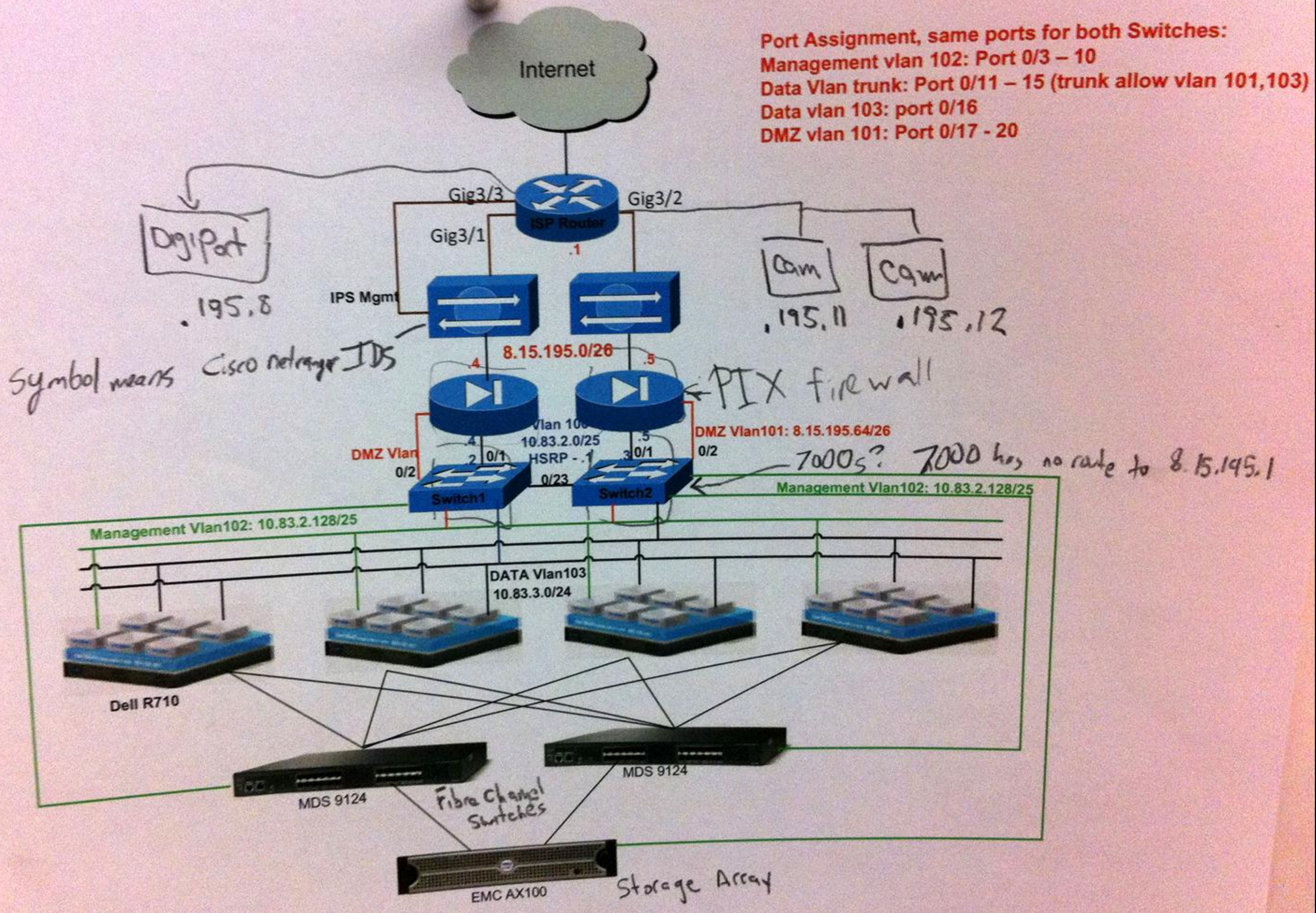
ballot.pdf → /tmp/49d5.pdf

ballot.xyz → /tmp/49d5.xyz

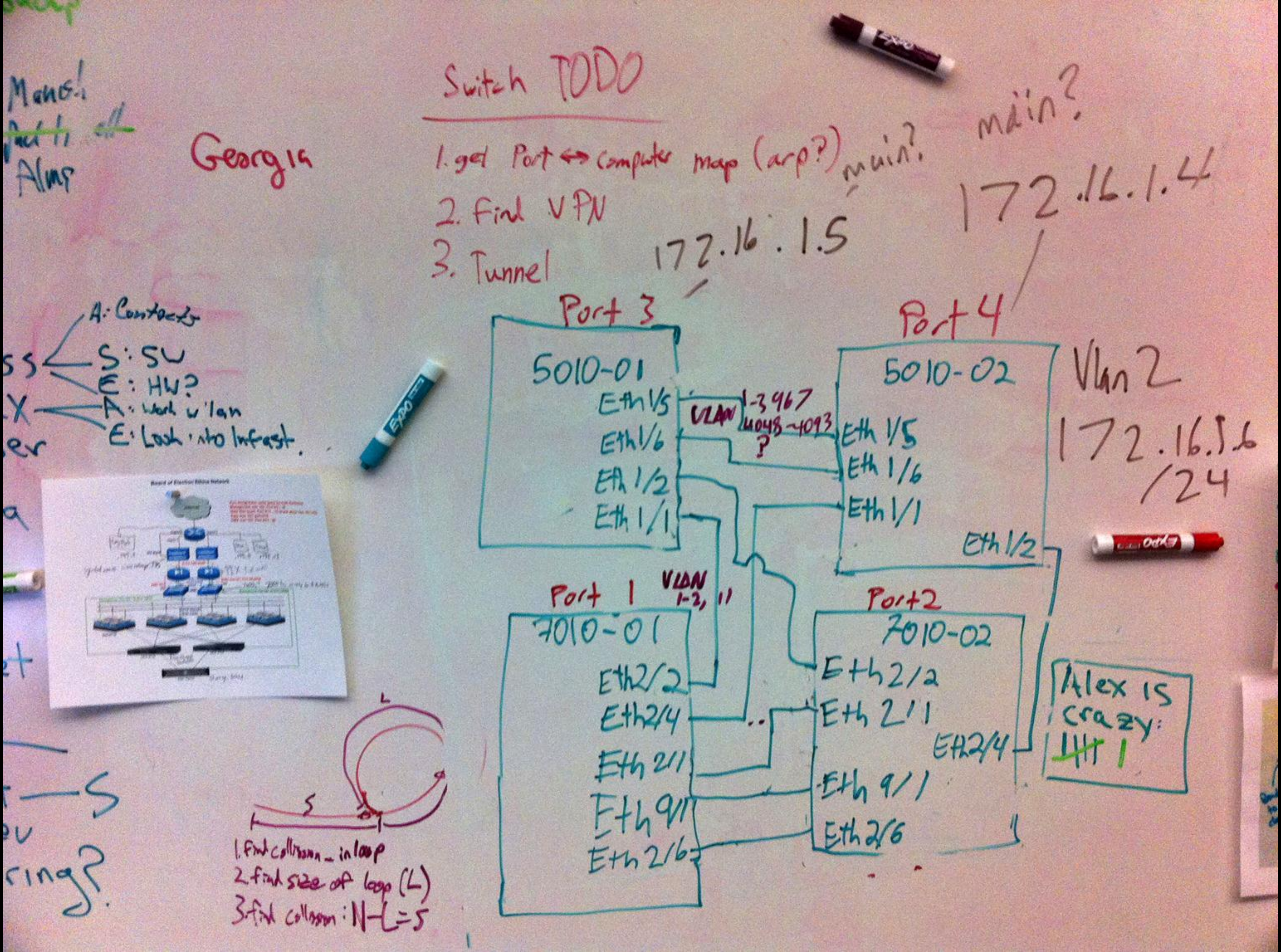
ballot.$(sleep 5) → /tmp/49d5.$(sleep 5)

SURVEIL

Board of Election Ethics Network



Port Assignment, same ports for both Switches:
Management vlan 102: Port 0/3 – 10
Data Vlan trunk: Port 0/11 – 15 (trunk allow vlan 101,103)
Data vlan 103: port 0/16
DMZ vlan 101: Port 0/17 - 20



Switch TODO

1. get Port ↔ computer map (arp?)
2. Find VPN
3. Tunnel

Georgia

Manos!

Alma

ss — A: Contacts
S: SW
E: HW?

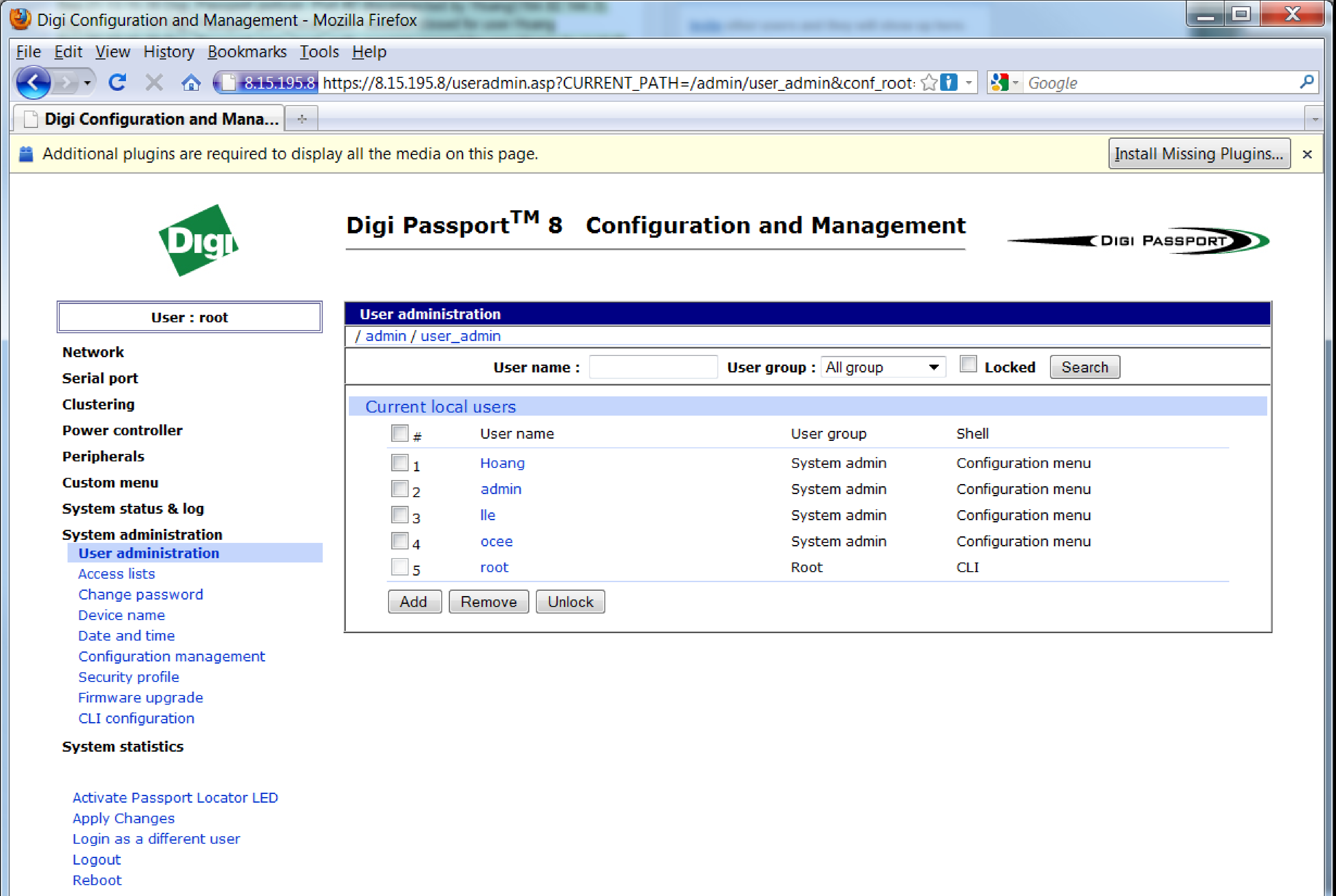
X — A: Work w/ lan
E: Look into Infrast.

er

1. Find collision in loop
2. find size of loop (L)
3. find collision: N−L=S

Alex is crazy:
~~IIII~~ I

ring?



Digi Passport^{TM} 8 Configuration and Management

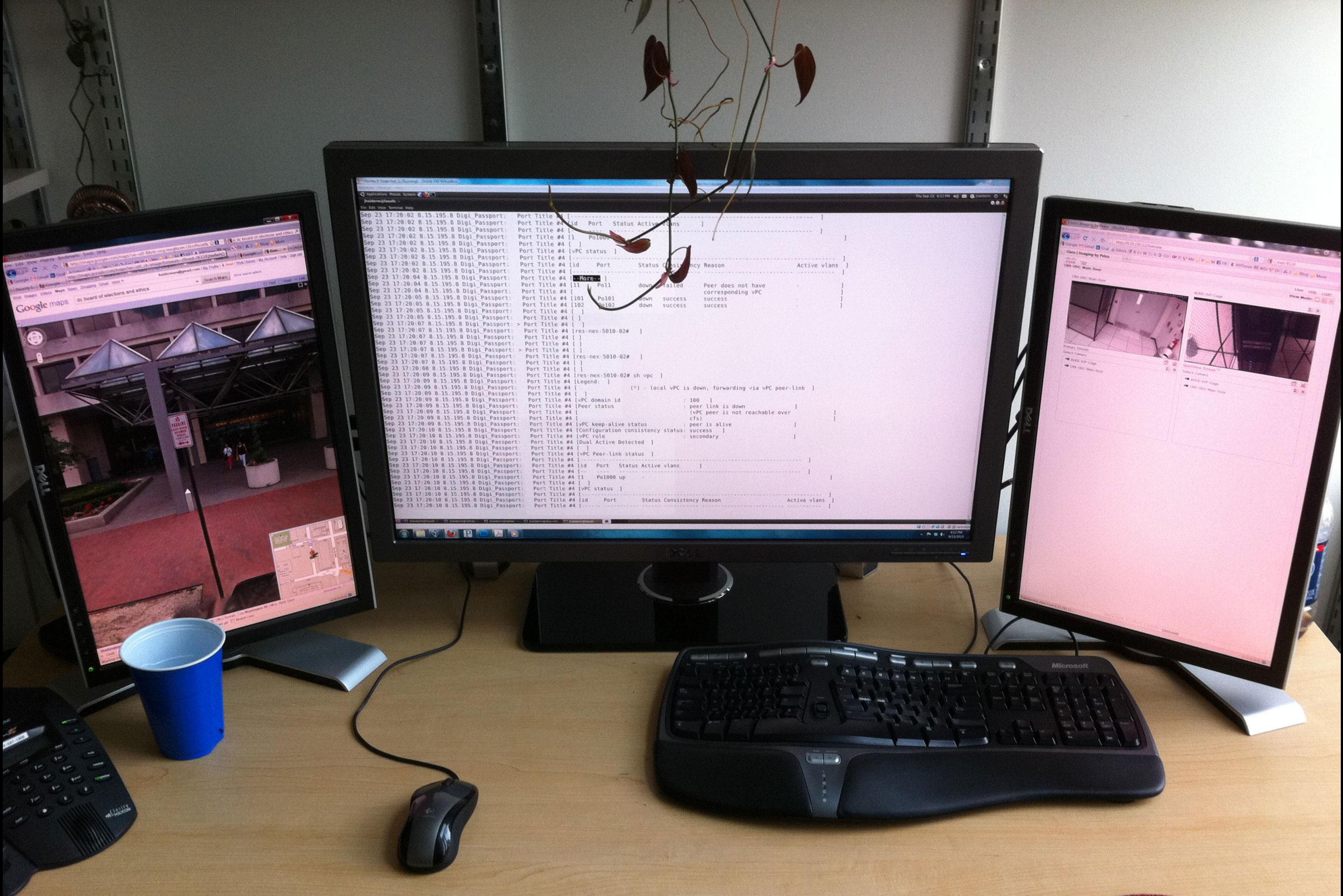
User administration

/ admin / user_admin

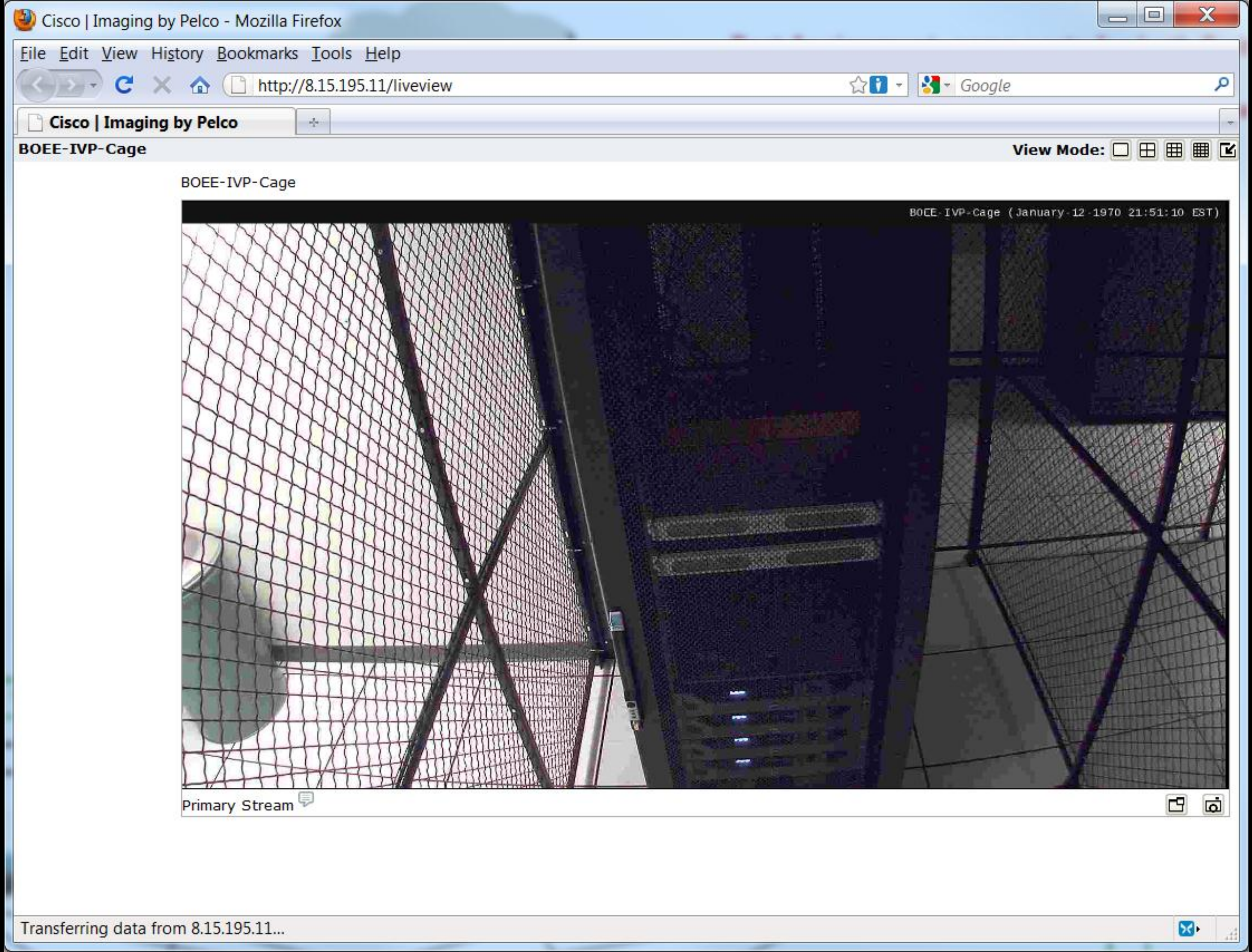
User name : ______ User group : All group ▾ □ Locked Search

Current local users

□ #	User name	User group	Shell
□ 1	Hoang	System admin	Configuration menu
□ 2	admin	System admin	Configuration menu
□ 3	lle	System admin	Configuration menu
□ 4	ocee	System admin	Configuration menu
□ 5	root	Root	CLI



```
Sep 23 17:20:02 8.15.195.8 Digi_Passport:   Port Title #4 [-------------------------------------------------------- ]
Sep 23 17:20:02 8.15.195.8 Digi_Passport:   Port Title #4 [id   Port   Status Active vlans       ]
Sep 23 17:20:02 8.15.195.8 Digi_Passport:   Port Title #4 [-- ---- ------ ----------------------------------------- ]
Sep 23 17:20:02 8.15.195.8 Digi_Passport:   Port Title #4 [1    Po1000                                                  ]
Sep 23 17:20:02 8.15.195.8 Digi_Passport:   Port Title #4 [  ]
Sep 23 17:20:02 8.15.195.8 Digi_Passport:   Port Title #4 [vPC status  ]
Sep 23 17:20:02 8.15.195.8 Digi_Passport:   Port Title #4 [--------------------------------------------------------------------- ]
Sep 23 17:20:02 8.15.195.8 Digi_Passport:   Port Title #4 [id     Port        Status Consistency Reason                     Active vlans  ]
Sep 23 17:20:02 8.15.195.8 Digi_Passport:   Port Title #4 [--------------------------------------------------------------------- ]
Sep 23 17:20:04 8.15.195.8 Digi_Passport:   Port Title #4 [ --More-- ]
Sep 23 17:20:04 8.15.195.8 Digi_Passport:   Port Title #4 [11     Po11        down   failed      Peer does not have        -      ]
Sep 23 17:20:04 8.15.195.8 Digi_Passport:   Port Title #4 [                                      corresponding vPC                ]
Sep 23 17:20:05 8.15.195.8 Digi_Passport:   Port Title #4 [101    Po101       down   success     success                   -      ]
Sep 23 17:20:05 8.15.195.8 Digi_Passport:   Port Title #4 [102    Po102       down   success     success                   -      ]
Sep 23 17:20:05 8.15.195.8 Digi_Passport:   Port Title #4 [  ]
Sep 23 17:20:05 8.15.195.8 Digi_Passport:   Port Title #4 [ ]
Sep 23 17:20:07 8.15.195.8 Digi_Passport: > Port Title #4 [  ]
Sep 23 17:20:07 8.15.195.8 Digi_Passport:   Port Title #4 [res-nex-5010-02#   ]
Sep 23 17:20:07 8.15.195.8 Digi_Passport:   Port Title #4 [ ]
Sep 23 17:20:07 8.15.195.8 Digi_Passport:   Port Title #4 [ ]
Sep 23 17:20:07 8.15.195.8 Digi_Passport: > Port Title #4 [ ]
Sep 23 17:20:07 8.15.195.8 Digi_Passport:   Port Title #4 [res-nex-5010-02#   ]
Sep 23 17:20:07 8.15.195.8 Digi_Passport:   Port Title #4 [ ]
Sep 23 17:20:08 8.15.195.8 Digi_Passport:   Port Title #4 [ ]
Sep 23 17:20:09 8.15.195.8 Digi_Passport:   Port Title #4 [res-nex-5010-02# sh vpc  ]
Sep 23 17:20:09 8.15.195.8 Digi_Passport:   Port Title #4 [Legend:  ]
Sep 23 17:20:09 8.15.195.8 Digi_Passport:   Port Title #4 [                (*) - local vPC is down, forwarding via vPC peer-link  ]
Sep 23 17:20:09 8.15.195.8 Digi_Passport:   Port Title #4 [  ]
Sep 23 17:20:09 8.15.195.8 Digi_Passport:   Port Title #4 [vPC domain id                     : 100   ]
Sep 23 17:20:09 8.15.195.8 Digi_Passport:   Port Title #4 [Peer status                       : peer link is down            ]
Sep 23 17:20:09 8.15.195.8 Digi_Passport:   Port Title #4 [                                    (vPC peer is not reachable over      ]
Sep 23 17:20:09 8.15.195.8 Digi_Passport:   Port Title #4 [                                    cfs)                                 ]
Sep 23 17:20:09 8.15.195.8 Digi_Passport:   Port Title #4 [vPC keep-alive status             : peer is alive                ]
Sep 23 17:20:10 8.15.195.8 Digi_Passport:   Port Title #4 [Configuration consistency status: success   ]
Sep 23 17:20:10 8.15.195.8 Digi_Passport:   Port Title #4 [vPC role                          : secondary                    ]
Sep 23 17:20:10 8.15.195.8 Digi_Passport:   Port Title #4 [Dual Active Detected  ]
Sep 23 17:20:10 8.15.195.8 Digi_Passport:   Port Title #4 [  ]
Sep 23 17:20:10 8.15.195.8 Digi_Passport:   Port Title #4 [vPC Peer-link status  ]
Sep 23 17:20:10 8.15.195.8 Digi_Passport:   Port Title #4 [-------------------------------------------------------- ]
Sep 23 17:20:10 8.15.195.8 Digi_Passport:   Port Title #4 [id   Port   Status Active vlans       ]
Sep 23 17:20:10 8.15.195.8 Digi_Passport:   Port Title #4 [--   ----   ------ ----------------------------------------- ]
Sep 23 17:20:10 8.15.195.8 Digi_Passport:   Port Title #4 [1    Po1000 up     -                                          ]
Sep 23 17:20:10 8.15.195.8 Digi_Passport:   Port Title #4 [  ]
Sep 23 17:20:10 8.15.195.8 Digi_Passport:   Port Title #4 [vPC status  ]
Sep 23 17:20:10 8.15.195.8 Digi_Passport:   Port Title #4 [--------------------------------------------------------------------- ]
Sep 23 17:20:10 8.15.195.8 Digi_Passport:   Port Title #4 [id     Port        Status Consistency Reason                     Active vlans  ]
Sep 23 17:20:10 8.15.195.8 Digi_Passport:   Port Title #4 [------ ----------- ------ ----------- -------------------------- ----------- ]
```



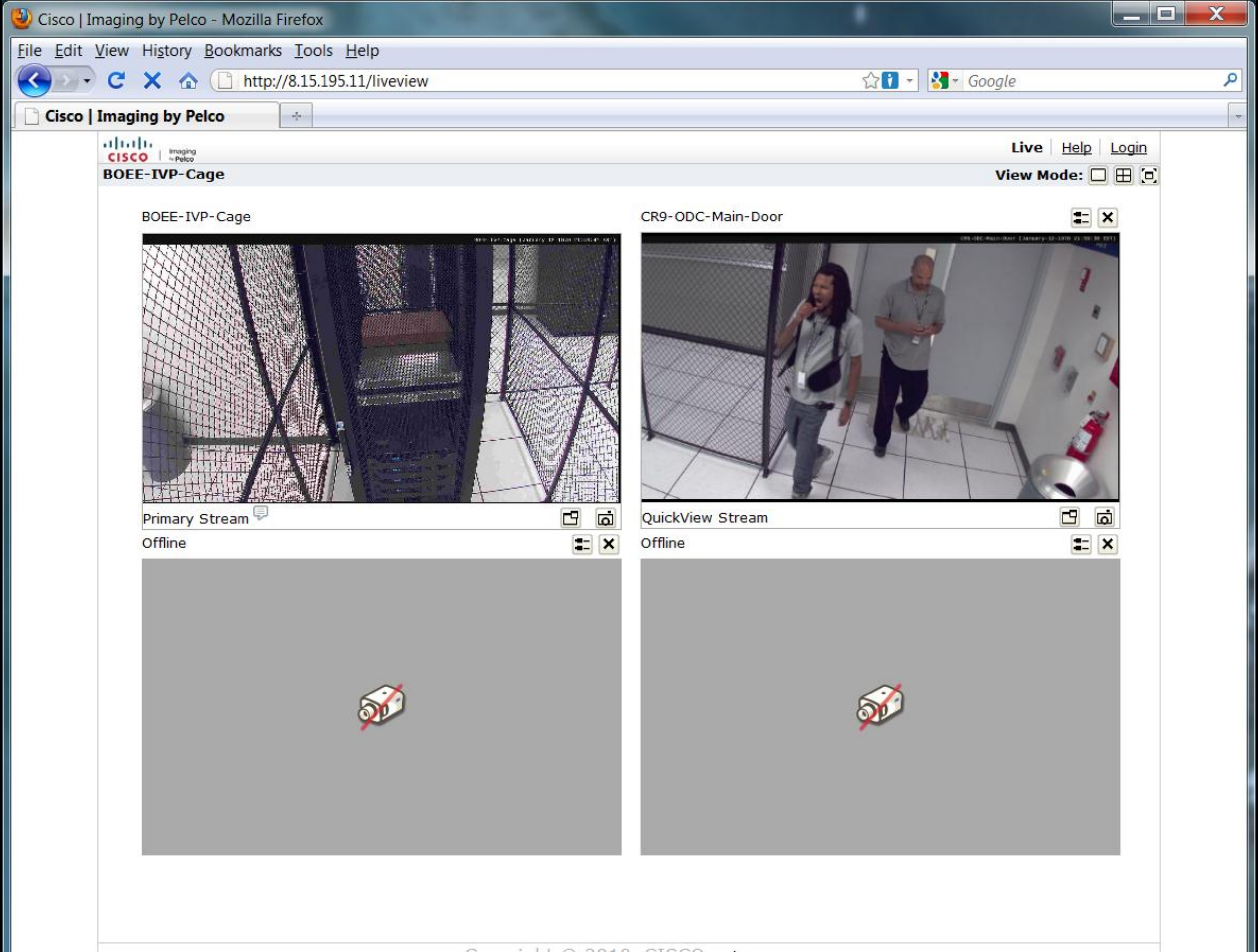
http://8.15.195.11/liveview

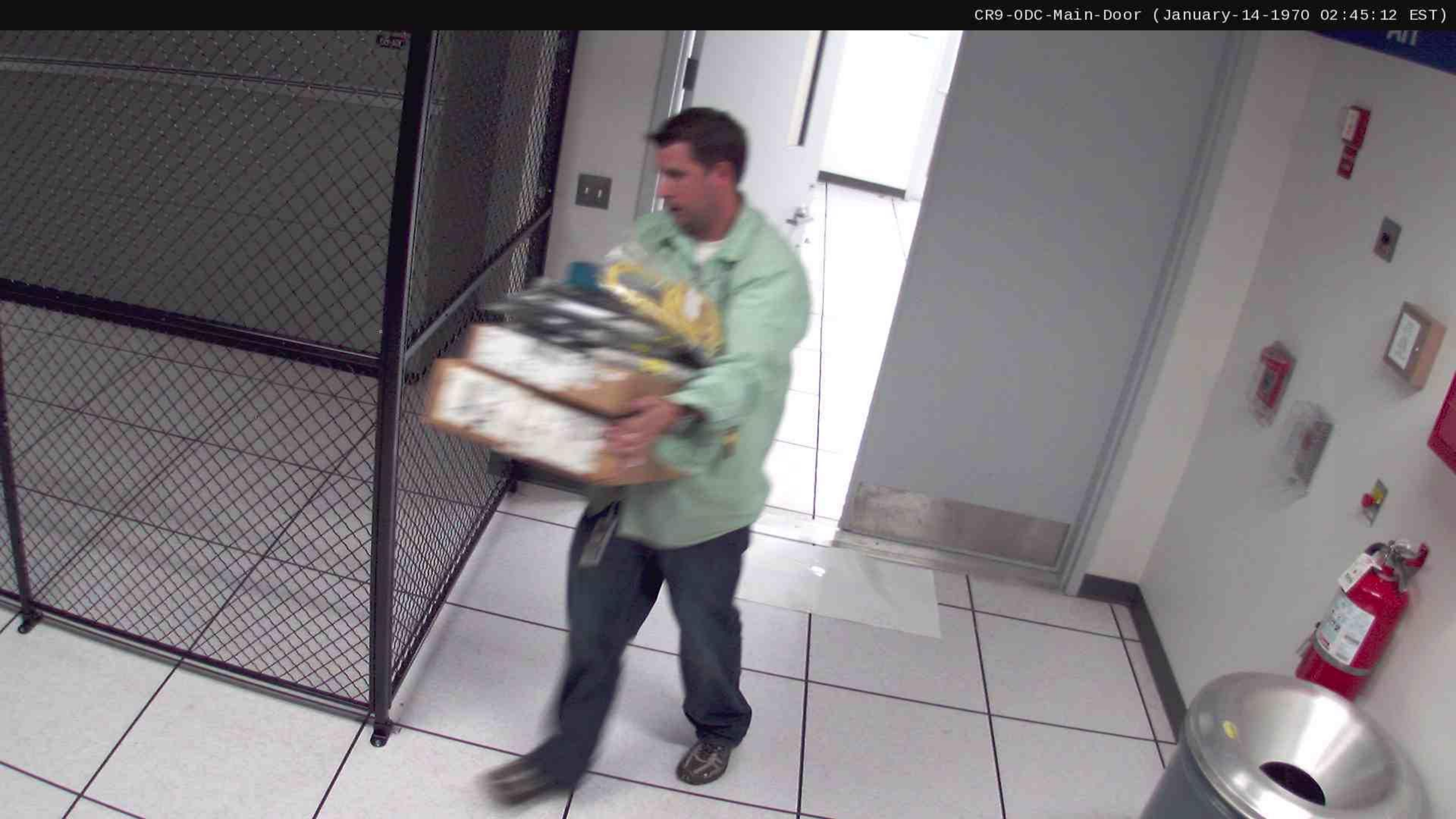
BOEE-IVP-Cage

BOEE-IVP-Cage

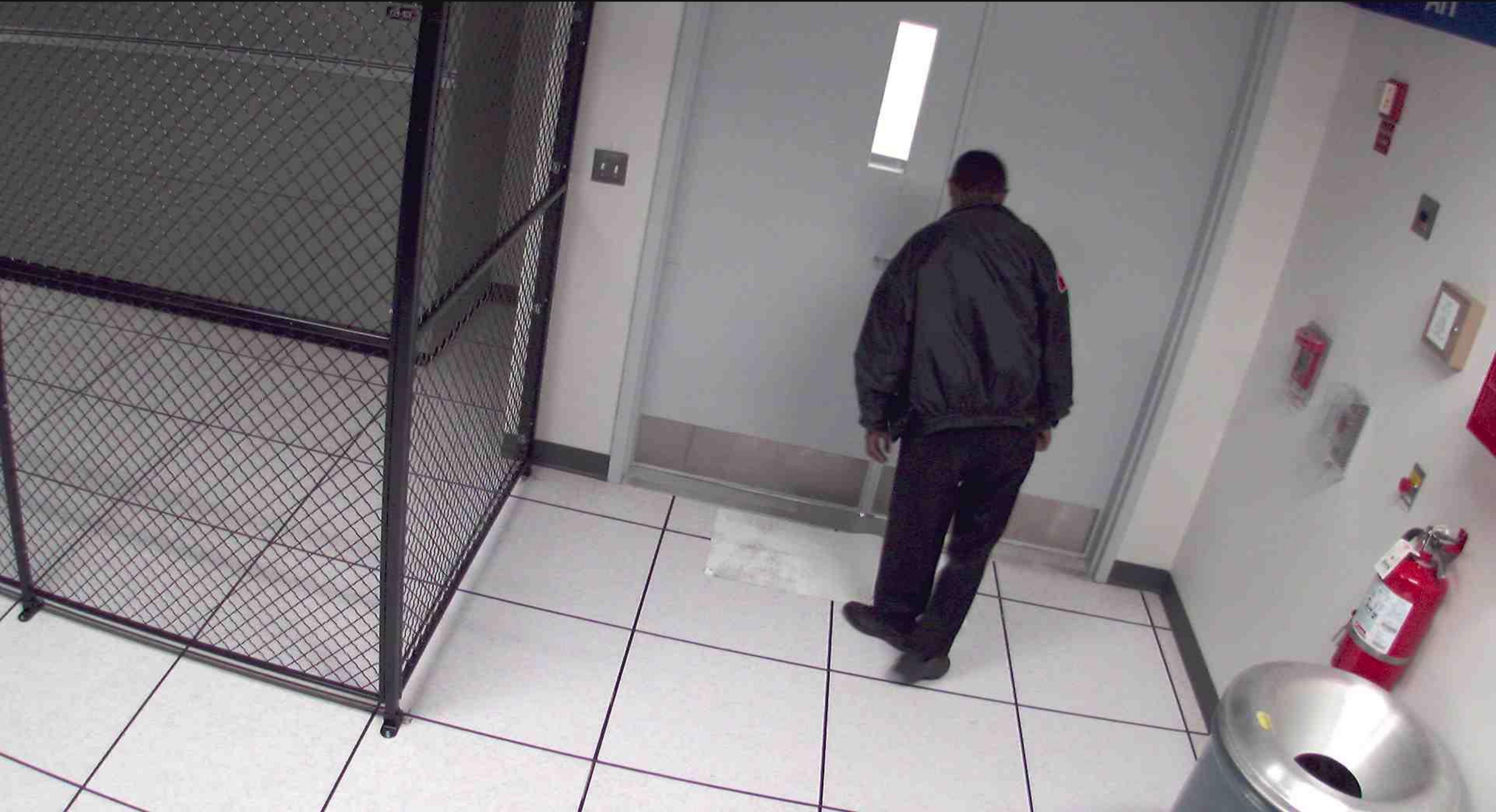
BOCE-IVP-Cage (January 12 1970 21:51:10 EST)

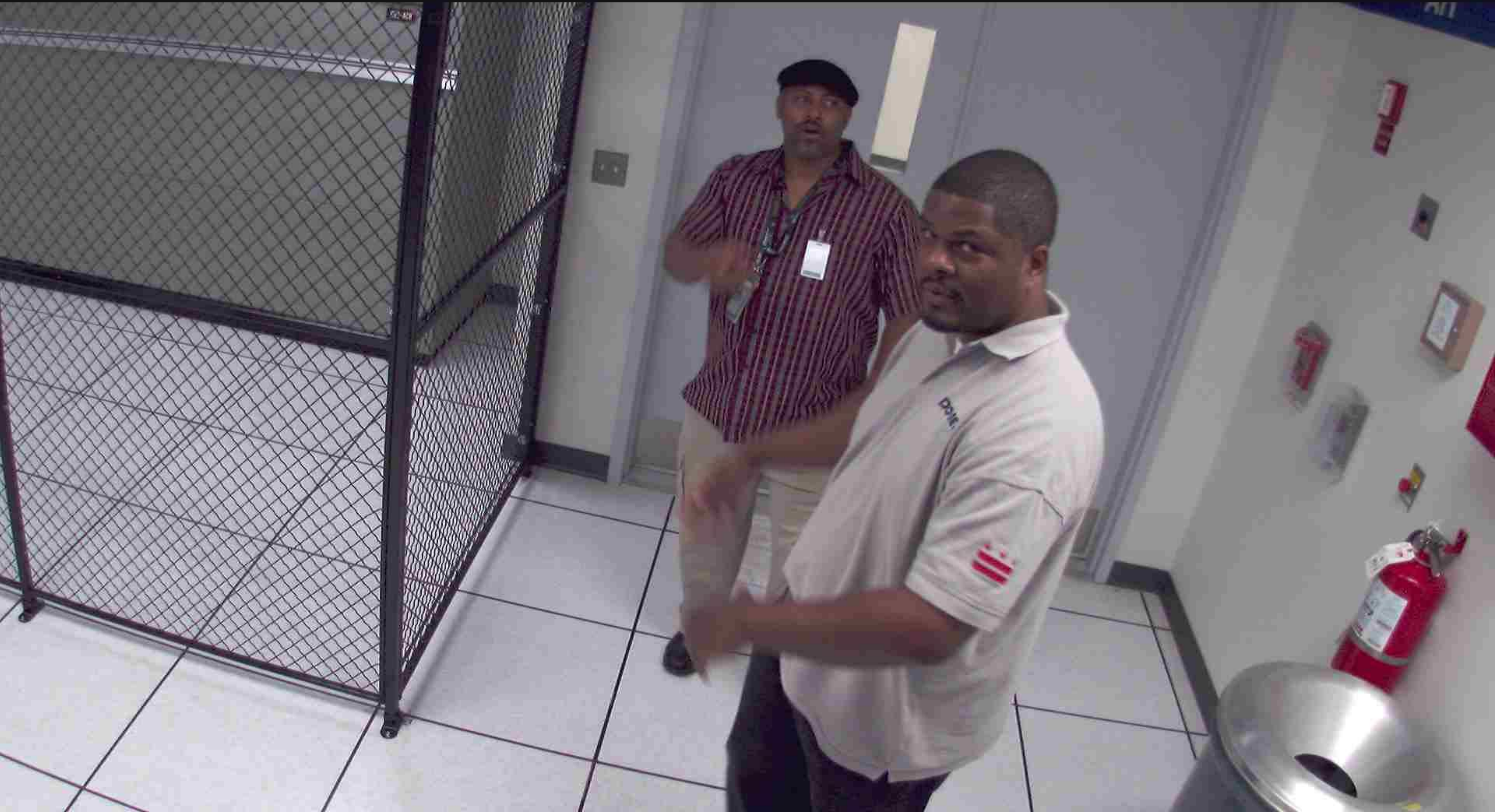
Transferring data from 8.15.195.11...


Cisco | Imaging by Pelco - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://8.15.195.11/liveview
Google
Cisco | Imaging by Pelco
cisco Imaging by Pelco
Live | Help | Login
BOEE-IVP-Cage
View Mode:
BOEE-IVP-Cage
CR9-ODC-Main-Door
Primary Stream
QuickView Stream
Offline
Offline

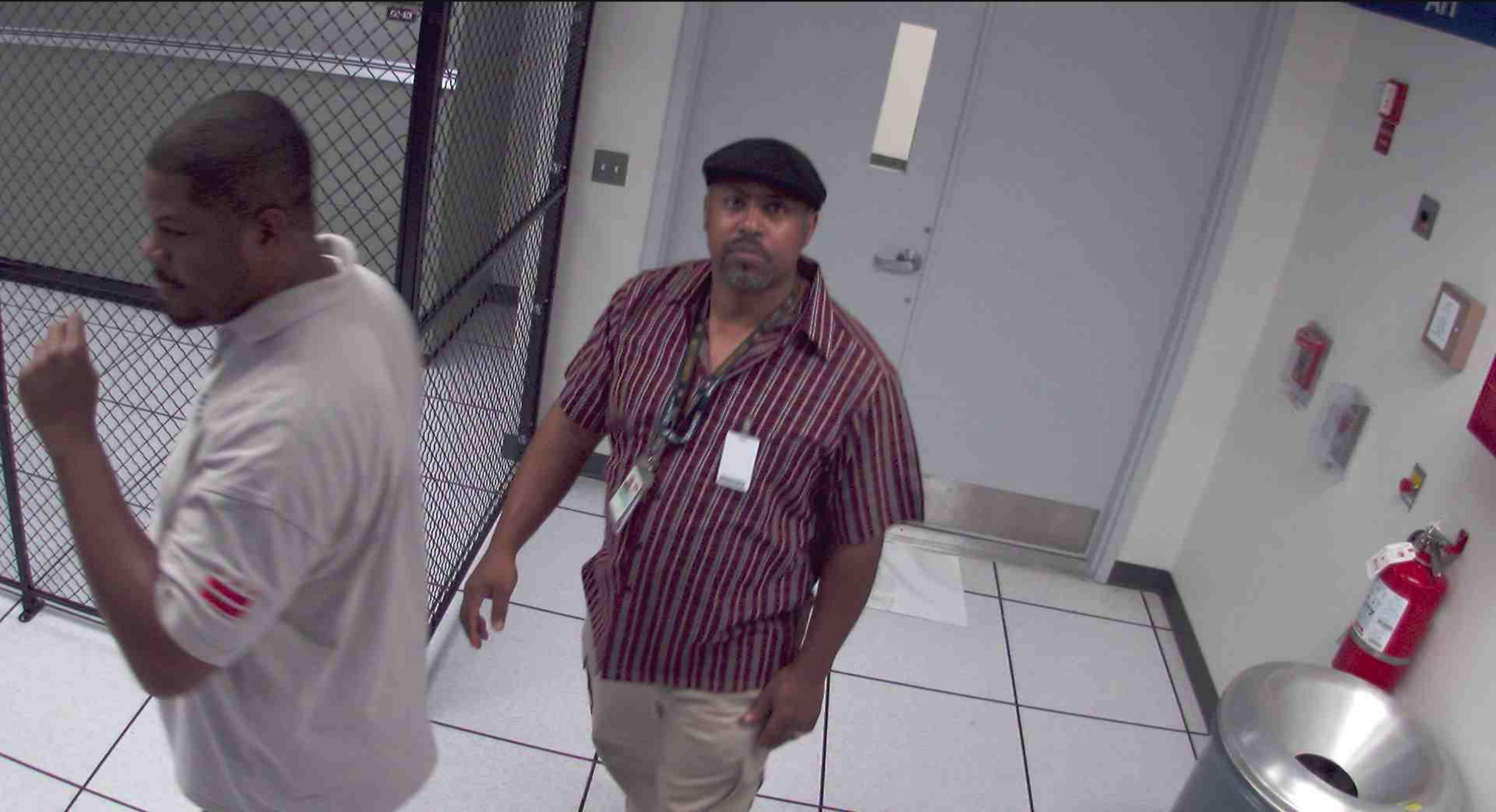

CR9-ODC-Main-Door (January-14-1970 02:45:12 EST)

CR9-ODC-Main-Door (January-14-1970 06:14:51 EST)

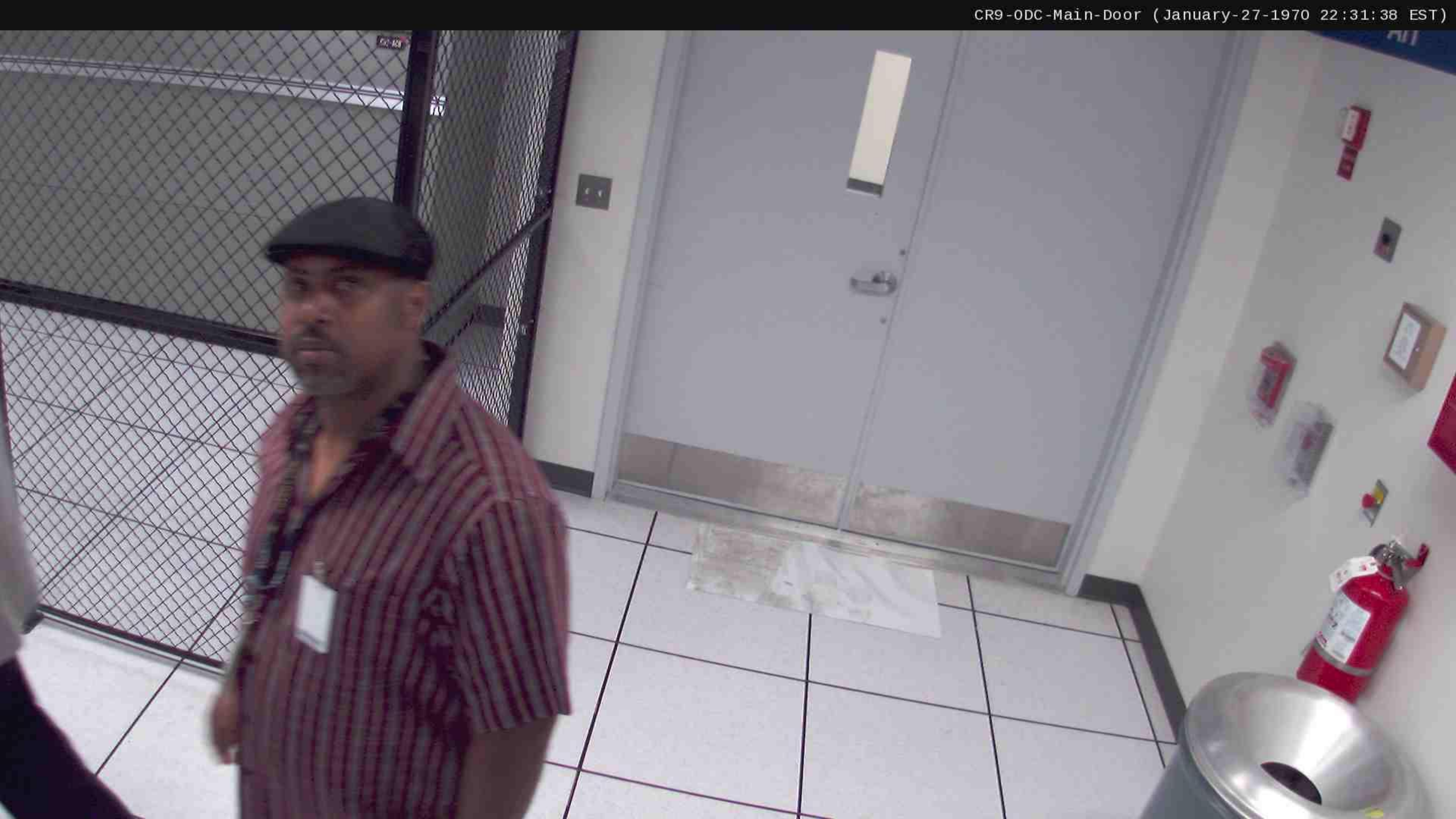




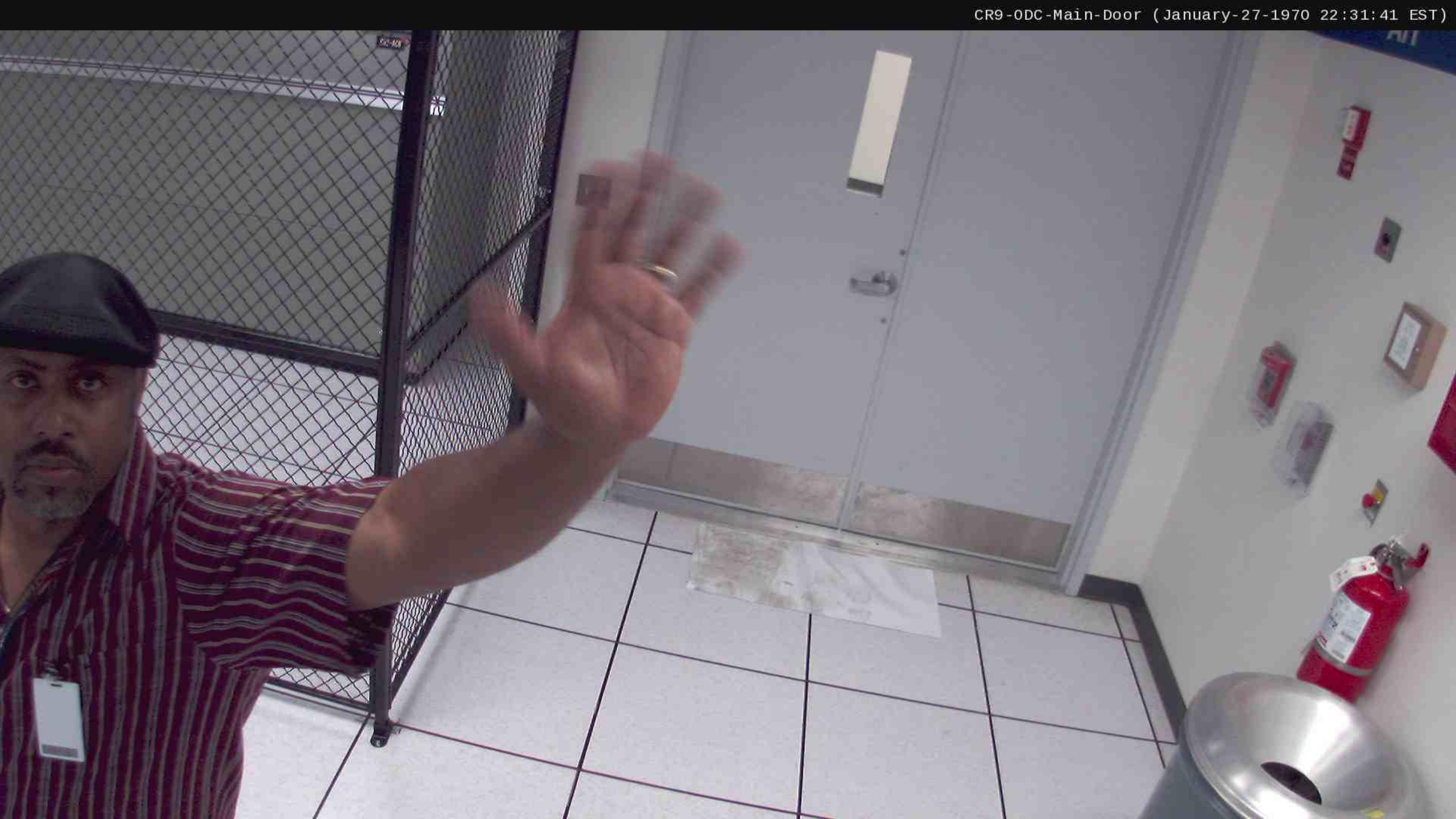
CR9-ODC-Main-Door (January-27-1970 22:31:35 EST)



CR9-ODC-Main-Door (January-27-1970 22:31:37 EST)



CR9-ODC-Main-Door (January-27-1970 22:31:38 EST)

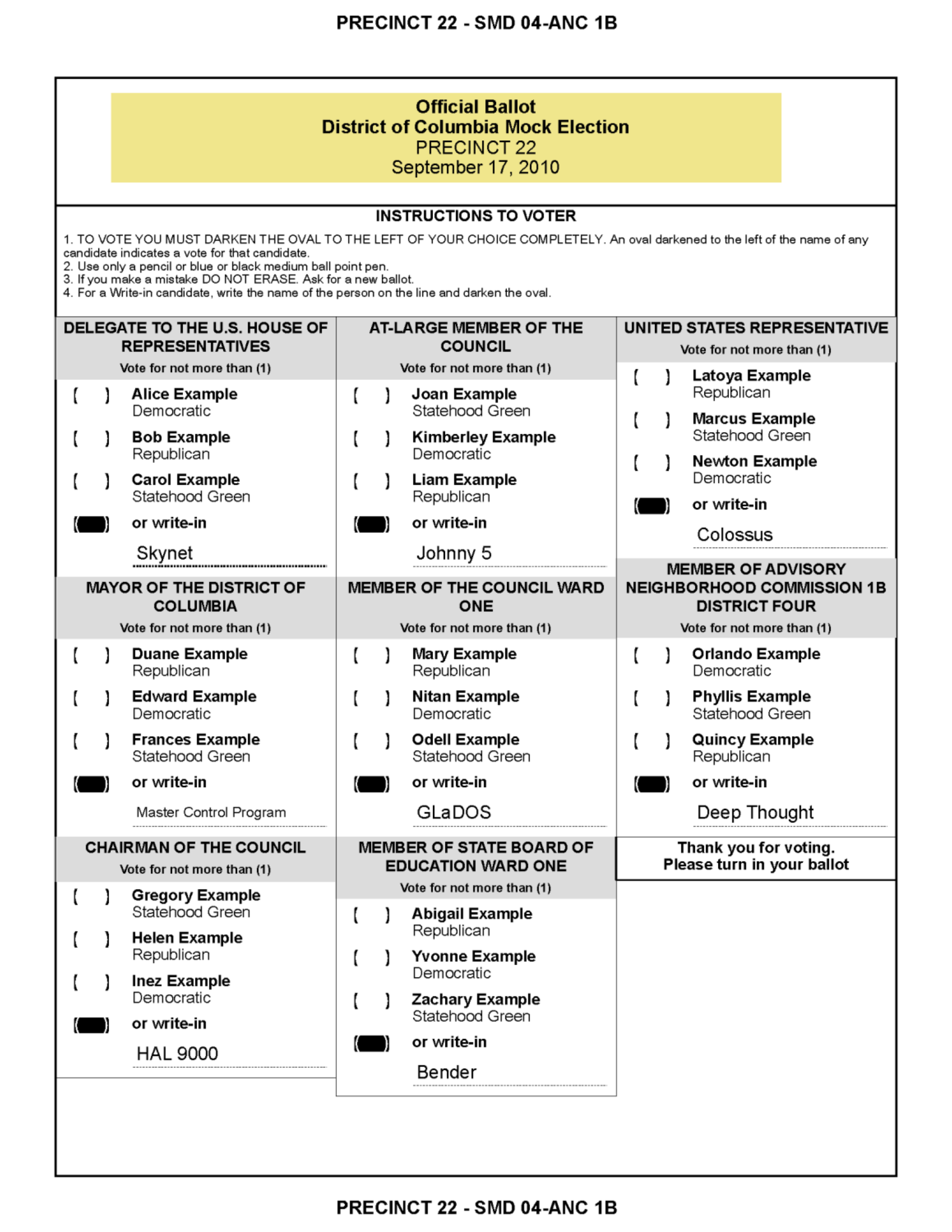


CR9-ODC-Main-Door (January-27-1970 22:31:41 EST)

ATTACK!

Steal database credentials, keys, logs, etc.

Replace all existing votes with our choices



PRECINCT 22 - SMD 04-ANC 1B

Official Ballot
District of Columbia Mock Election
PRECINCT 22
September 17, 2010

INSTRUCTIONS TO VOTER

1. TO VOTE YOU MUST DARKEN THE OVAL TO THE LEFT OF YOUR CHOICE COMPLETELY. An oval darkened to the left of the name of any candidate indicates a vote for that candidate.
2. Use only a pencil or blue or black medium ball point pen.
3. If you make a mistake DO NOT ERASE. Ask for a new ballot.
4. For a Write-in candidate, write the name of the person on the line and darken the oval.

DELEGATE TO THE U.S. HOUSE OF REPRESENTATIVES
Vote for not more than (1)

○ **Alice Example**
Democratic

○ **Bob Example**
Republican

○ **Carol Example**
Statehood Green

● **or write-in**
Skynet

MAYOR OF THE DISTRICT OF COLUMBIA
Vote for not more than (1)

○ **Duane Example**
Republican

○ **Edward Example**
Democratic

○ **Frances Example**
Statehood Green

● **or write-in**
Master Control Program

CHAIRMAN OF THE COUNCIL
Vote for not more than (1)

○ **Gregory Example**
Statehood Green

○ **Helen Example**
Republican

○ **Inez Example**
Democratic

● **or write-in**
HAL 9000

AT-LARGE MEMBER OF THE COUNCIL
Vote for not more than (1)

○ **Joan Example**
Statehood Green

○ **Kimberley Example**
Democratic

○ **Liam Example**
Republican

● **or write-in**
Johnny 5

MEMBER OF THE COUNCIL WARD ONE
Vote for not more than (1)

○ **Mary Example**
Republican

○ **Nitan Example**
Democratic

○ **Odell Example**
Statehood Green

● **or write-in**
GLaDOS

MEMBER OF STATE BOARD OF EDUCATION WARD ONE
Vote for not more than (1)

○ **Abigail Example**
Republican

○ **Yvonne Example**
Democratic

○ **Zachary Example**
Statehood Green

● **or write-in**
Bender

UNITED STATES REPRESENTATIVE
Vote for not more than (1)

○ **Latoya Example**
Republican

○ **Marcus Example**
Statehood Green

○ **Newton Example**
Democratic

● **or write-in**
Colossus

MEMBER OF ADVISORY NEIGHBORHOOD COMMISSION 1B DISTRICT FOUR
Vote for not more than (1)

○ **Orlando Example**
Democratic

○ **Phyllis Example**
Statehood Green

○ **Quincy Example**
Republican

● **or write-in**
Deep Thought

Thank you for voting.
Please turn in your ballot

PRECINCT 22 - SMD 04-ANC 1B

Steal database credentials, keys, logs, etc.

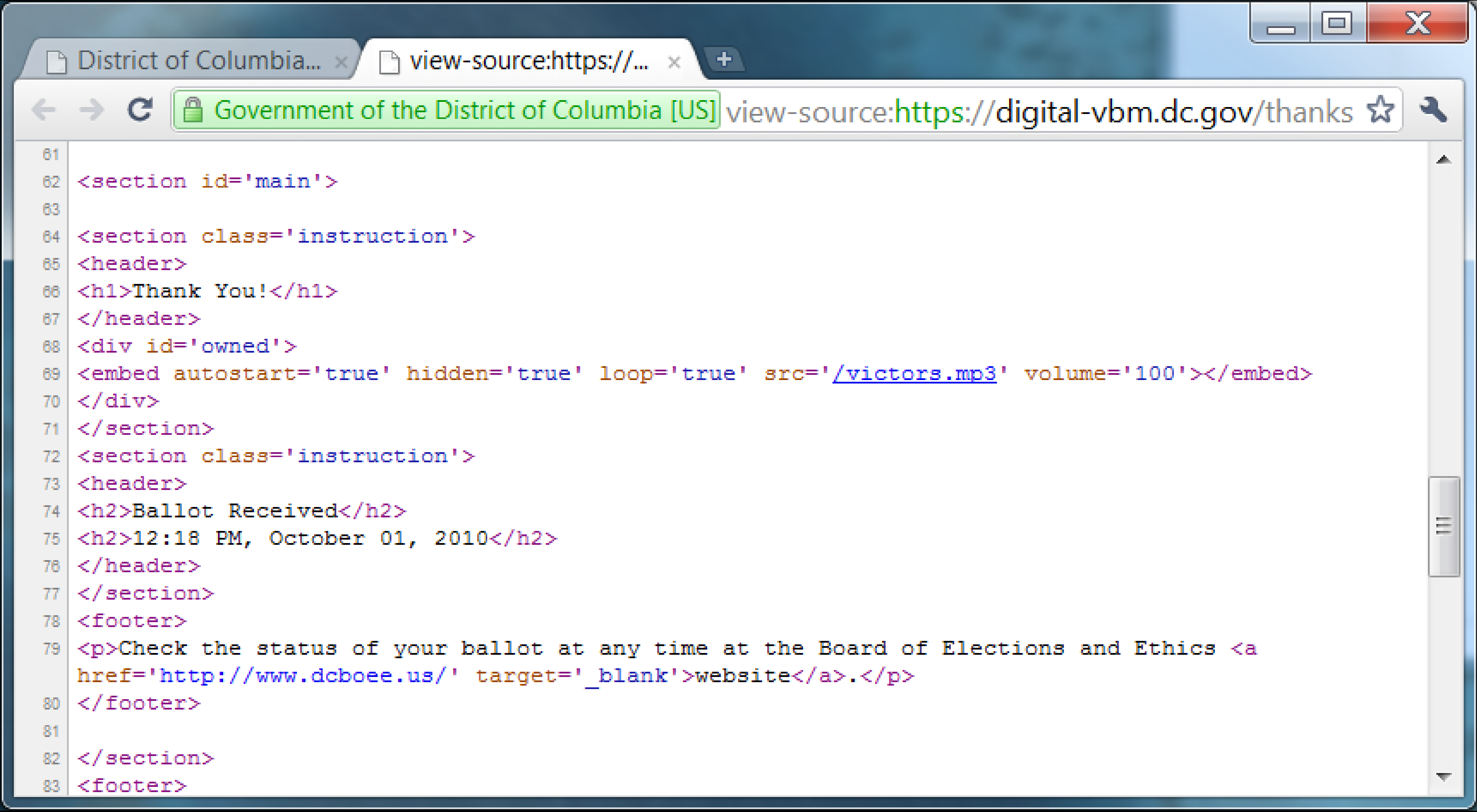
Replace all existing votes with our choices

Replace any new votes

Back door to reveal new votes

Clear logs

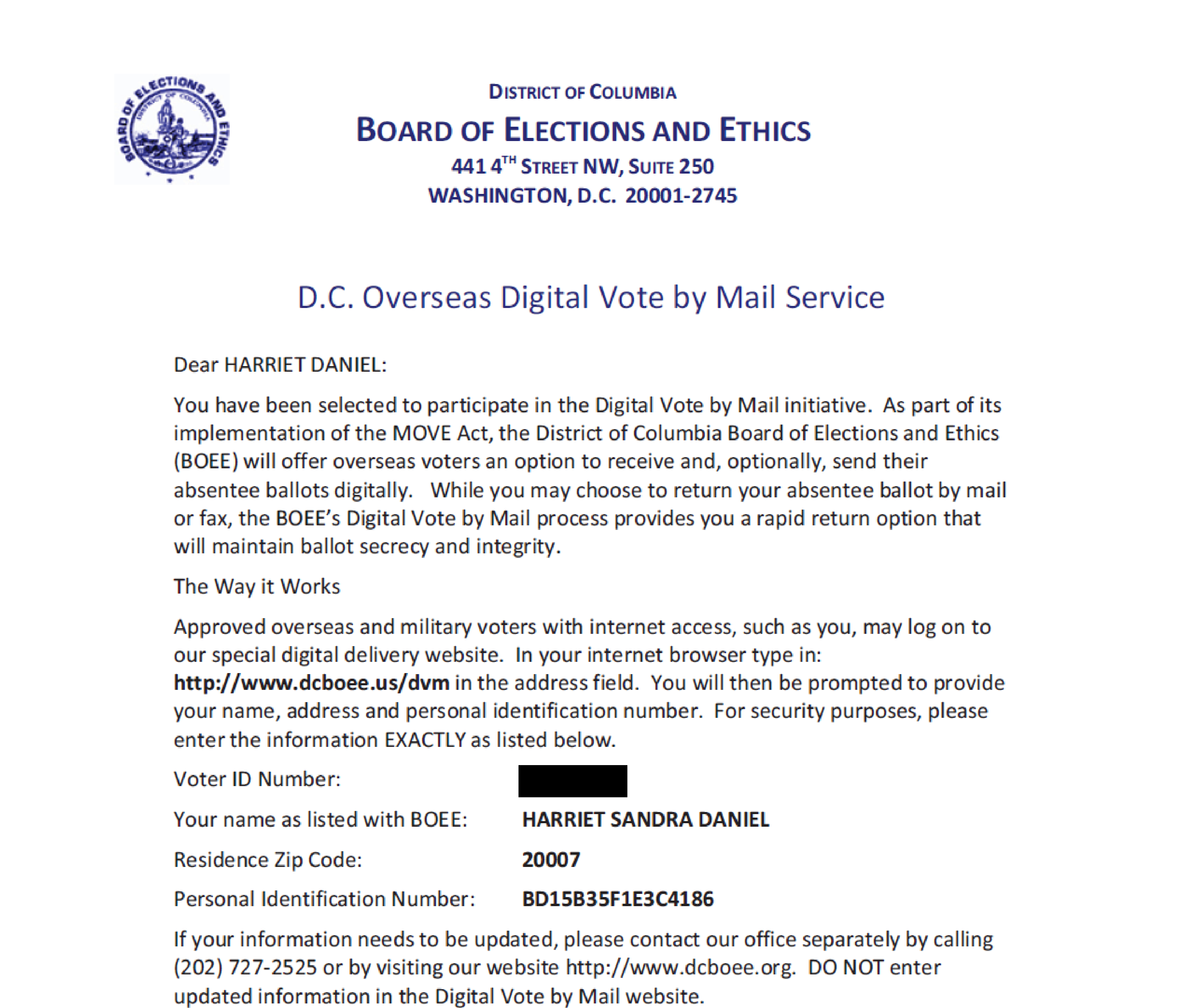
“Calling card”



District of Columbia...
view-source:https://...
Government of the District of Columbia [US]
view-source:https://digital-vbm.dc.gov/thanks

```

<section id='main'>

<section class='instruction'>
<header>
<h1>Thank You!</h1>
</header>
<div id='owned'>
<embed autostart='true' hidden='true' loop='true' src='/victors.mp3' volume='100'></embed>
</div>
</section>
<section class='instruction'>
<header>
<h2>Ballot Received</h2>
<h2>12:18 PM, October 01, 2010</h2>
</header>
</section>
<footer>
<p>Check the status of your ballot at any time at the Board of Elections and Ethics <a href='http://www.dcboee.us/' target='_blank'>website</a>.</p>
</footer>

</section>
<footer>
```

One more thing…



DISTRICT OF COLUMBIA

BOARD OF ELECTIONS AND ETHICS

441 4TH STREET NW, SUITE 250
WASHINGTON, D.C. 20001-2745

D.C. Overseas Digital Vote by Mail Service

Dear HARRIET DANIEL:

You have been selected to participate in the Digital Vote by Mail initiative. As part of its implementation of the MOVE Act, the District of Columbia Board of Elections and Ethics (BOEE) will offer overseas voters an option to receive and, optionally, send their absentee ballots digitally. While you may choose to return your absentee ballot by mail or fax, the BOEE's Digital Vote by Mail process provides you a rapid return option that will maintain ballot secrecy and integrity.

The Way it Works

Approved overseas and military voters with internet access, such as you, may log on to our special digital delivery website. In your internet browser type in: **http://www.dcboee.us/dvm** in the address field. You will then be prompted to provide your name, address and personal identification number. For security purposes, please enter the information EXACTLY as listed below.

Voter ID Number:	[redacted]
Your name as listed with BOEE:	**HARRIET SANDRA DANIEL**
Residence Zip Code:	**20007**
Personal Identification Number:	**BD15B35F1E3C4186**

If your information needs to be updated, please contact our office separately by calling (202) 727-2525 or by visiting our website http://www.dcboee.org. DO NOT enter updated information in the Digital Vote by Mail website.

CONCLUSIONS

Web applications tend to be *brittle*

Small mistakes can have huge consequences

Voting is harder to secure than e-commerce

Deep security challenges left to solve

Decades, *if ever,*

before we can vote online securely.

ATTACKING THE WASHINGTON, D.C. INTERNET VOTING SYSTEM

Full paper available at https://jhalderm.com

J. ALEX HALDERMAN
THE UNIVERSITY OF MICHIGAN

MichiganEngineering

Microsoft

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.