DEMOCRACY FORWARD

Re: Public Records Request

1 message

Tsujii, Tim Thu, May 28, 2026 at 3:33 PM

Good Afternoon,

Thank you for your email inquiry. I've passed along the records request to the Board Members listed and will coordinate their response and materials in a combined email. In the meantime, I've completed a search of all of my emails for any of the referenced external entities and have attached a zip file with those requested emails and attachments.

Please let me know if you have any questions or if I can be of further assistance.

All the best,
Tim

Tim Tsujii
Director of Elections | Forsyth County Board of Elections
201 N. Chestnut Street | Winston-Salem, NC 27101
(336) 703-2801 desk | (336) 727-2893 fax
www.fcvotes.com
connect with us on @fcvotes
FORSYTH COUNTY BOARD OF ELECTIONS
Forsyth County Government

Book time to meet with me

From: FOIA Requests
Sent: Tuesday, May 26, 2026 2:04 PM
To: FC Votes <fcvotes@forsyth.cc>
Subject: Public Records Request

Hello,

Please find the attached public records request. If you have any questions or concerns about fulfilling this request, please let us know as soon as possible. Thank you for your attention to this matter.

Sincerely,
Democracy Forward Foundation

DEMOCRACY FORWARD.zip
6494K

HOW TO RESPOND
WHEN AN ACTIVE SHOOTER IS IN YOUR VICINITY

QUICKLY DETERMINE THE MOST REASONABLE WAY TO PROTECT YOUR OWN LIFE. CUSTOMERS AND CLIENTS ARE LIKELY TO FOLLOW THE LEAD OF EMPLOYEES AND MANAGERS DURING AN ACTIVE SHOOTER SITUATION.

1. Run

- Have an escape route and plan in mind
- Leave your belongings behind
- Keep your hands visible

2. Hide

- Hide in an area out of the active shooter's view.
- Block entry to your hiding place and lock the doors

CALL 911 WHEN IT IS SAFE TO DO SO

3. Fight

- As a last resort and only when your life is in imminent danger.
- Attempt to incapacitate the active shooter
- Act with physical aggression and throw items at the active shooter

HOW TO RESPOND
WHEN LAW ENFORCEMENT ARRIVES ON THE SCENE

1. HOW YOU SHOULD REACT WHEN LAW ENFORCEMENT ARRIVES:

- Remain calm, and follow officers' instructions
- Immediately raise hands and spread fingers
- Keep hands visible at all times
- Avoid making quick movements toward officers such as attempting to hold on to them for safety
- Avoid pointing, screaming and/or yelling
- Do not stop to ask officers for help or direction when evacuating, just proceed in the direction from which officers are entering the premises

2. INFORMATION YOU SHOULD PROVIDE TO LAW ENFORCEMENT OR 911 OPERATOR:

- Location of the victims and the active shooter
- Number of shooters, if more than one
- Physical description of shooter/s
- Number and type of weapons held by the shooter/s
- Number of potential victims at the location

RECOGNIZING SIGNS
OF POTENTIAL WORKPLACE VIOLENCE

AN ACTIVE SHOOTER MAY BE A CURRENT OR FORMER EMPLOYEE. ALERT YOUR HUMAN RESOURCES DEPARTMENT IF YOU BELIEVE AN EMPLOYEE EXHIBITS POTENTIALLY VIOLENT BEHAVIOR. INDICATORS OF POTENTIALLY VIOLENT BEHAVIOR MAY INCLUDE ONE OR MORE OF THE FOLLOWING:

- Increased use of alcohol and/or illegal drugs
- Unexplained increase in absenteeism, and/or vague physical complaints
- Depression/Withdrawal
- Increased severe mood swings, and noticeably unstable or emotional responses
- Increasingly talks of problems at home
- Increase in unsolicited comments about violence, firearms, and other dangerous weapons and violent crimes

Contact your building management or human resources department
for more information and training on active shooter response in your workplace.

Emergency Action Plan Guide
Active Shooter Preparedness

Purpose

The Active Shooter Emergency Action Plan Video is a virtual learning tool that describes the fundamental concepts of developing an Emergency Action Plan (EAP) for an active shooter scenario. This instructive video guides organizations through important considerations of EAP development utilizing the first-hand perspectives of active shooter survivors, first responders, and other subject matter experts who share their unique insights.

Organizations are encouraged to use this guide as a medium to document the *initial steps* toward creating an Active Shooter preparedness plan. This guide *is not* meant to replace your organization's Emergency Action Plan. Rather, it is a tool that begins the EAP development process.

Pre-Planning Recommendations and Suggested Training

- ✓ Does your organization have an emergency action plan? If so, review your organization's policy or process for creating the plan. Determine if an active shooter preparedness plan can fit into your organization's overarching plan which may already include a plan for fire evacuation, severe weather, and bomb threats.
- ✓ Obtain a copy of the Federal Emergency Management Agency's (FEMA) Comprehensive Preparedness Guide (CPG) 101 *"Developing and Maintaining Emergency Operations Plan"* and review the six step planning process.
- ✓ Explore the Department of Homeland Security's Active Shooter Preparedness Website to better understand the active shooter threat.
- ✓ View the Options for Consideration Video to recognize possible actions to take if confronted with an active shooter scenario.
- ✓ Download and review the Active Shooter Preparedness Workshop Series presentations. This six module series contains additional information, instructor notes, and videos that supports the Active Shooter Emergency Action Plan process. The *Planning Steps (1-6)* below will correlate to the Training Modules (1-6) in the presentation slides. *Example: Module 2 will assist with completing Planning Step 2a and 2b.*

How to Use This Guide

Step 1 – Review the pre-planning recommendations and suggested training.

Step 2 – Allot *at least* **2-hours** to complete the Active Shooter Emergency Action Plan video.

Step 3 – Watch the EAP video.

Step 4 – Complete ***Planning Steps 1-6***. Use the fillable space to document the initial steps required to begin developing the organization's Emergency Action Plan. Note: *The Planning Steps contain information derived from the EAP video and other online resources to help inform the planning process.*

Step 5 – Begin drafting the organization's Active Shooter Emergency Action Plan. Refer to the EAP Guide and resources listed in *Pre-Planning Recommendations and Suggested Training* as required.

Need Help? Contact the DHS Active Shooter Preparedness team at ASworkshop@hq.dhs.gov

Planning Step - 1

Form a Collaborative Planning Team

Identify a cross-section of employees to represent your organization. The members should represent a broad perspective and include key segments of the organization. It is recommended that teams contain at least four members to ensure diversity of awareness and less than 10 members to avoid an unmanageable group. The positions listed below are examples of collaborative planning team members. Refer to *CPG 101 page 4-2* for additional information.

Human Resources	Information Technology Managers
Security, Risk or Safety Managers	Legal Advisors
Facility Managers or Engineers	Persons with Disabilities or Functional Needs
First Responders (Police, Fire/EMS)	Communication Managers

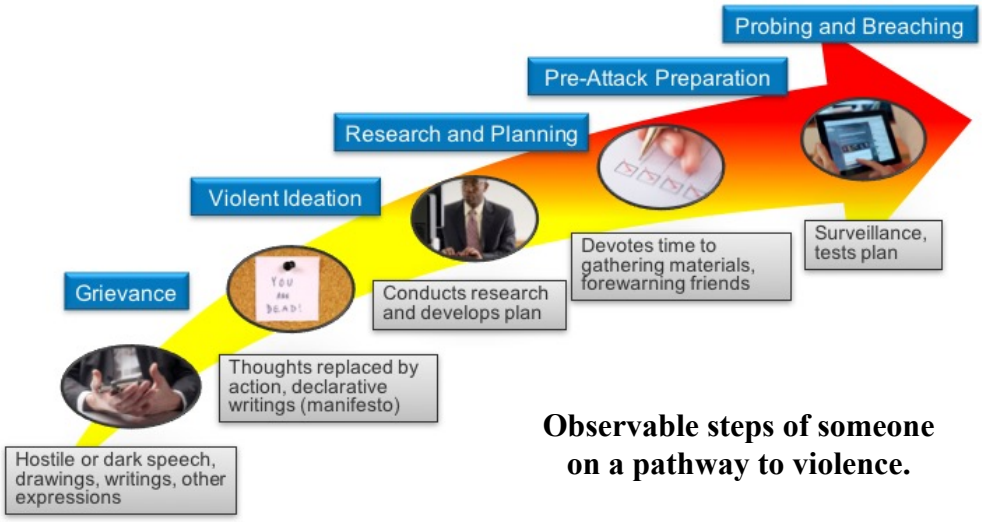
Position	Name	Contact Information

Planning Step – 2a

Develop an Active Shooter Prevention Plan

Effective prevention capabilities encompass three areas: training employees to recognize behaviors on the Pathway to Violence, a system for reporting that is tailored to your organization, and development of intervention capabilities that are trained and resourced to appropriately evaluate potential threats.

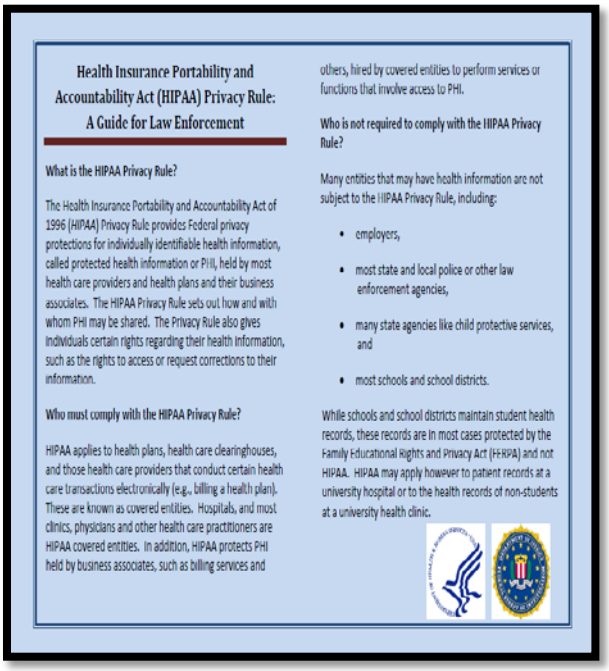
Pathway to Violence Training: The Pathway to Violence Video provides information regarding the behavior indicators that assailants often demonstrate before a violent act. It includes law enforcement expert interviews that discusses engagement strategies and recommended responses. Organizations can also refer to the Pathway to Violence Fact Sheet for additional information. Describe how you will train your organization to recognize the indicators of someone on a pathway to violence.



Observable steps of someone on a pathway to violence.

Reporting Mechanism: Describe the reporting process for your organization. Consider the types of information reportable to supervisors, security, human resources and law enforcement. How will employees know about the reporting process (policy, training, etc.)? How can the organization develop a culture of reporting?

Note: It's very important to consult with legal advisors throughout the planning process. For example, *The Health Insurance Portability and Accountability Act (HIPPA)* and *Family Education Rights and Privacy Act (FERPA)* both have ***exceptions*** that allow for information sharing to protect the health and safety of individuals.



Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement

What is the HIPAA Privacy Rule?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule provides Federal privacy protections for individually identifiable health information, called protected health information or PHI, held by most health care providers and health plans and their business associates. The HIPAA Privacy Rule sets out how and with whom PHI may be shared. The Privacy Rule also gives individuals certain rights regarding their health information, such as the rights to access or request corrections to their information.

Who must comply with the HIPAA Privacy Rule?

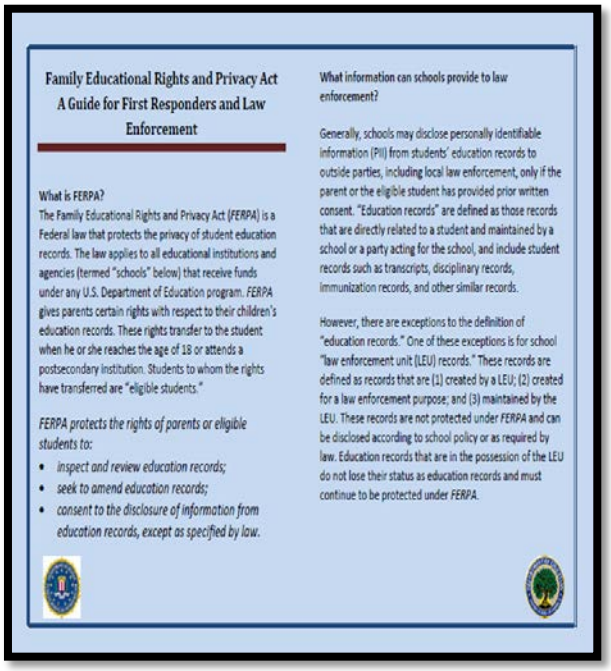
HIPAA applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically (e.g., billing a health plan). These are known as covered entities. Hospitals, and most clinics, physicians and other health care practitioners are HIPAA covered entities. In addition, HIPAA protects PHI held by business associates, such as billing services and others, hired by covered entities to perform services or functions that involve access to PHI.

Who is not required to comply with the HIPAA Privacy Rule?

Many entities that may have health information are not subject to the HIPAA Privacy Rule, including:

- employers,
- most state and local police or other law enforcement agencies,
- many state agencies like child protective services, and
- most schools and school districts.

While schools and school districts maintain student health records, these records are in most cases protected by the Family Educational Rights and Privacy Act (FERPA) and not HIPAA. HIPAA may apply however to patient records at a university hospital or to the health records of non-students at a university health clinic.



Family Educational Rights and Privacy Act A Guide for First Responders and Law Enforcement

What is FERPA?

The Family Educational Rights and Privacy Act (*FERPA*) is a Federal law that protects the privacy of student education records. The law applies to all educational institutions and agencies (termed "schools" below) that receive funds under any U.S. Department of Education program. *FERPA* gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a postsecondary institution. Students to whom the rights have transferred are "eligible students."

FERPA protects the rights of parents or eligible students to:

- *inspect and review education records;*
- *seek to amend education records;*
- *consent to the disclosure of information from education records, except as specified by law.*

What information can schools provide to law enforcement?

Generally, schools may disclose personally identifiable information (PII) from students' education records to outside parties, including local law enforcement, only if the parent or the eligible student has provided prior written consent. "Education records" are defined as those records that are directly related to a student and maintained by a school or a party acting for the school, and include student records such as transcripts, disciplinary records, immunization records, and other similar records.

However, there are exceptions to the definition of "education records." One of these exceptions is for school "law enforcement unit (LEU) records." These records are defined as records that are (1) created by a LEU; (2) created for a law enforcement purpose; and (3) maintained by the LEU. These records are not protected under *FERPA* and can be disclosed according to school policy or as required by law. Education records that are in the possession of the LEU do not lose their status as education records and must continue to be protected under *FERPA*.

Intervention Resources: Describe your organization's process to intervene early and prevent violence.

Does your organization have a Threat Management Team (TMT) to conduct threat evaluations? If not, who should be on your team and how will they be trained? Consider including members from security, human resources, employee assistance and mental health. Learn more about TMT in the Federal Bureau of Investigation's "Making Prevention a Reality: Identifying, Assessing and Managing the Threat of Targeted Attacks" chapter 5.

Threat Management Team / Intervention Resources

Position	Name	Contact Information

Planning Step – 2b

Conduct a Risk Assessment

Organizations should consider all *threats*, *vulnerabilities* and associated *consequences* during their risk assessment. FEMA's CPG 201 "Threat and Hazard Identification and Risk Assessment Guide" is an effective resource to use when conducting risk assessments. Conducting a risk assessment will ensure organizations understand their situation, prioritize their actions, identify and compare options, and effectively allocate their resources.

An important threat for organizations to consider is *Workplace Violence*. Having an effective workplace violence policy can protect lives and prevent legal liability. Ensure your policy supports the Occupational Safety and Health's General Duty Clause.

Estimate the Risk Factors your organization faces:

Do you operate a controversial business?	Do you have security measures on-site or off-site?
Does your business have high-stress positions?	What is your organizations security protocols?
Do you have a history of work place violence or prior threats / incidents?	What is your work environment? (open access to the public, large crowds, high-risk neighbors)

List prior threats and violent incidents:

What is the most likely type of Workplace Violence your organization may encounter? Type 1

TYPE 1: Violent acts by criminals who have no other connection with the workplace, but enter to commit robbery or another crime.

TYPE 2: Violence directed at employees by customers, clients, patients, students, inmates, or any others for whom an organization provides services.

TYPE 3: Violence against coworkers, supervisors, or managers by a present or former employee.

TYPE 4: Violence committed in the workplace by someone who doesn't work there, but has a personal relationship with an employee—an abusive spouse or domestic partner.

Planning Step - 3

Establish Goals and Objectives

Goals are broad statements of what personnel, equipment and resources are supposed to achieve. Objectives lead to achieving goals and determining the actions that participants in the process must accomplish. Goals and objectives are key to determining operational priorities and resources required to achieve a needed capability.

Active Shooter preparedness goals and objectives may vary depending on an organization's security posture, physical environment and available resources. Consider the following to determine what goals and objectives are needed in your organization. Use the space provided to describe additional goals and objectives.

Access control

- Updated access rosters
- Lockdown procedures
- Shelter in place (door locks)

Notification

- Employees
- Visitors
- Disabled (Seeing / Hearing impaired)
- Non-English speakers

Evacuation

- Routes
- People with disabilities
- Rally points

Emergency responder coordination

- Organization liaison
- Go-bags (facility maps, master keys, etc)

Accountability

- Reporting procedures

Communications management

- First responders / incident commander
- Survivors
- Family
- Media

Short-term recovery

- Hours
- Days
- Weeks

Long-term recovery

- Months
- Years
- Anniversary

Describe a security/response goal and objective. Include the resources your organization needs to achieve the goals (without regard for the resource availability). CPG-101 (page 4-11)

Goal

Objective

Resource

Example:

Goal: *Achieve 100% notification and acknowledgement of Run-Hide-Fight message among all personnel. Conduct immediate accessible messaging or notification by all methods, including texting and pop-up notification on the computer.*

Objective: *Immediately initiate emergency notification protocol, to include proliferation of Run-Hide-Fight message via all available mediums, such as telephone, pager, email, SMS, MMS, public announcements systems, desktop/website banners, social media, etc. Encourage acknowledgment of message when feasible/prudent for accountability purposes. Utilize all communications methods to notify all persons of an active shooter incident within a short period onset.*

Resource: *Accessible notification software, public address system, captioning, outgoing texting through emergency notification in the area. New technologies being developed that may be applicable.*

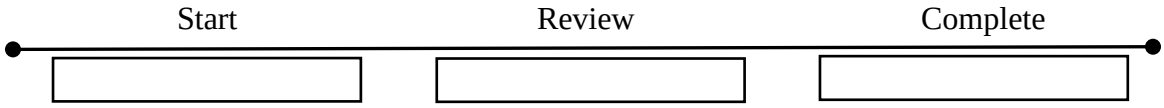
Planning Step - 4

Assess Courses of Action

Organizations must develop and analyze courses of action (COA) that accomplish specific goals and objectives. The COA should have a desired outcome that is measurable and incorporates an organization-wide focus. Assign the COA development to a member of the organization and include a timeline with decision points.

Describe at least two courses of action supporting the goal and objective listed in *Planning Step – 3* along with an anticipated timeline. CPG-101 (page 4-12)

Timeline: Establish preliminary start, review, and completion dates to establish expected timeframe.



COA #1 – Assigned to:

COA #2 – Assigned to:

Example:

COA 1: *Utilize computer screen with real-time caption pop-up announcements, "All-Call" alert for staff.*

COA 2 : *Sent a text to all employees "Run, Hide, Fight – Active Shooter on premises".*

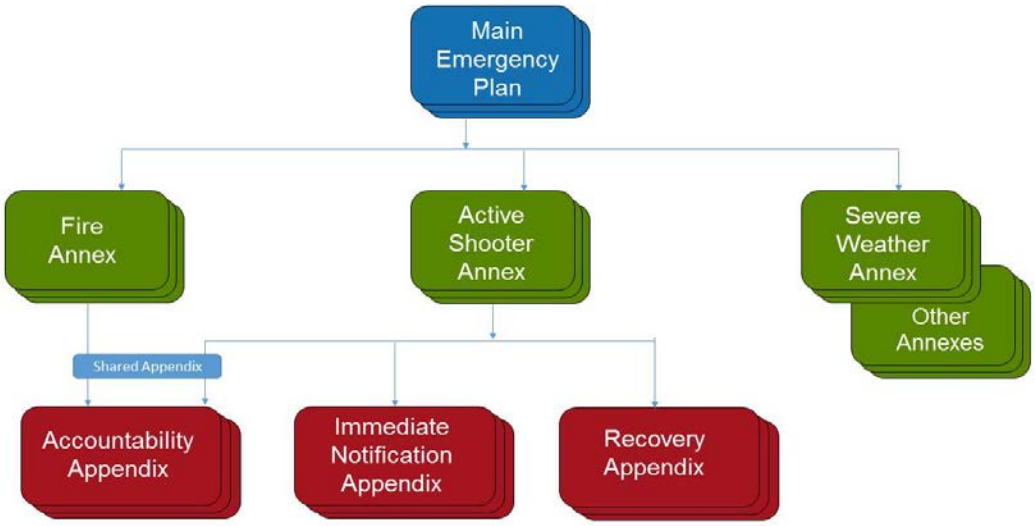
Planning Step - 5

Draft Plan and Approve

A planning team's main concern is to develop an Emergency Action Plan that includes all essential information and instructions that protect against an Active Shooter. CPG 101 (pages 3-1 & 4-16) recommends a format that users understand, are comfortable with, and can extract the information they need. Organizations are encouraged to use the Active Shooter Emergency Action Plan Template if they do not have an established format.

Draft the Plan

Determine if the Active Shooter plan will stand alone or supplement a main emergency plan. As seen below, organizations typically have a main emergency plan with annexes that cover specific hazards.

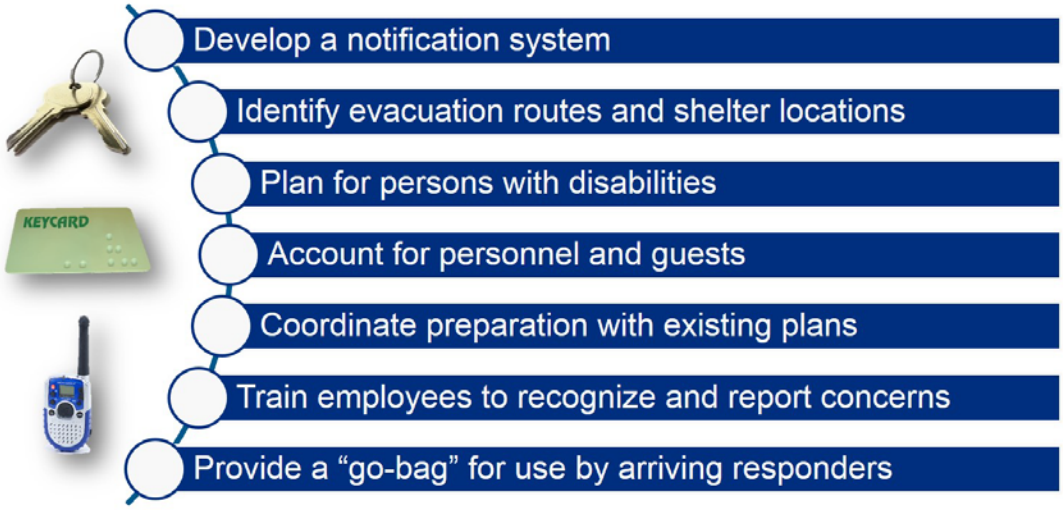


Recommended Rules for Drafting Plans – CPG 101 (page 4-16)

- Keep the language simple and use short sentences in active voice.
- Summarize important information with checklists and visual aids, such as maps and flowcharts.
- Avoid using jargon and minimize the use of acronyms.
- Provide enough detail to convey an easily understood plan that is actionable.
- Format the plan so that readers can quickly find solutions and options.
- Provide mission guidance and avoid discussing policy.
- Ensure accessibility by developing alternate formats: e.g. print, electronic, video.

Validate the Plan and Prepare for Approval – CPG 101 (page 4-17)

Check to ensure the written plan supports all goals and objectives developed by the planning group. Coordinate with a legal adviser to confirm plan supports all local, state, and federal regulatory and statutory requirements including Americans with Disabilities Act (ADA) mandates.



Approve and Disseminate

Staff the plan through the organization's official approval process. This will ensure all relevant staff have input and organization-wide support before senior leadership approval. Once approved, ensure widest dissemination possible using various communication channels. The next step is to begin training and exercising the plan.

Planning Step - 6

Training and Exercise

Train

After an Emergency Action Plan is approved and disseminated, organizations should train their personnel so they have the knowledge, skills, and abilities to perform the tasks identified in the plan. Training can be accomplished in a variety of ways including new employee orientation, "All Hands" meetings, conferences and workshops, newsletters and internal broadcasts, and online courses.

Describe ways your organization can train.

Useful FEMA Online Independent Study Courses

IS 906
Workplace Security Awareness

IS 907
Active Shooter: What You Can Do

IS 914
Surveillance Awareness: What You Can Do

IS 915
Protecting Critical Infrastructure Against Insider Threat

Exercise

Evaluating the effectiveness of plans involves a combination of training events and exercises to determine whether the goals, objectives, decisions, actions, and timing outlined in the plan led to a successful response. Conducting regular exercises help organizations discover resource gaps, develop individual performance, improve coordination with local, state, and federal partners, and identify opportunity for improvement. FEMA's Homeland Security Exercise and Evaluation Program (HSEEP) provides a set of guiding principles for exercise programs. Organizations can use HSEEP to develop, execute, and evaluate exercises that address their Active Shooter preparedness.

In addition, the DHS Sector-Specific Tabletop Exercise Program (SSTEP) provides an exercise planning resource to assist critical infrastructure owners and operators design their organization's tabletop exercise. Contact the Stakeholder Readiness and Exercise Section at sopd.exercise@hq.dhs.gov for more information.

Develop a time line to accomplish the milestones displayed to the right. Leveraging this "crawl, walk, run" method helps organizations prepare their staff and improve their plan.

Remember – Planning is a Process of Continuous Improvement.

Emergency Action Plan: Active Shooter

Organization:

Address:

City, State, Zipcode:

Phone number:

Website:

Applicability and Scope

The objective of this emergency action plan template is to help organizations prepare their personnel for active shooter scenarios. This template documents basic information recommended for an effective emergency action plan. Organizations are encouraged to consider their unique circumstances and/or structure to ensure a more comprehensive plan. It applies to permanent employees, temporary employees, contractors, and visitors associated with this organization.

This plan should be updated when information listed below requires modification. The crisis manager will review this plan for accuracy on a reoccurring basis. Time frame:

Key Individuals / Teams

The organization's primary/alternate crisis manager responsible for this plan.

	Position/Office	Name	Phone Number	E-mail
P				
A				
A				
A				
A				

The following people will participate in developing the active shooter emergency action plan. Together, they will form the ***Active Shooter Planning Team*.**

Position/Office	Name	Phone Number	E-mail

Emergency Action Plan: Active Shooter

The following personnel are responsible for conducting threat evaluations and intervening to reduce workplace violence. Together, they form the ***Threat Management Team***.

Position/Office	Name	Phone Number	E-mail

The following are external partners that will participate in active shooter planning.

Organization	Name	Phone Number	E-mail

It is critical that only authorized personnel are granted access to the organization's facilities. This requires human resources, physical security and information security teams to collaborate. The following personnel are responsible for ensuring access rosters are regularly updated.

Position/Office	Name	Phone Number	E-mail

Emergency Action Plan: Active Shooter

Lockdown Procedures

The following are responsible for initiating lockdown procedures (primary & alternate).

	Position/Office	Name	Phone Number	E-mail
P				
A				
A				
A				
A				

Lockdown procedures are initiated in the following manner:

Notification

The following are responsible for ensuring the organization has an effective process to announce the presence of an active shooter (primary & alternate).

	Position/Office	Name	Phone Number	E-mail
P				
A				
A				
A				
A				

The following methods are used to announce the presence of an active shooter.

Message displayed in all notifications:

Emergency Action Plan: Active Shooter

Contacting 9-1-1 immediately is critical to ensuring first responders arrive quickly. The notification team should be trained to accurately describe the incident to 9-1-1 call centers. The following information will be provided to 9-1-1.

Employees will be notified in the following manner:

Visitors will be notified in the following manner:

Emergency Action Plan: Active Shooter

Employees and visitors that are seeing impaired will be notified in the following manner:

Employees and visitors that are hearing impaired will be notified in the following manner:

Employees that are non-English speakers will be notified in the following manner:

Emergency Action Plan: Active Shooter

Evacuation / Assembly / Accountability

The ability to quickly and safely evacuate is critical to surviving an active shooter scenario. Personnel must be familiar with the evacuation plan and practice using the nearest exit without exposing themselves to danger. They should also be familiar with the location of staging areas.

The following are responsible for ensuring the organization has an evacuation plan (primary & alternate).

	Position/Office	Name	Phone Number	E-mail
P				
A				
A				
A				
A				

The following areas will be checked regularly and updated if required.

- ☐ Building/site maps with designated evacuation routes are located at key locations.
- ☐ Exits are clearly marked.
- ☐ Evacuation plans include the ability to assist people with functional needs.
- ☐ Designated rally points are located a safe distance away.
- ☐ Primary and alternate rally points are identified.
- ☐ Employee rosters and contact information are updated regularly.

Conducting timely and accurate accountability is critical during and following an event. This information will prove vital when coordinating with first responders and communicating with concerned family. The following are responsible for conducting accountability (primary / alternate).

	Position/Office	Name	Phone Number	E-mail
P				
A				
A				
A				
A				

Emergency Action Plan: Active Shooter

Listed below are the procedures for conducting accountability. It includes a process to account for employees conducting business away from the facility and those on leave. It also accounts for personnel visiting the organization.

First Responder Coordination

Communicating information to first responders in a timely manner is vital to quickly eliminating the active shooter threat. The following are responsible for providing information to first responders (primary / alternate).

	Position/Office	Name	Phone Number	E-mail
P				
A				
A				
A				
A				

Pre-coordination with local law enforcement ensures the organization understands and is prepared to provide requested information. The local law enforcement contact information is provided below.

	Position/Office	Name	Phone Number	E-mail
P				
A				
A				
A				
A				

Emergency Action Plan: Active Shooter

Local law enforcement requires the following information when responding to an active shooter event.

A first responder “Go-Bag” is a ready resource that assists law enforcement with navigating a facility.

The “Go-Bag” is located at:

The “Go-Bag” contains the following items. It will be inventoried regularly and updated as required.

Communications Management

Providing consistent and accurate information to authorities, employees, family and the media can reduce the impact of an active shooter scenario on an organization and its people. The following are responsible for communicating the organization's message internally and externally.

	Position/Office	Name	Phone Number	E-mail
P				
A				
A				
A				
A				

Emergency Action Plan: Active Shooter

The following are key considerations the communication team must address.

Recovery

Recovery from an active shooter scenario will likely be a whole community effort. It may include hospitals, grief counselors, lawyers, employee assistance, and other assistance as required. The following will be activated as needed.

Organization	Name	Phone Number	E-mail

Business Continuity

Does your organization have a business continuity plan that allows for continuity of operations? This plan includes actions taken if a neighboring organization experiences an active shooter event. It also considers major suppliers and critical components in the supply chain.

The organization has a business continuity plan. ◯ Yes ◉ No

Emergency Action Plan: Active Shooter

Training

Providing the necessary training for all employees is important to this plan's success. Training should include "Run, Hide, Fight" to prepare individuals. Individuals listed in the plan should also be trained to carry out their responsibilities. The organization should also involve neighboring organizations, business affiliates, and first responders in their training.

The following are responsible for ensuring all stakeholder are trained (primary & alternate).

	Position/Office	Name	Phone Number	E-mail
P				
A				
A				
A				
A				

A list of required training is provided below.

Training	Location (portal, www, in-house, etc.)

This plan was last reviewed.

This plan is approved.

Outlook

[External] U.S. Department of Homeland Security - Elections Outreach

From Aspey, Darryl <darryl.aspey@HQ.DHS.GOV>
Date Mon 7/23/2018 8:03 AM
To Aspey, Darryl <darryl.aspey@HQ.DHS.GOV>

3 attachments (3 MB)

Election Infrastructure Security Practices Checklist (Final) 30April2018....pdf; Election Outreach.pdf; Incident Handling Elections Final 508.pdf;

Good Morning,

I am following up on the email from the North Carolina Board of Elections Executive Director, Kim Strach, regarding the Department of Homeland Security's, Elections Infrastructure Outreach.

The Department of Homeland Security's (DHS) Office of Infrastructure Protection (IP) leads the national effort to secure critical infrastructure from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community. The DHS Election Infrastructure Outreach is one of many initiatives that IP leads in an effort to increase the security and resilience of the nation's critical infrastructure. The Election Infrastructure refers to assets, systems, and networks most critical to the security and resilience of the election process.

DHS offers a broad range of services and programs to help secure the Election Infrastructure. These programs and services are free and are provided upon request. As a Protective Security Advisor with DHS, I would like to discuss some of the programs, training and other resources available to you and your organization. Some of the additional products that I would like to discuss include security-preparedness considerations to protect Elections Infrastructure facilities, enhancing or developing active shooter plans and training, explosives awareness training, communications, and cyber security related programs.

I have attached a few documents that you may find helpful and I will look forward to meeting and talking to you about our programs.

Regards,

Darryl

Darryl Aspey
Protective Security Advisor
U.S. Department of Homeland Security
North Carolina District – Charlotte
919-208-7448

darryl.aspey@hq.dhs.gov

Outlook

RE: [External] U.S. Department of Homeland Security - Elections Outreach

From Aspey, Darryl <darryl.aspey@HQ.DHS.GOV>
Date Thu 11/14/2019 8:08 PM
To Tim Tsujii <tsujiidt@forsyth.cc>

Tim,

Thank you for the follow-up information. It was a pleasure meeting you and your team today, you have a great office and you have implemented several commendable measures to enhance security.

Regards,

Darryl

Darryl Aspey
Protective Security Advisor
Region IV North Carolina District - Charlotte
Cybersecurity and Infrastructure Security Agency
Cell: 919-208-7448
Email: darryl.aspey@hq.dhs.gov

From: Tim Tsujii <tsujiidt@forsyth.cc>
Sent: Thursday, November 14, 2019 2:12 PM
To: Aspey, Darryl <darryl.aspey@HQ.DHS.GOV>
Cc: Michelle Bobadilla <bobadimb@forsyth.cc>
Subject: Re: [External] U.S. Department of Homeland Security - Elections Outreach

Darryl,

It was a pleasure meeting with you today and really appreciate your help in conducting the site assessment for our facilities. Per your request, I am providing you with Captain Charles Bean's email address (charles.bean@aus.com) and have attached a copy of our emergency contingency plan. Please let me know if you have any questions or if I can be of further help in completing the survey for our assessment.

Thank you again and I look forward to hearing from you soon.

All the best,

Tim Tsujii
Director of Elections | Forsyth County Board of Elections
201 N. Chestnut Street | Winston-Salem, NC 27101
(336) 703-2801 desk | (336) 727-2893 fax
www.fcvotes.com

connect with us: [redacted] [redacted]

[redacted] [redacted]

On Mon, Jul 23, 2018 at 12:44 PM Aspey, Darryl <darryl.aspey@hq.dhs.gov> wrote:

Good Morning,

I am following up on the email from the North Carolina Board of Elections Executive Director, Kim Strach, regarding the Department of Homeland Security's, Elections Infrastructure Outreach.

The Department of Homeland Security's (DHS) Office of Infrastructure Protection (IP) leads the national effort to secure critical infrastructure from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community. The DHS Election Infrastructure Outreach is one of many initiatives that IP leads in an effort to increase the security and resilience of the nation's critical infrastructure. The Election Infrastructure refers to assets, systems, and networks most critical to the security and resilience of the election process.

DHS offers a broad range of services and programs to help secure the Election Infrastructure. These programs and services are free and are provided upon request. As a Protective Security Advisor with DHS, I would like to discuss some of the programs, training and other resources available to you and your organization. Some of the additional products that I would like to discuss include security-preparedness considerations to protect Elections Infrastructure facilities, enhancing or developing active shooter plans and training, explosives awareness training, communications, and cyber security related programs.

I have attached a few documents that you may find helpful and I will look forward to meeting and talking to you about our programs.

Regards,

Darryl

Darryl Aspey
Protective Security Advisor
U.S. Department of Homeland Security
North Carolina District – Charlotte
919-208-7448
darryl.aspey@hq.dhs.gov


Homeland
Security

Outlook

DHS/CISA Follow-up Information

From Aspey, Darryl <darryl.aspey@HQ.DHS.GOV>
Date Wed 11/20/2019 6:07 PM
To Tim Tsujii <tsujiidt@forsyth.cc>; bobadimb@forsyth.cc <bobadimb@forsyth.cc>

10 attachments (5 MB)

active-shooter-emergency-action-plan-Guide 112017-508v2.pdf; active-shooter-emergency-action-plan-template-112017-508.pdf; active_shooter_poster_508.pdf; active-shooter-how-to-respond-508.pdf; dhs-pathway-to-violence-09-15-16-508.pdf; Mail Security.pdf; See-Say Partnership 1-pager FINAL_8_11_17.pdf; dhs-doj-bomb-threat-guidance-brochure-2016-508.pdf; dhs-bomb-threat-checklist-2014-508.pdf; SeeSay-Indicator-Infographic-final-508.pdf;

Tim and Michelle,

Thanks again for taking the time to meet with me last week. , I have attached the information that we discussed, and the following information includes some links that I think you will find helpful, as you continue to enhance your security posture. Your facility and the procedures that you have implemented are well done. I hope to have your survey completed this week.

DHS Active Shooter Program Resources:

DHS has incorporated three new resources within the DHS active shooter preparedness website
https://www.dhs.gov/active-shooter-workshop-participant

“Active Shooter Emergency Action Plan Guide” The guide supplements the 90-minute emergency action planning video to more effectively assist the critical infrastructure community in developing emergency action plans in a more structured approach (attached).

“Active Shooter Emergency Action Plan Template” The template provides a simple to use fillable format for organizations to leverage if they currently do not have a plan in place (attached).

“Pathway to Violence Video” The video provides information regarding behavioral indicators that are often exhibited prior to an attack. The video details the actions that individuals can take to help thwart an incident and references other resources available. The video also includes law enforcement expert interviews that discuss engagement strategies and recommended responses to someone potentially on a pathway to violence. -
https://www.dhs.gov/pathway-violence-video

Online Active Shooter Course: https://training.fema.gov/is/courseoverview.aspx?code=IS-907
****Note:** Participants will have to establish a Student Identification Number (SID) to take this and other free courses.

See Something Say Something:

The following link will take you to the “See Something Say Something” information.
https://www.dhs.gov/see-something-say-something/campaign-materials
Protect Your Every Day PSA

Homeland security begins with hometown security. This PSA seeks to empower everyday citizens to protect their neighbors and the communities they call home by recognizing and reporting suspicious activity. Across the country, we all play a role in keeping each other safe.
You can also click the following - Protect Your Ever Day Video PSAs and it will take you directly to the video:

Protect Your Every Day Video PSAs
English Radio: 90 sec.

Mail Handling
Suspicious Mail Handling:
https://www.dhs.gov/sites/default/files/publications/Mail_Handling_Document_NonFOUO%209-27-2012.pdf
Suspicious Mail: https://about.usps.com/securing-the-mail/suspiciousmail.htm

Business Continuity Planning Suite
With the goal of helping a business or organization better prepare to minimize disruption of service and maintain normal business operations during an emergency or crisis, the Business Continuity Planning Suite aims to create, update, or improve an organization's business continuity plan.

DHS Office for Bombing Prevention - https://cdp.dhs.gov/obp
FEMA Student ID Number required
Virtual Instructor Led Training (VILT) courses provide general awareness level counter-improvised explosive device (C-IED) information to a broad audience through an on-line virtual training experience with a live instructor. These courses enhance participants' awareness and capability to prevent, protect against, respond to, and mitigate attacks that use IEDs against people, critical infrastructure, and other soft targets.

Bomb Threat Video - https://www.dhs.gov/what-to-do-bomb-threat

Homeland Security Information Network:
How to Join the Homeland Security Information Network (HSIN):

HSIN access is based on nomination and acceptance into one or more Communities of Interest (COIs). Your COI is the Commercial Sector.

To apply for access to HSIN-CI, please submit the information below via email to HSINCI@hq.dhs.gov:

•Full name
•Organization
•Phone number
•Official work email address
•Critical infrastructure sector you support and are requesting access to (Government Sector – Elections Infrastructure)

Communications:
https://www.dhs.gov/safecom/resources-library

Government Emergency Telecommunications Service (GETS)
https://www.dhs.gov/gets

Wireless Priority Service (WPS)
https://www.dhs.gov/wps

Telecommunications Service Priority (TSP)
https://www.dhs.gov/tsp

Please don’t hesitate to call or email me if you have any questions.

Regards,

Darryl

Darryl Aspey
Protective Security Advisor
Region IV North Carolina District - Charlotte
Cybersecurity and Infrastructure Security Agency
Cell: 919-208-7448
Email: darryl.aspey@hq.dhs.gov

Homeland Security

Election Infrastructure Outreach Security Checklist

April 3, 2018

This baseline security practices checklist is intended only as a guide; it is not a requirement under any regulation or legislation. This checklist was developed using Federal Emergency Management Agency (FEMA), FEMA 426, Reference Manual to Mitigate Terrorist Attacks Against Buildings (December 2003) Building Vulnerability Assessment Checklist (Pages 1-45 to 1-93) with a specific focus on items relevant to Government Sector, Elections Infrastructure Sub-Sector facilities. The Department of Homeland Security, Office of Infrastructure Protection's (DHS IP) Rapid Survey Tool (RST) Notebook (2018) and Infrastructure Survey Tool (IST) Version-5 (2016) were also used to identify focus areas. The checklist is organized using the 13 major section areas from the FEMA 426 checklist.

Prior to any visit, checklist users should also become familiar with the additional reference materials from U.S. Department of Commerce, National Institute of Standards and Technology (NIST) and Election Center (National Association of Election Officials). The items highlighted in the references are relevant to the protection of Elections Infrastructure Sub-Sector sites to include information technology systems.

SITE				
Does the terrain place the building in a depression or low area?	*FEMA-426 1.2*	Yes ☐	No ☐	N/A ☐
In dense, urban areas, does curb lane parking allow uncontrolled vehicles to park unacceptably close to a building in public rights-of-way?	*FEMA-426 1.3*	Yes ☐	No ☐	N/A ☐
Is a perimeter fence or other types of barrier controls in place?	*FEMA-426 1.4*	Yes ☐	No ☐	N/A ☐
Is vehicle traffic separated from pedestrian traffic on the site?	*FEMA-426 1.5*	Yes ☐	No ☐	N/A ☐
Is there vehicle and pedestrian access control at the perimeter of the site?	*FEMA-426 1.7*	Yes ☐	No ☐	N/A ☐
Is there any potential access to the site or building through utility paths or water runoff?	*FEMA-426 1.9*	Yes ☐	No ☐	N/A ☐
Does the facility have one or more avenues of high speed approach? (Page-23)	*RST Notebook*	Yes ☐	No ☐	N/A ☐
Does the facility use barriers to mitigate a high speed avenue of approach? (Page-23)	*RST Notebook*	Yes ☐	No ☐	N/A ☐
Are perimeter barriers capable of stopping vehicles?		Yes ☐	No ☐	N/A ☐
Will the vehicle barriers at the perimeter and building maintain access for emergency responders, including large fire apparatus? *[Existing barriers don't hamper first responders]*	*FEMA-426 1.12*	Yes ☐	No ☐	N/A ☐
Does site circulation prevent high-speed approaches by vehicles?	*FEMA-426 1.13*	Yes ☐	No ☐	N/A ☐
Are there offsetting vehicle entrances from the direction of a vehicle's approach to force a reduction of speed?	*FEMA-426 1.14*	Yes ☐	No ☐	N/A ☐
Can any vehicle be placed (legally or illegally) within 400 feet of the facility? (Page-23)	*RST Notebook*	Yes ☐	No ☐	N/A ☐
Does the facility use barriers to enforce standoff? (Page-24)	*RST Notebook*	Yes ☐	No ☐	N/A ☐
Is there a minimum setback distance between the building and parked vehicles?	*FEMA-426 1.15*	Yes ☐	No ☐	N/A ☐
Does adjacent surface parking on site maintain a minimum stand-off distance?	*FEMA-426 1.16*	Yes ☐	No ☐	N/A ☐
Do standalone, aboveground parking garages provide adequate visibility across as well as into and out of the parking garage?	*FEMA-426 1.17*	Yes ☐	No ☐	N/A ☐

Are garage or service area entrances for employee permitted vehicles protected by suitable anti-ram devices?	*FEMA-426 1.18*	Yes ☐	No ☐	N/A ☐
Do site landscaping and street furniture provide hiding places?	*FEMA-426 1.19*	Yes ☐	No ☐	N/A ☐
Is the site lighting adequate from a security perspective in roadway access and parking areas?	*FEMA-426 1.20*	Yes ☐	No ☐	N/A ☐
Is the illumination of fences, gates, and parking areas similar and uniform in type with overlapping light pattern coverage in most areas? (Page-25)	*RST Notebook*	Yes ☐	No ☐	N/A ☐
Is the illumination of building entrance and delivery areas similar and uniform in type with overlapping light pattern coverage in most areas? (Page-25)	*RST Notebook*	Yes ☐	No ☐	N/A ☐
Are line-of-sight perspectives from outside the secured boundary to the building and on the property along pedestrian and vehicle routes integrated with landscaping and green space?	*FEMA-426 1.21*	Yes ☐	No ☐	N/A ☐
Do signs provide control of vehicles and people?	*FEMA-426 1.22*	Yes ☐	No ☐	N/A ☐

ARCHITECTURAL				
Does the site and architectural design incorporate strategies from a Crime Prevention Through Environmental Design (CPTED) perspective?	*FEMA-426 2.1*	Yes ☐	No ☐	N/A ☐
Is it a mixed-tenant building?	*FEMA-426 2.2*	Yes ☐	No ☐	N/A ☐
Are there trash receptacles and mailboxes in close proximity to the building that can be used to hide explosive devices?	*FEMA-426 2.4*	Yes ☐	No ☐	N/A ☐
Do entrances avoid significant queuing *[waiting in line]?*	*FEMA-426 2.5*	Yes ☐	No ☐	N/A ☐
Does security screening cover all public and private areas?	*FEMA-426 2.6*	Yes ☐	No ☐	N/A ☐
Are public and private activities separated?		Yes ☐	No ☐	N/A ☐
Are public and private activities separated?		Yes ☐	No ☐	N/A ☐
Are public toilets, service spaces, or access to stairways and elevators located in any non-secure areas, including the queuing area before screening at the public entrance?		Yes ☐	No ☐	N/A ☐
Is access control provided through main entrance points for employees and visitors?	*FEMA-426 2.7*	Yes ☐	No ☐	N/A ☐
Is access to private and public space or restricted area space clearly defined through the design of the space, signage, use of electronic security devices, etc.?	*FEMA-426 2.8*	Yes ☐	No ☐	N/A ☐
Is access to elevators distinguished as to those that are designated only for employees and visitors?	*FEMA-426 2.9*	Yes ☐	No ☐	N/A ☐
Do [pedestrian] circulation routes have unobstructed views of people approaching controlled access points? *[Pedestrian flow facilitates visual detection and monitoring of unauthorized personnel approaching]*	*FEMA-426 2.13*	Yes ☐	No ☐	N/A ☐
Is roof access limited to authorized personnel by means of locking mechanisms?	*FEMA-426 2.14*	Yes ☐	No ☐	N/A ☐

Are high-value or critical assets located as far into the interior of the building as possible and separated from the public areas of the building?	*FEMA-426 2.16*	Yes ☐	No ☐	N/A ☐
Is high visitor activity away from critical assets?	*FEMA-426 2.17*	Yes ☐	No ☐	N/A ☐
Are critical assets located in spaces that are occupied 24 hours per day?	*FEMA-426 2.18*	Yes ☐	No ☐	N/A ☐
Are assets located in areas where they are visible to more than one person?		Yes ☐	No ☐	N/A ☐
Are mailrooms located away from building main entrances, areas containing critical services, utilities, distribution systems, and important assets?	*FEMA-426 2.20*	Yes ☐	No ☐	N/A ☐
Is the mailroom located near the loading dock?		Yes ☐	No ☐	N/A ☐
Does the mailroom have adequate space available for equipment to examine incoming packages and for an explosive disposal container?	*FEMA-426 2.21*	Yes ☐	No ☐	N/A ☐
Are areas of refuge *[safe rooms/areas]* identified, with special consideration given to egress?	*FEMA-426 2.22*	Yes ☐	No ☐	N/A ☐
Do interior barriers differentiate level of security within a building?	*FEMA-426 2.25*	Yes ☐	No ☐	N/A ☐
Is interior glazing *[glass]* near high-risk areas minimized?	*FEMA-426 2.27*	Yes ☐	No ☐	N/A ☐
Is interior glazing *[glass]* in other areas shatter-resistant?		Yes ☐	No ☐	N/A ☐

STRUCTURAL SYSTEMS				
Will the loading dock design limit damage to adjacent areas and vent explosive force to the exterior of the building?	*FEMA-426 3.10*	Yes ☐	No ☐	N/A ☐
Are mailrooms, where packages are received and opened for inspection, and unscreened retail spaces designed to mitigate the effects of a blast on primary vertical or lateral bracing members?	*FEMA-426 3.11*	Yes ☐	No ☐	N/A ☐

BUILDING ENVELOPE				
Does the facility have ground floor windows (less than 18 feet from the ground)? (Page-17)	*RST Notebook*	Yes ☐	No ☐	N/A ☐
Are there protective measures on the ground floor windows for the facility? (Page-17)	*RST Notebook*	Yes ☐	No ☐	N/A ☐

UTILITY SYSTEMS				
Is the incoming water supply in a secure location?	*FEMA-426 5.3*	Yes ☐	No ☐	N/A ☐
Are sewer systems accessible?	*FEMA-426 5.9*	Yes ☐	No ☐	N/A ☐
Are they *[sewer systems]* protected or secured?		Yes ☐	No ☐	N/A ☐
Is the incoming electric service to the building secure?	*FEMA-426 5.17*	Yes ☐	No ☐	N/A ☐
Is the emergency power collocated with the commercial electric service?	*FEMA-426 5.18*	Yes ☐	No ☐	N/A ☐

Are there multiple or redundant locations for the telephone and communications service?	*FEMA-426 5.20*	Yes ☐	No ☐	N/A ☐
Does the fire alarm system require communication with external sources?	*FEMA-426 5.21*	Yes ☐	No ☐	N/A ☐

MECHANICAL SYSTEMS				
Are the intakes and exhausts accessible to the public?	*FEMA-426 6.1*	Yes ☐	No ☐	N/A ☐
Does facility have an air handling system with an external air intake less than or equal to 10 feet from the ground with unrestricted access? (Page-18)	*RST Notebook*	Yes ☐	No ☐	N/A ☐
Is roof access limited to authorized personnel by means of locking mechanisms?	*FEMA-426 6.2*	Yes ☐	No ☐	N/A ☐
Is access to mechanical areas similarly controlled?		Yes ☐	No ☐	N/A ☐
Is there any collective protection for chemical, biological, radiological contamination designed into the building?	*FEMA-426 6.4*	Yes ☐	No ☐	N/A ☐
Are supply, return, and exhaust air systems for critical areas secure?	*FEMA-426 6.12*	Yes ☐	No ☐	N/A ☐
Where are the building automation control centers and cabinets located? Are they in secure areas?	*FEMA-426 6.14*	Yes ☐	No ☐	N/A ☐
Does the control of air handling systems support plans for sheltering in place or other protective approach?	*FEMA-426 6.15*	Yes ☐	No ☐	N/A ☐
Do fire walls and doors maintain their integrity?	*FEMA-426 6.19*	Yes ☐	No ☐	N/A ☐
Do elevators have recall capability and emergency message capability?	*FEMA-426 6.20*	Yes ☐	No ☐	N/A ☐

PLUMBING AND GAS SYSTEMS				
Is their redundancy to the main [water] piping distribution?	*FEMA-426 7.3*	Yes ☐	No ☐	N/A ☐
Where are gas storage tanks located? How are they piped to the distribution system? (above or below ground) *[Are the tanks and distribution systems secure?]*	*FEMA-426 7.5*	Yes ☐	No ☐	N/A ☐

ELECTRICAL SYSTEMS				
Are there any transformers or switchgears located outside the building or accessible from the building exterior?	*FEMA-426 8.1*	Yes ☐	No ☐	N/A ☐
Are they *[transformers or switchgears]* vulnerable to public access? Are they secured?		Yes ☐	No ☐	N/A ☐
Are they *[transformers or switchgears]* secured?		Yes ☐	No ☐	N/A ☐
What is the extent of the external building lighting in utility and service areas and at normal entryways used by the building occupants? *[Is the lighting sufficient?]*	*FEMA-426 8.2*	Yes ☐	No ☐	N/A ☐
How are the electrical rooms secured and where are they located relative to other higher-risk areas, starting with the main electrical distribution room at the service entrance? *[Are the security measures sufficient?]*	*FEMA-426 8.3*	Yes ☐	No ☐	N/A ☐
Are critical electrical systems collocated with other building systems?		Yes ☐	No ☐	N/A ☐

Are critical electrical systems located in areas outside of secured electrical areas?	*FEMA-426 8.4*	Yes ☐	No ☐	N/A ☐
Is security system wiring located separately from electrical and other service systems?	*FEMA-426 8.4*	Yes ☐	No ☐	N/A ☐
How are electrical distribution panels serving branch circuits secured or are they in secure locations?	*FEMA-426 8.5*	Yes ☐	No ☐	N/A ☐
Does emergency backup power exist for all areas within the building or for critical areas only? *[Does backup power serve the entire building?]*	*FEMA-426 8.6*	Yes ☐	No ☐	N/A ☐
Is the emergency power system independent from the normal electrical service, particularly in critical areas?		Yes ☐	No ☐	N/A ☐
Is it *[primary electrical wiring]* collocated with other major utilities?	*FEMA-426 8.7*	Yes ☐	No ☐	N/A ☐
Is there redundancy of distribution to critical areas?		Yes ☐	No ☐	N/A ☐

FIRE ALARM SYSTEMS				
Are critical documents and control systems located in a secure yet accessible location?	*FEMA-426 9.1*	Yes ☐	No ☐	N/A ☐
Where are the fire alarm panels located? Do they allow access to unauthorized personnel?	*FEMA-426 9.2*	Yes ☐	No ☐	N/A ☐
Is there redundant off-premises fire alarm reporting?	*FEMA-426 9.5*	Yes ☐	No ☐	N/A ☐

COMMUNICATIONS AND IT (INFORMATION TECHNOLOGY) SYSTEMS				
Is the main telephone distribution room secure?	*FEMA-426 10.1*	Yes ☐	No ☐	N/A ☐
Does the telephone system have an uninterruptible power supply (UPS)?	*FEMA-426 10.2*	Yes ☐	No ☐	N/A ☐
Where are communication systems wiring closets located? (voice, data, signal, alarm) Are they collocated with other utilities?	*FEMA-426 10.3*	Yes ☐	No ☐	N/A ☐
Are they *[communication systems wiring closets]* in secure areas?		Yes ☐	No ☐	N/A ☐
How is the communications system wiring distributed? (secure chases and risers, accessible public areas) *[Is the communications wiring system secure?]*	*FEMA-426 10.4*	Yes ☐	No ☐	N/A ☐
Are there redundant communications systems available?	*FEMA-426 10.5*	Yes ☐	No ☐	N/A ☐
Where are the main distribution facility, data centers, routers, firewalls, and servers located and are they secure?	*FEMA-426 10.6*	Yes ☐	No ☐	N/A ☐
Where are the secondary and/or intermediate distribution facilities and are they secure?		Yes ☐	No ☐	N/A ☐
Is there a mass notification system that reaches all building occupants? (public address, pager, cell phone, computer override, etc.)	*FEMA-426 10.15*	Yes ☐	No ☐	N/A ☐
Will one or more of these systems be operational under hazard conditions? (UPS, emergency power)		Yes ☐	No ☐	N/A ☐
Do control centers and their designated alternate locations have equivalent or reduced capability for voice, data, mass notification, etc.? (emergency operations, security, fire alarms, building automation)	*FEMA-426 10.16*	Yes ☐	No ☐	N/A ☐

Do the alternate locations also have access to backup systems, including emergency power?	*FEMA-426 10.16*	Yes ☐	No ☐	N/A ☐

EQUIPMENT OPERATIONS AND MAINTENANCE				
Are there composite drawings indicating location and capacities of major systems and are they current? (electrical, mechanical, and fire protection; and date of last update)	*FEMA-426 11.1*	Yes ☐	No ☐	N/A ☐
Are backup power systems periodically tested under load?	*FEMA-426 11.7*	Yes ☐	No ☐	N/A ☐
Is stairway and exit sign lighting operational?	*FEMA-426 11.8*	Yes ☐	No ☐	N/A ☐

SECURITY SYSTEMS				
PERIMETER SYSTEMS				
Are black/white or color CCTV (closed circuit television) cameras used?	*FEMA-426 12.1*	Yes ☐	No ☐	N/A ☐
Are they *[CCTV]* monitored and recorded 24 hours/7 days a week?		Yes ☐	No ☐	N/A ☐
Are the cameras programmed to respond automatically to perimeter building alarm events?	*FEMA-426 12.2*	Yes ☐	No ☐	N/A ☐
Do they have built-in video motion capabilities?		Yes ☐	No ☐	N/A ☐
Are panic/duress alarm buttons or sensors used?	*FEMA-426 12.4*	Yes ☐	No ☐	N/A ☐
Are intercom call boxes used in parking areas or along the building perimeter?	*FEMA-426 12.5*	Yes ☐	No ☐	N/A ☐
Who monitors the CCTV system? *[Is CCTV system consistently monitored?]*	*FEMA-426 12.7*	Yes ☐	No ☐	N/A ☐
What is the quality of the video images both during day and hours of darkness? *[Does video quality adequately support protection of critical assets?]*	*FEMA-426 12.8*	Yes ☐	No ☐	N/A ☐
Are infrared camera illuminators used?		Yes ☐	No ☐	N/A ☐
INTERIOR SECURITY				
Are black/white or color CCTV cameras used?	*FEMA-426 12.12*	Yes ☐	No ☐	N/A ☐
Are they monitored and recorded 24 hours/7days a week?		Yes ☐	No ☐	N/A ☐
Are the *[CCTV]* cameras programmed to respond to automatically to interior building alarm events?	*FEMA-426 12.13*	Yes ☐	No ☐	N/A ☐
Do they *[CCTV cameras]* have built-in video motion capabilities?		Yes ☐	No ☐	N/A ☐
Are interior camera video images of good visual and recording quality?	*FEMA-426 12.17*	Yes ☐	No ☐	N/A ☐
Are interior cameras supported by uninterruptable power supply source, battery, or building emergency power?	*FEMA-426 12.18*	Yes ☐	No ☐	N/A ☐
What type of security access control system is used? Are the devices used for physical security also used (integrated) with security computer networks (e.g., in place of or in combination with user ID and system passwords)?	*FEMA-426 12.20*	Yes ☐	No ☐	N/A ☐

For each of the following groups, are controls in place that limit entry?	*Employees? (Page-21)*	*RST Notebook*	Yes □	No □	N/A □
	Visitors? (Page-21)	*RST Notebook*	Yes □	No □	N/A □
	Contractors/Vendors? (Page-21)		Yes □	No □	N/A □
	Customer/Patron/Public? (Page-21)		Yes □	No □	N/A □
What is the backup power supply source for the access control systems? (battery, uninterruptible power supply) *[Does the backup power provide sufficient support?]*		*FEMA-426 12.22*	Yes □	No □	N/A □
Are panic/duress alarm sensors used?		*FEMA-426 12.24*	Yes □	No □	N/A □
Are intercom call-boxes or a building intercom system used throughout the building?		*FEMA-426 12.25*	Yes □	No □	N/A □
Are magnetometers (metal detectors) and x-ray equipment used?		*FEMA-426 12.26*	Yes □	No □	N/A □
Does the facility utilize an interior intrusion detection method or application? (Page-27)		*RST Notebook*	Yes □	No □	N/A □
What type of interior IDS sensors are used: electromagnetic; fiber optic; active infrared-motion detector; photoelectric; glass break (vibration/shock); single, double, and roll-up door magnetic contacts or switches? *[Does the IDS provide sufficient coverage?]*		*FEMA-426 12.27*	Yes □	No □	N/A □
Are mechanical electrical gas, power supply, radiological material storage, voice/data telecommunication system nodes, security system panels, elevator and critical system panels, and other sensitive rooms continuously locked, under electronic security, CCTV camera, and intrusion alarm systems surveillance?		*FEMA-426 12.28*	Yes □	No □	N/A □
What types of locking hardware are used throughout the building? Are manual and electromagnetic cipher, keypad, pushbutton, panic bar, door strikes, and related hardware and software used?		*FEMA-426 12.29*	Yes □	No □	N/A □
Are any potentially hazardous chemicals, combustible, or toxic materials stored on site in non-secure and non-monitored areas?		*FEMA-426 12.30*	Yes □	No □	N/A □
What security controls are in place to handle the processing of mail and protect against potential biological, explosive, or other threatening exposures? *[Are the mail security controls sufficient?]*		*FEMA-426 12.31*	Yes □	No □	N/A □
Is there a designated security control room and console in place to monitor security, fire alarm, and other building systems?		*FEMA-426 12.32*	Yes □	No □	N/A □
Is there a backup control center designated and equipped?			Yes □	No □	N/A □
Is there off-site 24-hour monitoring of intrusion detection systems?			Yes □	No □	N/A □
Is the location of the security room in a secure area with limited, controlled, and restricted access controls in place?		*FEMA-426 12.34*	Yes □	No □	N/A □

What are the means by which facility and security personnel can communicate with one another (e.g., portable radio, pager, cell phone, personal data assistants (PDAs))? *[Does the means provide sufficient capability?]*		*FEMA-426 12.35*	Yes ☐	No ☐	N/A ☐
Is there a computerized security incident reporting system used to prepare reports and track security incident trends and patterns?		*FEMA-426 12.36*	Yes ☐	No ☐	N/A ☐
Security Force Profile	Does the facility have a security force? (Page-11)	*RST Notebook*	Yes ☐	No ☐	N/A ☐
	Is the security force armed? (Page-11)		Yes ☐	No ☐	N/A ☐
	Is the security force on site? (Page-11)		Yes ☐	No ☐	N/A ☐
	Are there static posts? (Page-13)		Yes ☐	No ☐	N/A ☐
	Are there roving patrols? (Page-13)		Yes ☐	No ☐	N/A ☐
Is there a *[Security Force]* Surge Capacity Plan? (Page-81)		*IST Version-5*	Yes ☐	No ☐	N/A ☐
Are vaults or safes in the building? Where are they located? *[Does the location and access procedures provide sufficient protection?]*		*FEMA-426 12.38*	Yes ☐	No ☐	N/A ☐
SYSTEM SECURITY DOCUMENTS					
Do all security system documents include current as-built drawings?		*FEMA-426 12.44*	Yes ☐	No ☐	N/A ☐
Are security systems decentralized, centralized, or integrated? Do they operate over an existing IT network or are they a standalone method of operation? *[Does the system configuration present vulnerabilities?]*		*FEMA-426 12.46*	Yes ☐	No ☐	N/A ☐
What maintenance or service agreements exist for security systems? *[Is the system maintained to specifications?]*		*FEMA-426 12.48*	Yes ☐	No ☐	N/A ☐

SECURITY MASTER PLAN				
Does a written security plan exist for this site or building?	*FEMA-426 13.1*	Yes ☐	No ☐	N/A ☐
Are personnel trained on the plan? (Page-5)	*RST Notebook*	Yes ☐	No ☐	N/A ☐
Is the plan exercised at least once a year? (Page-5)	*RST Notebook*	Yes ☐	No ☐	N/A ☐
Has the security plan been communicated and disseminated to key management personnel/departments?	*FEMA-426 13.2*	Yes ☐	No ☐	N/A ☐
Has the security plan been benchmarked or compared against related organizations and operational entities?	*FEMA-426 13.3*	Yes ☐	No ☐	N/A ☐
Are threats/hazards, vulnerabilities, and risks adequately defined and security countermeasures addressed and prioritized relevant to their criticality and probability of occurrence?	*FEMA-426 13.6*	Yes ☐	No ☐	N/A ☐
Does the security plan address the protection of people, property, assets, and information?	*FEMA-426 13.11*	Yes ☐	No ☐	N/A ☐

Does the facility have procedures for suspicious packages? (Page-7)		*RST Notebook*	Yes ☐	No ☐	N/A ☐
The security plan has procedures for… (Page-50)	Assessment of possible security risks	*IST Version-5*	Yes ☐	No ☐	N/A ☐
	Review of threats to and vulnerability of facility operations/activities		Yes ☐	No ☐	N/A ☐
	Identification of critical assets or areas		Yes ☐	No ☐	N/A ☐
	Exercising the plan	*IST Version-5*	Yes ☐	No ☐	N/A ☐
	Executive Protection		Yes ☐	No ☐	N/A ☐
Has the *[security]* plan been coordinated with local law enforcement? (Page-51)		*IST Version-5*	Yes ☐	No ☐	N/A ☐
The security plan has procedures for Security awareness training program (Active Shooter)? (Page-53)		*IST Version-5*	Yes ☐	No ☐	N/A ☐
Are you [facility] aware of the DHS "See Something Say Something" campaign? (Page-5)		*IST Version-5*	Yes ☐	No ☐	N/A ☐
Have there been onsite visit(s) with this first responder?	Primary Law Enforcement Agency (Page-16)	*IST Version-5*	Yes ☐	No ☐	N/A ☐
	Primary Fire Response Agency (Page-16)	*IST Version-5*	Yes ☐	No ☐	N/A ☐
	Primary Emergency Medical Response Agency (Page-16)	*IST Version-5*	Yes ☐	No ☐	N/A ☐
Is there Interoperable Communication with this first responder [not 911]? (Page-16)		*IST Version-5*	Yes ☐	No ☐	N/A ☐
Does the security plan address the following major components: access control surveillance, response, building hardening, and protection against CBR *[Chemical/Biological/Radiological]* and cyber-network attacks?		*FEMA-426 13.12*	Yes ☐	No ☐	N/A ☐
Has the level of risk been identified and communicated in the security plan through the performance of a physical security assessment?		*FEMA-426 13.13*	Yes ☐	No ☐	N/A ☐
Does the facility security plan utilize different threat levels? (Page-47)		*IST Version-5*	Yes ☐	No ☐	N/A ☐
Are different protective measures employed/ implemented during elevated threat situations? (Page-47)		*IST Version-5*	Yes ☐	No ☐	N/A ☐
Physical Security Profile	Does the facility have a written agreement with entities other than emergency responders? (Page-29)	*RST Notebook*	Yes ☐	No ☐	N/A ☐
	Does the facility participate in security exercises or tabletops with outside agencies? (Page-29)		Yes ☐	No ☐	N/A ☐
Resilience Management Profile	Does the facility have a written Emergency Operation/Emergency Action Plan? (Page-35)	*RST Notebook*	Yes ☐	No ☐	N/A ☐

	Does the plan include both physical and cyber assets? (Page-35)	*RST Notebook*	Yes □	No □	N/A □
	Are personnel trained on the plan? (Page-36) Is the plan exercised at least once a year? (Page-36)		Yes □	No □	N/A □
	Is the plan exercised at least once a year? (Page-36)		Yes □	No □	N/A □
Does the emergency action plan have procedures for:	HAZMAT spills/releases (Page-72)	*IST Version-5*	Yes □	No □	N/A □
	Active shooter (Page-73)		Yes □	No □	N/A □
	Hostage situations (Page-73)		Yes □	No □	N/A □
	Shelter-in-place (Page-73)		Yes □	No □	N/A □
	Bomb threat (Page-73)		Yes □	No □	N/A □
	Civil unrest/Riot (Page-73)		Yes □	No □	N/A □
	Explosion (Page-73)		Yes □	No □	N/A □
Does the facility have an incident management and command center? (Page-75)		*IST Version-5*	Yes □	No □	N/A □
Resilience Management Profile	Does the facility receive threat information, security-related bulletins, advisories, and/or alerts from an external source? (Page-37)	*RST Notebook*	Yes □	No □	N/A □
	Does the facility share threat and/or security-related information with outside organizations? (Page-37)		Yes □	No □	N/A □

Sources

Federal Emergency Management Agency (FEMA)
FEMA 426, *Reference Manual to Mitigate Terrorist Attacks Against Buildings*, 2003

Department of Homeland Security, Office of Infrastructure Protection (DHS IP)
Rapid Survey Tool (RST) Notebook, 2018

Department of Homeland Security, Office of Infrastructure Protection (DHS IP)
Infrastructure Survey Tool (IST) Version-5, 2016

Additional Reference Material

U.S. Department of Commerce, National Institute of Standards and Technology
Framework for Improving Critical Infrastructure Cybersecurity (Version 1.0), 2014
Pages 21, 23, 25, 26, 27, 31, 32, 33 and 34.
https://www.nist.gov/cyberframework

U.S. Department of Commerce, National Institute of Standards and Technology
NIST Special Publication 800-53 (Revision 4), Security and Privacy Controls for Federal Information Systems and Organizations, 2013
*Physical and Environmental (PE) Controls (*Pages F-127 to F-138*): PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9, PE-10, PE-11, PE-12, PE-16, PE-18 and PE-20.*
http://dx.doi.org/10.6028/NIST.SP.800-53r4

Election Center (National Association of Election Officials)
Elections Security Checklist©, 2016
https://www.electioncenter.org/election-security-infrastructure-elections-security-checklist.html

This document was developed by the Office of Infrastructure Protection (Federal Region-4), DHS, to provide information to DHS Protective Security Advisors (PSAs) assigned with the responsibility of conducting security walkthrough surveys per request of State, Local, Tribal or Territorial (SLTT) election officials. The information herein is not all inclusive. This guide presents an overview of election infrastructure security practices. SLTT election officials and legal counsel should work together to ensure that these practices are employed in a manner consistent with legal requirements.

Election Infrastructure Security Initiative

February 23, 2018

Elections: Critical to American Democracy

"Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law."

– DHS Election Infrastructure Designation Statement, Jan. 6, 2017

- Critical infrastructure is defined as:

  "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

What Is Critical Infrastructure?

- There are 16 critical infrastructure sectors:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare & Public Health
- Information Technology
- Nuclear Reactors Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems

DHS's Role In Critical Infrastructure

- The Homeland Security Act of 2002 created DHS and gave it responsibility for coordinating national critical infrastructure protection, including:
  - Work with state, local, tribal, and territorial governments, the private sector, and international partners;
  - Conduct risk assessments and identify priorities for protective measures;
  - Develop and maintain the National Infrastructure Protection Plan (NIPP).

National Infrastructure Protection Plan

- The National Infrastructure Protection Plan (NIPP) 2013 established a framework for national, coordinated efforts to protect critical infrastructure by managing risk in each of 16 sectors.
- NIPP's voluntary partnership model is the ***primary*** means of coordinating public and private sector infrastructure protection efforts through collaboration:

Sector-Specific Agency (SSA)	Coordinates security and resilience efforts in each sector.
Government Coordinating Council (GCC)	Forum for stakeholders from different levels of government.
Sector Coordinating Council (SCC)	Forum for private sector entities to work jointly among themselves and with the GCC and SSA.

Critical Infrastructure Designation Benefits

- Enables DHS to **prioritize assistance** to and resources for State and local government ***when*** and ***only if*** the officials request such assistance. (DHS only provides assistance if it is requested.)
- Enables secret level clearances to be given to state and local stakeholders.
- Allows frank discussions between DHS and stakeholders on vulnerabilities.
- Signals to domestic and international adversaries U.S. election infrastructure receives all the protections and benefits of critical infrastructure.
- Provides protection to specific information given to DHS under the Protected Critical Infrastructure Information Program from public and other disclosure.
- Establishes an Information Sharing Analysis Center (ISAC) to provide tailored cybersecurity analysis to officials.

What The Designation Does Not Do

- **Does not impose** any federal regulation or requirement on state and local operation or management of election infrastructure.
- **Does not give** DHS or any federal agency authority over state and local election infrastructure.
- **Does not require** state and local election officials to use DHS programs and services.

Election Infrastructure

Election infrastructure refers to assets, systems, and networks most critical to the security and resilience of the election process, such as:

- Storage facilities

- Polling places

- Voter registration databases, and the information technology infrastructure and systems used to maintain such databases.

- Information technology infrastructure and systems used to count, audit, and display election results.

DHS's Critical Infrastructure Partner Role

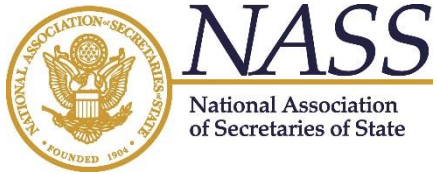
- DHS is the sector-specific agency (SSA) responsible to and for the Election Infrastructure Subsector (EIS).
- As its SSA, DHS remains a partner to, not an overseer of, state and local election officials, and supports the work of state and local election officials.
- DHS funds the Multi-State Information Sharing and Analysis Center to provide information services to state and local election officials.
- To further develop and support the state and local partnership, DHS created the Election Task Force (ETF) as part of a **whole-of-nation** approach to unify federal efforts to ensure security and resilience of election infrastructure.

DHS Employs A "Whole of Nation" Approach

- Securing election infrastructure is a national priority and no one entity can be successful working alone - it takes a "whole of nation" approach.
- Just as most critical infrastructure is not federally owned or managed, election infrastructure is outside federal control.
- DHS values and builds partnerships based on a foundation of trust, information sharing.

DHS Works With A Variety Of State and Local Partners

DHS works with partners in all levels of government:

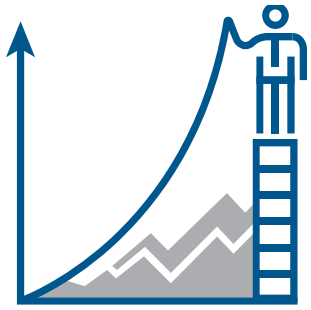


ETF: Federal Support for Election Infrastructure

Formed in October 2017, the Election Task Force coordinates and synchronizes all federal activity on behalf of election infrastructure.

ETF's work is guided by three primary goals:

- **Understand threat and characterize risk** to election infrastructure to inform planning, resourcing, and prioritization of EI efforts.
- **Provide services** to EI stakeholders to help reduce both cyber and physical risk to state infrastructures, ensure access to actionable threat information, and maintain situational awareness of trends across the sector.
- **Mature** the organization of the EI Subsector to ensure a representative and effective security-informed partnership.



Election Task Force Members

NIST
National Institute
of Standards
and Technology

FVAP.GOV
FEDERAL VOTING ASSISTANCE PROGRAM

EIS Government Coordinating Council

- Formed in October 2017, the EIS Government Coordinating Council (GCC) is a 27-member body of 24 state and local government representatives and 3 federal government representatives
- The EIS GCC:
  - Provides a forum for government to work jointly on an array of efforts to support election infrastructure through collective and individual expertise and resources.
  - Will receive classified threat information as well as threat and vulnerability information.
  - Will also help determine who else in the election community should receive that information so they are both recipients and involved in the sharing of information.

EIS Sector Coordinating Council

- Formation of the EIS Sector Coordinating Council (SCC) is underway.
- The EIS SCC will be a self-governing group, enabling private-sector critical infrastructure owners and operators and industry representatives to work jointly on sector-specific strategies, policies, and activities.
- The EIS SCC will coordinate and collaborate with the EIS GCC and DHS as its SSA to address critical infrastructure security and resilience policies and efforts for election infrastructure.

DHS Election Infrastructure Services

- DHS offers a broad range of services and programs to help secure election infrastructure.
- Services and programs are free, and all are voluntary and provided upon request.
- Contact Cybersecurity Advisors (CSA) to discuss how to select, prioritize, and sequence available services and educational programs based on specific needs.

Cybersecurity Service Centers

Homeland Security

MS-ISAC
Multi-State Information Sharing & Analysis Center

24/7 cybersecurity operations centers that maintain close coordination among the private sector, government officials, the intelligence community, and law enforcement to provide situational awareness and incident response, as appropriate.

Contact Information

For more information on DHS cyber programs, visit www.dhs.gov/cyber

For access to the full range of DHS cyber resources, email SLTTCyber@hq.dhs.gov

To become an MS-ISAC member, visit www.cisecurity.org/ms-isac/

Summary of DHS Services:
Cybersecurity Assessments

Needs	DHS Services	Summary
Identify and Limit Vulnerabilities	Cyber Hygiene Scanning	Broadly assess Internet-accessible systems for known vulnerabilities and configuration errors on a persistent basis. As potential issues are identified DHS works with impacted stakeholders to mitigate threats and risks to their systems prior to their exploitation.
	Risk and Vulnerability Assessment (RVA)	• Penetration testing • Social engineering • Wireless access discovery • Database scanning • Operating system scanning
	Phishing Campaign Assessment	• Measures susceptibility to email attack • Delivers simulated phishing emails • Quantifies click-rate metrics over a 10-week period

18

Summary of DHS Services:
Cybersecurity Assessments, Cont'd

Needs	DHS Services	Summary
Cyber Risk and IT Security Program Assessment	Cyber Resilience Review (CRR)	One-day, onsite engagement conducted on an enterprise-wide basis to give insight on areas of strength and weakness, guidance on increasing organizational cybersecurity posture, preparedness, and ongoing investment strategies.
	External Dependencies Management Assessment	To access the activities and practices used by an organization to manage risk arising from external dependencies that constitute the information and communication technology service supply chain.
	Cyber Infrastructure Survey (CIS)	Assesses an organization's implementation and compliance with more than 80 cybersecurity controls.

19

Summary of DHS Services:
Physical Assessments

Needs	DHS Services	Summary
Identify and Limit Vulnerabilities	Assist Visit (AV)	On-site engagement to inform and educate owners and operators on threats from terrorism, the criticality of their facilities, and available Office of Infrastructure Protection (IP) and Department of Homeland Security (DHS) resources.
	Infrastructure Survey Tool (IST)	Facilitated survey to Identify and document critical infrastructure overall security and resilience, and provide information for protective measures planning and resource allocation.
	Hometown Security	A source for providing tools and resources to protect public gathering venues.

To learn more about our products and services, please visit https://www.dhs.gov/ecip and https://www.dhs.gov/hometown-security.

Summary of DHS Services:
Detect and Prevent

Needs	DHS Services	Summary
Detect Network Threats	Cyber Threat Hunting	Utilizes advanced hunting capabilities to identify adversary presence in a network that evades traditional security controls. For more information, call (888) 282-0870
Enhance Network Protection	Enhanced Cyber Services (ECS)	Intrusion prevention service to augment, not replace, existing cybersecurity capabilities. Leverages sensitive and classified cyber threat indicators to block malicious traffic from entering customer networks. Service offerings, available through accredited commercial service providers, include: • Domain Name Service (DNS) Sinkholing • Email (SMTP) Filtering • Netflow Analysis For more information, visit www.dhs.gov/enhanced-cybersecurity-services

21

Summary of DHS Services:
Information Sharing & Awareness

Needs	DHS Services	Summary
Cyber Alerts and Advisories	National Cyber Awareness System (NCAS)	Timely information about security topics and threats via subscription to a mailing list. NCCIC provides current activity, alerts, bulletins, and security tips to stakeholders. For more information, visit www.us-cert/gov/ncas
Collaboration	Homeland Security Information Network (HSIN)	The NCCIC portal provides stakeholders a platform to securely collaborate and share cybersecurity information, threat analysis and products within trusted communities of interest. For more information, contact HSIN.Outreach@hq.dhs.gov Connect to HSIN at https://auth.dhs.gov/oam/hsinlogin/HSINLogin

22

Summary of DHS Services:

Information Sharing & Awareness, Cont'd

Needs	DHS Services	Summary
Exchange of Cyber Threat Indicators	Automated Indicator Sharing (AIS)	Enables real-time bidirectional exchange of cyber threat indicators at machine speed, with the goal of reducing the number of cyber attacks. For more information, visit www.us-cert.gov/ais Share Indicators at www.us-cert.gov/forms/share-indicators
Applying Security Expertise and Best Practices	Cybersecurity Advisors (CSAs) & Protective Security Advisors (PSAs)	Regionally located personnel who engage state and local governments, election crime coordinators, and vendors to offer immediate and sustained assistance, coordination, and outreach to prepare and protect from cyber and physical threats. For more information, visit www.dhs.gov/protective-security-advisors

Summary of DHS Services:

Information Sharing & Awareness, Cont'd

Needs	DHS Services	Summary
Exchange of Cyber Threat Indicators	Automated Indicator Sharing (AIS)	Enables real-time bidirectional exchange of cyber threat indicators at machine speed, with the goal of reducing the number of cyber attacks. For more information, visit www.us-cert.gov/ais Share Indicators at www.us-cert.gov/forms/share-indicators
Applying Security Expertise and Best Practices	Cybersecurity Advisors (CSAs) & Protective Security Advisors (PSAs)	Regionally located personnel who engage state and local governments, election crime coordinators, and vendors to offer immediate and sustained assistance, coordination, and outreach to prepare and protect from cyber and physical threats. For more information, visit www.dhs.gov/protective-security-advisors

24

Summary of DHS Services:
Training & Education

Needs	DHS Services	Summary
Educational Material	Stop.Think Connect. Toolkit	Resources and materials to help promote cybersecurity awareness. Provides a better understanding of cyber threats and empowers people to be safer and more secure online. **For more information, visit** www.dhs.gov/stopthinkconnect
Career Development	Federal Virtual Training Environment (FedVTE)	Online and on-demand cybersecurity training system for Federal/SLTT government personnel and veterans. Courses range from beginner to advanced levels. Training is accessible from any Internet enabled computer. **For more information, visit** https://fedvte.usalearning.gov
	National Initiative for Cybersecurity Careers and Studies Catalog (NICCS)	Catalog of more than 3,000 cybersecurity-related courses both online and in-person from more than 125 different providers across the nation. Courses are aligned to the specialty areas of the National Cybersecurity Workforce Framework. **For more information, visit** www.niccs.us-cert.gov/training

25

Summary of DHS Services:
Training & Education, Cont'd

Needs	DHS Services	Summary
Exercises & Planning	National Cyber Exercises and Planning Program (NCEPP)	Provide cyber exercise planning workshops and seminars, and conduct tabletop, full-scale and functional exercises for organizations to rehearse their response to staged incidents, allowing organizations to develop "muscle memory" and identify areas that may need to be improved in order to prepare for a real-world situation. For more information, contact CEP@hq.dhs.gov
	IP Stakeholder Readiness & Exercise Program	Conduct discussion- and operation-based exercises focused on enhancing critical infrastructure security and resilience. Provide resources for the critical infrastructure community to conduct independent tabletop exercises through the Sector-Specific Tabletop Exercise Program (SSTEP). For more information, contact SOPD.Exercise@hq.dhs.gov

Summary of DHS Services:
Physical Security Initiatives

Needs	DHS Services	Summary
Physical Security	IP Active Shooter Preparedness Program	Provide a comprehensive set of resources to position public and private sector organizations to reduce the impacts of an active shooter event. Includes in-person training, online training, and educational resources. For more information, contact ASWorkshop@hq.dhs.gov or visit www.dhs.gov/active-shooter-preparedness
	IP Unmanned Aircraft System (UAS) Initiative	Address threats posed to critical infrastructures from emergent adversary use of UAS. Offers policies and risk mitigation solutions for safe, secure, and beneficial use of UAS, associated countermeasures, and cyber/physical emerging technology analysis. For more information, contact IP-UAS@hq.dhs.gov

Summary of DHS Services:
Physical Security Initiatives, Cont'd

Needs	DHS Services	Summary
Physical Security	IP Soft Target Security Initiative	Provides national leadership on technology, standards, and best practices to demonstrably reduce the risk of successful attacks on soft targets. Serves as a center of gravity for DHS-wide resources available to support the critical infrastructure community in securing soft targets. For more information, contact IP-SoftTargetSecurity@hq.dhs.gov

Summary of DHS Services:
Incident Response

Needs	DHS Services	Summary
Analysis of Malicious Code	Advanced Malware Analysis Center	Provides 24/7 dynamic analyses of malicious code. Stakeholders submit samples via an online website and receive a technical document outlining the results of the analysis. Experts will detail recommendations for malware removal and recovery activities. This service can be performed in concert with Incident Response services, should the incident warrant the need. **To submit malware for analysis, visit** www.malware.us-cert.gov
Mitigation and Recovery	Incident Response	Provides 24/7 intrusion analysis in response to a cyber incident. Dispatches skilled personnel when a cyber incident occurs to assist in identifying malicious actors, technical analysis, containment, mitigation guidance, and post-incident recovery. **Report an incident, at** www.us-cert.gov/forms/report **For more information, visit** www.us-cert.gov

29

MS-ISAC
Multi-State Information Sharing & Analysis Center

- Provides cybersecurity support to SLTT governments.
- Furthers DHS efforts to secure cyberspace by distributing early warnings of cyber threats to SLTT governments.
- Shares security incident information and analysis.
- Runs a 24/7 watch and warning security operations center.
- Funded by DHS.

For more information, see https://www.cisecurity.org/ms-isac.

30

For more information:

- First Last– DHS Protective Security Advisor (PSA) State
  - First.Las@hq.dhs.gov
- Shawn Stallworth – Chief, Protective Security
  - Shawn.Stallworth@hq.dhs.gov
- Donald Robinson – DHS Infrastructure Protection Regional Director – Region 4
  - Donald.Robinson@hq.dhs.gov

Outlook

RE: [External] Region 4 Point of Contact

From Hanna, Raymond A <Raymond.A.Hanna@HQ.DHS.GOV>

Date Tue 9/6/2022 6:08 PM

To Bell, Karen B <Karen.Bell@ncsbe.gov>; Johnson, Erick <ERICK.JOHNSON@cisa.dhs.gov>; Godwin, Sasha <sasha.godwin@ncdps.gov>; Roberts, Jacob D <jacob.roberts@ncdps.gov>; Eichel, Lydia R <lydia.eichel@ncdps.gov>; Clifton, Richard <Richard.Clifton@ncdps.gov>; McGrath, Tom <Tom.McGrath@ncdps.gov>; Reinwald, Alexander E <alexander.reinwald@ncdps.gov>

Cc Crass, Torry <Torry.Crass@ncsbe.gov>; Velez, Trena <trena.velez@ncsbe.gov>; Love, Katelyn <Katelyn.Love@ncsbe.gov>; Tsujii, Tim <tsujiidt@forsyth.cc>; Davis, Dave <dave.davis@pittcountync.gov>

You are correct, it is 9/29, it was either my eyes, or I was having a senior moment, or both – sorry about that

Raymond A. Hanna
Protective Security Advisor – Raleigh District
U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
443.827.2059 | Raymond.A.Hanna@hq.dhs.gov

From: Bell, Karen B <Karen.Bell@ncsbe.gov>
Sent: Tuesday, September 6, 2022 5:52 PM
To: Hanna, Raymond A <Raymond.A.Hanna@HQ.DHS.GOV>; Johnson, Erick <ERICK.JOHNSON@cisa.dhs.gov>; Godwin, Sasha <sasha.godwin@ncdps.gov>; Roberts, Jacob D <jacob.roberts@ncdps.gov>; Eichel, Lydia R <lydia.eichel@ncdps.gov>; Clifton, Richard <Richard.Clifton@ncdps.gov>; McGrath, Tom <Tom.McGrath@ncdps.gov>; Reinwald, Alexander E <alexander.reinwald@ncdps.gov>
Cc: Crass, Torry <Torry.Crass@ncsbe.gov>; Velez, Trena <trena.velez@ncsbe.gov>; Love, Katelyn <Katelyn.Love@ncsbe.gov>; Tim Tsujii <tsujiidt@forsyth.cc>; Davis, Dave <dave.davis@pittcountync.gov>
Subject: RE: [External] Region 4 Point of Contact

Great!

It's September 29 not 19 from 1 to 2:30 PM. Thank you! -- Karen

Karen Brinson Bell, CERA, PMP
Executive Director, NCSBE

(919) 814-0700

NORTH CAROLINA
STATE BOARD OF ELECTIONS

From: Hanna, Raymond A <Raymond.A.Hanna@HQ.DHS.GOV>
Sent: Tuesday, September 6, 2022 4:31 PM
To: Bell, Karen B <Karen.Bell@ncsbe.gov>; Johnson, Erick <ERICK.JOHNSON@cisa.dhs.gov>; Godwin, Sasha <sasha.godwin@ncdps.gov>; Roberts, Jacob D <jacob.roberts@ncdps.gov>; Eichel, Lydia R <lydia.eichel@ncdps.gov>; Clifton, Richard <Richard.Clifton@ncdps.gov>; McGrath, Tom <Tom.McGrath@ncdps.gov>; Reinwald, Alexander E <alexander.reinwald@ncdps.gov>
Cc: Crass, Torry <Torry.Crass@ncsbe.gov>; Velez, Trena <trena.velez@ncsbe.gov>; Love, Katelyn <Katelyn.Love@ncsbe.gov>; Tim Tsujii <tsujiidt@forsyth.cc>; Davis, Dave <dave.davis@pittcountync.gov>
Subject: Re: [External] Region 4 Point of Contact

Hey Karen, yes - Sasha and I have talked, she will see if she can schedule the SCIF, if so, I will push you alls clearance to the NCARNG. You are talking about the Sept. 19th call from 1:00p - 2:30p, right?

Ray

From: Bell, Karen B <Karen.Bell@ncsbe.gov>
Sent: Tuesday, September 6, 2022 4:24 PM
To: Hanna, Raymond A <Raymond.A.Hanna@HQ.DHS.GOV>; Johnson, Erick <ERICK.JOHNSON@cisa.dhs.gov>; Godwin, Sasha <sasha.godwin@ncdps.gov>; Roberts, Jacob D <jacob.roberts@ncdps.gov>; Eichel, Lydia R <lydia.eichel@ncdps.gov>; Clifton, Richard <Richard.Clifton@ncdps.gov>; McGrath, Tom <Tom.McGrath@ncdps.gov>; Reinwald, Alexander E <alexander.reinwald@ncdps.gov>
Cc: Crass, Torry <Torry.Crass@ncsbe.gov>; Velez, Trena <trena.velez@ncsbe.gov>; Love, Katelyn <Katelyn.Love@ncsbe.gov>; Tim Tsujii <tsujiidt@forsyth.cc>; Davis, Dave <dave.davis@pittcountync.gov>
Subject: FW: [External] Region 4 Point of Contact

Good afternoon Ray and Erik from CISA, Sasha, Jake, Lydia, and Rich from DPS, Tom from Fusion, and Alex from NCNG, (cc: Torry, Trena, Katelyn, Tim, and Dave)

Making sure you all received this. Sasha and I had some correspondence that made me uncertain about whether you all were aware and had initiated plans for the SCIF.

Please let me know how I can be of help. David and Tim, we look forward to having you with us for your first briefing.

Thank you for all you do,
Karen

Karen Brinson Bell, CERA, PMP
Executive Director, NCSBE
(919) 814-0700

NORTH CAROLINA
STATE BOARD OF ELECTIONS

From: Election Infrastructure SSA <eisrma@cisa.dhs.gov>
Sent: Thursday, August 25, 2022 2:29 PM
To: Election Infrastructure SSA <eisrma@cisa.dhs.gov>
Cc: CISA Region 4 <CISARegion4@cisa.dhs.gov>
Subject: [External] Region 4 Point of Contact

Election Infrastructure Subsector clearance holders,

The Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with our Intelligence Community partners at the DHS Office of Intelligence and Analysis (I&A), Federal Bureau of Investigation (FBI), National Security Agency (NSA), National Intelligence Council (NIC), and the Office of the Director of National Intelligence (ODNI) is holding a SECERT-level classified briefing via secure video teleconference (SVTC) on **Thursday, September 29, 2022 from 1:00 – 2:30 pm ET**. Please note, there is no specific, credible threat to election infrastructure driving the briefing at this time.

All GCC and SCC members who have active clearances are invited to attend the briefing. Your CISA Regional team has been alerted to the briefing and is standing by to coordinate your access to a secure facility to receive the brief. If you have not been contacted by your CISA Regional team already, please reach out to them at CISARegion4@hq.dhs.gov as soon as possible to ensure ample time for coordination, including processing visitor access requests and passing clearances.

Thank you,

EI SRMA

Election Infrastructure Subsector Risk Management Agency

Election Security and Resilience

Cybersecurity and Infrastructure Security Agency

Email: EISRMA@CISA.DHS.GOV

Outlook

Re: Confirming Classified Briefing

From Hanna, Raymond A <Raymond.A.Hanna@HQ.DHS.GOV>
Date Wed 9/28/2022 6:04 PM
To Bell, Karen B <Karen.Bell@ncsbe.gov>; Reinwald, Alexander E <alexander.reinwald@ncdps.gov>; Godwin, Sasha <sasha.godwin@ncdps.gov>
Cc Velez, Trena <trena.velez@ncsbe.gov>; Crass, Torry <Torry.Crass@ncsbe.gov>; Love, Katelyn <Katelyn.Love@ncsbe.gov>; Davis, Dave <dave.davis@pittcountync.gov>; Tsujii, Tim <tsujiidt@forsyth.cc>; Johnson, Erick <ERICK.JOHNSON@cisa.dhs.gov>

Hi Karen,

I spoke to Sasha this week and the SVTC is still on as DHS did not cancel it and she said NCEM would still host it. Yes, enter the NCEM by going down the steps to NCEM as the SVTC will take place in their secure room.

CPT Reinwald, can you please confirm that Katelyn Love's permcert is still active - her clearance is held by DHS and not CISA, so Nick Klem has her on his list, but I believe he said her permcert is still good.

Sasha, if I got any of that wrong please correct.

I won't be there, Erick Johnson will be there to represent CISA R4.

Thanks,
Ray

From: Bell, Karen B <Karen.Bell@ncsbe.gov>
Sent: Wednesday, September 28, 2022 5:56:18 PM
To: Hanna, Raymond A <Raymond.A.Hanna@HQ.DHS.GOV>; Reinwald, Alexander E <alexander.reinwald@ncdps.gov>; Godwin, Sasha <sasha.godwin@ncdps.gov>
Cc: Velez, Trena <trena.velez@ncsbe.gov>; Crass, Torry <Torry.Crass@ncsbe.gov>; Love, Katelyn <Katelyn.Love@ncsbe.gov>; Davis, Dave <dave.davis@pittcountync.gov>; Tim Tsujii <tsujiidt@forsyth.cc>
Subject: Confirming Classified Briefing

Good evening Ray, Alex, and Sasha,

Just confirming that all is on go for the classified briefing tomorrow at the EOC given the emergency response for Hurricane Ian. Do we still report to the ground floor lobby and then get directed from there? I've copied the others with secret clearance from our team. Note Katelyn Love was not on the calendar invitation, which I have forwarded to her. Katelyn is on leave currently and has not separated from the agency. She's going to attend since we are still in process for obtaining clearance for our new general counsel.

Thank you,
Karen

Karen Brinson Bell, CERA, PMP
Executive Director, NCSBE
(919) 814-0700

NORTH CAROLINA
STATE BOARD OF ELECTIONS

Homeland Security

INCIDENT HANDLING OVERVIEW FOR ELECTION OFFICIALS

Incident Handling Overview for Election Officials

This document provides election officials with cyber incident handling steps to assist with incident readiness and the incident response services that the Department of Homeland Security National Protection and Programs Directorate can provide, by request, through its National Cybersecurity and Communications Integration Center.

NOTE: If you are experiencing or suspect malicious cyber behavior, contact the National Cybersecurity and Communications Integration Center (NCCIC) at 888-282-0870 or NCCICCustomerService@hq.dhs.gov

NCCIC INCIDENT RESPONSE TEAM SERVICES

Once you request assistance from the NCCIC Incident Response Team (IRT), we will work with you and provide the following capabilities and services, as needed.

- **Incident triage**: In order to best understand the severity of the incident, first we scope the incident and determine what resources are required.
- **Network topology review**: This is an assessment of network structure with recommendations, including potential access points (ingress and egress), remote access, segmentation, and interconnectivity.
- **Infrastructure configuration review**: Analysis of core devices on the network that are or can be used for network security. Log analysis is used to determine possible malicious activity.
- **Incident specific risk overview**: Provide tailored products and in-person briefings for technical, program manager, or senior leadership audiences on the specifics of the incident in question.
- **Hunt analysis**: We deploy tools which identify evidence of compromise, potential for persistent adversarial access, and detect indicators of compromise.
- **Security Program Review**: A review of the client's existing security roles, responsibilities, and policies.
- **Digital media analysis**: Technical forensic examination of digital artifacts to detect malicious activity and develop further indicators to prevent future attacks.
- **Malware analysis**: Reverse engineering of malware artifacts to determine functionality and build indicators to prevent future attacks.

To request these services, please contact NCCICCustomerService@hq.dhs.gov.

Homeland Security

Incident Handling Overview for Election Officials

INCIDENT RESPONSE PLANNING

No one can predict when or how severe an incident will be, however, there are a few best practices we suggest so that you are better positioned to handle a cybersecurity incident.

- Develop a comprehensive Incident Response Plan that includes:
  - Command Center, if needed, as single point of channeled communications
    - Dedicated resources, as needed, including supplies and equipment
  - Adaptability to different types of incidents, severity
  - Assigned roles and responsibilities of the response team, as well as backups so that each person knows exactly what is expected should an incident occur
  - Communication decision tree
  - Procedures to include:
- Log book which will detail the information that is needed to be collected per incident
- Notification schedule, including point(s) of contact with the most up-to-date contact information.
- Contact information should include: Up, Lateral, Down – per State, County, or Local
- Exercise incident response procedures
  - Conduct table top exercises
  - Simulate forensic scenarios, practice collecting forensic data
  - Make sure your team is trained and comfortable with all tools to ensure they are well versed to use in high pressure scenarios.
  - Have a sample press release written so that you can distribute to your stakeholders should an incident occur.

Homeland Security

Incident Handling Overview for Election Officials

CHECKLIST FOR REQUESTING ASSISTANCE FROM OUR CYBER INCIDENT RESPONSE TEAM

Do you suspect an incident has occurred? Review the checklist below, these are common questions we will ask upon your request.

- Are you reporting an active incident or has it already occurred? ☐ **Active** ☐ **Previous**
- Has Law Enforcement been contacted? ☐ **Yes** ☐ **No**
  - If yes, who? PoC, contact information
- Do you have a third party vendor working with you on this incident? ☐ **Yes** ☐ **No**
  - If yes, who? PoC, contact information
- Do you know the initial vector of attack? ☐ **Yes** ☐ **No**
  - If yes, where?
- Do you know where on your network potentially malicious activity was observed? ☐ **Yes** ☐ **No**
  - If yes, where?
- Do you believe infrastructure to cast or tally votes has been affected? ☐ **Yes** ☐ **No**
- Do you have any indicators of compromise from this incident? ☐ **Yes** ☐ **No**
  - If yes, are you able to provide the IRT with copies? (examples: domains, IP addresses, files, suspected malware)
- Do you have current and historical log data? ☐ **Yes** ☐ **No**
  - If yes, you should preserve the log data for further analysis. This includes any network and host based logs.
- Has any of the hosts that are potentially compromised been powered down? ☐ **Yes** ☐ **No**
  - If no, please leave the hosts online and powered on until we can discuss further with you.
- Do you have the ability to take a live forensic memory capture and disc image of compromised or potentially compromised host(s)? ☐ **Yes** ☐ **No**
- Do you have a recovery point objective (usually identified in an Incident Response Plan or Continuity of Operations Plan)? ☐ **Yes** ☐ **No**
  - If yes, do you know how long is it going to take you recover?
- What is the total number of endpoints on your network?

Homeland Security

Incident Handling Overview for Election Officials

INCIDENT RESPONSE OVERVIEW

After requesting assistance from our team, we will likely undertake a process that includes or recommends actions for the following practices:

- **Incident Identification**
  - Fully scope the incident before making any mitigation efforts
  - Capture live forensic data and collect logs
  - Analyze data to understand lateral movement and persistence mechanisms
  - Determine business impact
  - Determine whether the adversary is still present
- **Incident Containment**
  - Closely monitor compromised systems
  - Isolate compromised network systems
  - Limit scope and magnitude of intrusion
  - Gain visibility into the adversary's foothold
    - Setup alerts for known malicious network infrastructure
    - Setup alerts for known compromised accounts
    - Setup alerts for known host-level Tactics, Techniques and Procedures
  - Create containment and eradication strategy
- **Incident Eradication**
  - Remove compromised machines
  - Alert/Block known malicious infrastructure
  - Reset user account passwords
  - De-privilege user accounts
  - Reset service account passwords (difficult!)
  - Implement additional controls
  - Execute all steps concurrently
- **Incident Recovery**
  - Rebuild compromised hosts offline
  - Validate and restore data
  - Continue to monitor compromised systems and accounts

Once recovered from an incident, many organizations benefit from implementing the following practices:

- Conduct an after action assessment (lessons learned)
- Identify what worked during the incident response process and identify breakdowns or gaps
- Create a comprehensive post-incident report
- Revise policies, procedures, incident response plans, etc.
- Create new signatures to detect this type of malicious activity
- Identify areas to improve security posture
- Submit incident and recommendations report to leadership

Homeland Security

Incident Handling Overview for Election Officials

COMMON MISTAKES IN INCIDENT HANDLING

Over the years we have seen mistakes that could have easily been avoided – check out our list and the impact those mistakes can have while handling an incident.

- Mitigating the affected systems before responders can protect and recover data
  - Can cause the loss of volatile data such as memory and other host based artifacts.
  - Adversary will notice and change Tactics, Techniques and Procedures.
- Touching adversary infrastructure (Pinging, NSlookup, Browsing, etc.)
  - These actions can tip off the adversary that they have been detected.
- Preemptively blocking adversary infrastructure
  - Network infrastructure is fairly inexpensive. Adversary can easily change to new command and control infrastructure and you will lose visibility of their activity.
- Preemptive Password Resets
  - Adversary likely has multiple credentials, or worse, and has access to your entire active directory.
  - Adversary will use other credentials, create new credentials, or forge tickets.
- Failure to preserve or collect log data that could be critical to identifying access to the compromised systems
  - Learn what log types would be critical to an investigation in your organization.
    - Collect and retain these logs for as long as possible.

Homeland Security

Incident Handling Overview for Election Officials

NOTES:

Homeland Security

INCIDENT HANDLING OVERVIEW FOR ELECTION OFFICIALS

Homeland Security

Outlook

Re: OLU A BROWNE - Voter Reg Num:000010154020

From Tsujii, Tim <tsujiidt@forsyth.cc>
Date Wed 12/3/2025 12:04 PM
To Irby, Jaquon E <Jaquon.E.Irby@ice.dhs.gov>

3 attachments (725 KB)
ob_vr_profile.pdf; Ob_Name_Address Change_redacted.pdf; ob_Cancelation_redacted.pdf;

Please see the attached documents per your request. Let me know if you have any questions or if I can be of further assistance.

All the best,
Tim

Tim Tsujii
Director of Elections | Forsyth County Board of Elections
201 N. Chestnut Street | Winston-Salem, NC 27101
(336) 703-2801 desk | (336) 727-2893 fax
www.fcvotes.com
connect with us on @fcvotes

FORSYTH COUNTY BOARD OF ELECTIONS
Forsyth County Government

From: Irby, Jaquon E <Jaquon.E.Irby@ice.dhs.gov>
Sent: Tuesday, December 2, 2025 11:20 AM
To: Tsujii, Tim <tsujiidt@forsyth.cc>
Subject: RE: OLU A BROWNE - Voter Reg Num:000010154020

Thank you for the information.

Any information that you have to show this individuals history regarding voting in North Carolina would be greatly appreciated.

Jaquon E. Irby
Assistant Chief Counsel
Office of the Principal Legal Advisor, Atlanta (Charlotte)
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security

From: Tsujii, Tim <tsujiidt@forsyth.cc>
Sent: Tuesday, December 2, 2025 11:13 AM
To: Irby, Jaquon E <Jaquon.E.Irby@ice.dhs.gov>
Subject: Re: OLU A BROWNE - Voter Reg Num:000010154020

Good Afternoon,

I apologize for the delay in responding, our office has been closed due to the Thanksgiving holiday. Also, this particular's voter registration from 1995 was part of our legacy database system and we've been trying to find a copy of the requested document but have been unable to do so. No one on the current staff was employed with this office during that time and are uncertain of the access to the old system and the filing system in our office basement.

We do have access to more recent documents, such as an address change form. Please let me know if those would suffice.

Thank you,
Tim

From: Irby, Jaquon E <Jaquon.E.Irby@ice.dhs.gov>
Sent: Tuesday, December 2, 2025 8:13 AM
To: Tsujii, Tim <tsujiidt@forsyth.cc>
Subject: RE: OLU A BROWNE - Voter Reg Num:000010154020

Good Morning,

I sent the attached request for information regarding Olu Browne last Wednesday to the fcvotes@forsyth.cc address.

I write to check on the status of this request. Thank you in advance for your assistance in this matter and the assistance you provided in the past.

Best,

Jaquon E. Irby
Assistant Chief Counsel
Office of the Principal Legal Advisor, Atlanta (Charlotte)
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security

From: Irby, Jaquon E
Sent: Wednesday, November 26, 2025 9:25 AM
To: 'fcvotes@forsyth.cc' <fcvotes@forsyth.cc>
Subject: OLU A BROWNE - Voter Reg Num:000010154020

Good Morning,

Olu A Browne registered to vote on December 8, 1995, in Forsyth County. NC. Records indicated that he early voted for the November 4, 2008, general election, and voting in person during the primary election on May 5, 2008. He has since been removed from the North Carolina voter roll.

I write to request a copy of her voter registration application from 1995.

Thank you in advance for the assistance. Please let me know if you have any questions.

Best,

Jaquon E. Irby
Assistant Chief Counsel
Office of the Principal Legal Advisor, Atlanta (Charlotte)
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security

To register for eService, please go to https://eserviceregistration.ice.gov/

Outlook

Re: SHUQIN YIN - Voter Reg Num:000030280576

From Tsujii, Tim <tsujiidt@forsyth.cc>
Date Wed 11/19/2025 2:49 PM
To Irby, Jaquon E <Jaquon.E.Irby@ice.dhs.gov>
Cc FC Votes <fcvotes@forsyth.cc>

1 attachment (257 KB)
Yin, Shuqin_VRapp_11.19.25.pdf;

Good Afternoon,

Thank you for your email inquiry. Please see the attachment for the requested document. Let me know if you have any questions or if I can be of further help.

All the best,

Tim Tsujii
Director of Elections | Forsyth County Board of Elections
201 N. Chestnut Street | Winston-Salem, NC 27101
(336) 703-2801 desk | (336) 727-2893 fax
www.fcvotes.com
connect with us on @fcvotes

FORSYTH COUNTY BOARD OF ELECTIONS
Forsyth County Government We care

From: Irby, Jaquon E <Jaquon.E.Irby@ice.dhs.gov>
Sent: Wednesday, November 19, 2025 1:20 PM
To: FC Votes <fcvotes@forsyth.cc>
Subject: SHUQIN YIN - Voter Reg Num:000030280576

Good Afternoon,

Shuqin Yin registered to vote on November 4, 2016, in Forsyth County. NC. Records indicated that she early voted for the November 8, 2016, general election. She has since been removed from the North Carolina voter roll.

I write to request a copy of her voter registration application from 2016.

Thank you in advance for the assistance. Please let me know if you have any questions.

Best,

Jaquon E. Irby
Assistant Chief Counsel
Office of the Principal Legal Advisor, Atlanta (Charlotte)
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security

To register for eService, please go to https://eserviceregistration.ice.gov/

**** Warning *** Attorney/Client Privilege *** Attorney Work Product ****

FORSYTH COUNTY BOARD OF ELECTIONS

VOTER PROFILE

Full Name: BROWNE, OLU A

Residence Address: 2925 POINSETTA DR
WINSTON SALEM, NC 27107

Mailing Address on File:

VRN: 000010154020

Age: 55

Register Date: 12/08/1995

Status: R

Sex: MALE

Race: B **Ethnicity:** NL

Party: DEMOCRATIC

Birth Place: NY

Districts

Voting History (36 Most Recently Voted Elections)

11/04/2008	11/04/2008 GENERAL
05/06/2008	05/06/2008 PRIMARY

I CERTIFY THAT THIS INFORMATION IS TRUE AND ACCURATE. Signature: _____ **Date:** 12/02/2025

FORSYTH COUNTY BOARD OF ELECTIONS

Name/Address Change Form

VRN: 000010154020

New Name: OLU A BROWNE

:Date 10/28/2008

New Residence Address: 2925 POINSETTA DR
WINSTON SALEM NC 27107

New Mailing Address:

Sig [redacted]

CANCELLATION OF VOTER REGISTRATION
NORTH CAROLINA

NC STATE BOARD OF ELECTIONS
P. O. BOX 27255
RALEIGH, NC 27611-7255

PHONE: 1-866-522-4723
FAX: 919-715-0135
elections.sboe@ncsbe.gov

PURPOSE

This form is intended to provide notification of a voter's request to cancel his or her voter registration. Upon submission of this form, the appropriate county board of elections will remove the voter from the county's list of registered voters. Requested information will only be used to ensure that we are removing the correct voter.

INSTRUCTIONS

This form can **only** be completed by the voter. Voter should complete form as thoroughly as possible. Sign the form and then submit (*mail, fax, or scan & email*) it to the county board of elections office in the county in which the voter is registered. Contact information for the county boards of elections is available at www.ncsbe.gov.

10154020

Voter Information

Last Name (Required)	First Name (Required)	Middle Name	Suffix
Browne	Olu	Alexter	

Date of Birth (Required) (MM/DD/YYYY)	Age	Gender	Last 4 Digits of SSN	Driver License or ID No.	Voter Registration Number (if known)
[redacted]	46	☑ Male ☐ Female	[redacted]	[redacted]	

Voter Registration Address (Required)

2925 Poinsetta Drive

City (Required)	State	Zip Code	County (in which you were last registered)
Winston Salem	NC	27107	Forsyth

By signing this form, I give the county board of elections consent to cancel my voter registration record.

Signature	Date Signed
X [redacted]	8/4/17

FRAUDLENTLY OR FALSELY COMPLETING THIS FORM IS A CLASS I FELONY UNDER CHAPTER 163 OF THE NC GENERAL STATUTES.

Send Form To:

NC STATE BOARD OF ELECTIONS
P. O. BOX 27255
RALEIGH, NC 27611-7255
(or your local County Board of Elections)

Thank you for providing this information.

2017 AUG -4 PM 12:2
FORSYTH COUNTY BOARD OF ELECTIONS
RECEIVED

V2015.04

Outlook

RE: OLU A BROWNE - Voter Reg Num:000010154020

From Irby, Jaquon E <Jaquon.E.Irby@ice.dhs.gov>
Date Wed 12/3/2025 1:02 PM
To Tsujii, Tim <tsujiidt@forsyth.cc>

Good Afternoon,

Could you provide a certified copy of the ob_vr_profile?

Best,

Jaquon E. Irby
Assistant Chief Counsel
Office of the Principal Legal Advisor, Atlanta (Charlotte)
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security

From: Tsujii, Tim <tsujiidt@forsyth.cc>
Sent: Wednesday, December 3, 2025 12:05 PM
To: Irby, Jaquon E <Jaquon.E.Irby@ice.dhs.gov>
Subject: Re: OLU A BROWNE - Voter Reg Num:000010154020

Please see the attached documents per your request. Let me know if you have any questions or if I can be of further assistance.

All the best,
Tim

Tim Tsujii

Director of Elections | Forsyth County Board of Elections

201 N. Chestnut Street | Winston-Salem, NC 27101

(336) 703-2801 desk | (336) 727-2893 fax

www.fcvotes.com

connect with us on @fcvotes

FORSYTH COUNTY BOARD OF ELECTIONS

Forsyth County Government

From: Irby, Jaquon E <Jaquon.E.Irby@ice.dhs.gov>
Sent: Tuesday, December 2, 2025 11:20 AM
To: Tsujii, Tim <tsujiidt@forsyth.cc>
Subject: RE: OLU A BROWNE - Voter Reg Num:000010154020

Thank you for the information.

Any information that you have to show this individuals history regarding voting in North Carolina would be greatly appreciated.

Jaquon E. Irby
Assistant Chief Counsel
Office of the Principal Legal Advisor, Atlanta (Charlotte)
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security

From: Tsujii, Tim <tsujiidt@forsyth.cc>
Sent: Tuesday, December 2, 2025 11:13 AM
To: Irby, Jaquon E <Jaquon.E.Irby@ice.dhs.gov>
Subject: Re: OLU A BROWNE - Voter Reg Num:000010154020

Good Afternoon,

I apologize for the delay in responding, our office has been closed due to the Thanksgiving holiday. Also, this particular's voter registration from 1995 was part of our legacy database system and we've been trying to find a copy of the requested document but have been unable to do so. No one on the current staff was employed with this office during that time and are uncertain of the access to the old system and the filing system in our office basement.

We do have access to more recent documents, such as an address change form. Please let me know if those would suffice.

Thank you,
Tim

From: Irby, Jaquon E <Jaquon.E.Irby@ice.dhs.gov>
Sent: Tuesday, December 2, 2025 8:13 AM

To: Tsujii, Tim <tsujiidt@forsyth.cc>
Subject: RE: OLU A BROWNE - Voter Reg Num:000010154020

Good Morning,

I sent the attached request for information regarding Olu Browne last Wednesday to the fcvotes@forsyth.cc address.

I write to check on the status of this request. Thank you in advance for your assistance in this matter and the assistance you provided in the past.

Best,

Jaquon E. Irby
Assistant Chief Counsel
Office of the Principal Legal Advisor, Atlanta (Charlotte)
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security

From: Irby, Jaquon E
Sent: Wednesday, November 26, 2025 9:25 AM
To: 'fcvotes@forsyth.cc' <fcvotes@forsyth.cc>
Subject: OLU A BROWNE - Voter Reg Num:000010154020

Good Morning,

Olu A Browne registered to vote on December 8, 1995, in Forsyth County. NC. Records indicated that he early voted for the November 4, 2008, general election, and voting in person during the primary election on May 5, 2008. He has since been removed from the North Carolina voter roll.

I write to request a copy of her voter registration application from 1995.

Thank you in advance for the assistance. Please let me know if you have any questions.

Best,

Jaquon E. Irby
Assistant Chief Counsel
Office of the Principal Legal Advisor, Atlanta (Charlotte)
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security

To register for eService, please go to https://eserviceregistration.ice.gov/

Outlook

Re: Forsyth County BOE

From James Kaylor <jmkaylor@fbi.gov>
Date Wed 7/31/2024 5:39 PM
To Tsujii, Tim <tsujiidt@forsyth.cc>; Phillip Spainhour <pwspainhour@fbi.gov>

Hey Tim, feel free to give me a call.

704-942-8968.

Thank you,
James

From: Tsujii, Tim <tsujiidt@forsyth.cc>
Sent: Wednesday, July 31, 2024 5:37:30 PM
To: Spainhour, Phillip W. (CE) (FBI) <pwspainhour@fbi.gov>
Cc: Kaylor, James Martin (CE) (FBI) <jmkaylor@fbi.gov>
Subject: [EXTERNAL EMAIL] - Re: Forsyth County BOE

Agent Spainhour,

I wanted to follow up on my last phone inquiry regarding Mr. James Knox. Is he still listed on any watch list or any additional reports from the NC State Board of Elections? He has expressed interest in working as a poll worker and I did not want to proceed without confirming with you.

I appreciate your help with this and look forward to hearing back from you.

All the best,
Tim

Tim Tsujii
Director of Elections | Forsyth County Board of Elections
201 N. Chestnut Street | Winston-Salem, NC 27101
(336) 703-2801 desk | (336) 727-2893 fax
www.fcvotes.com
connect with us on @fcvotes

FORSYTH COUNTY BOARD OF ELECTIONS

Forsyth County Government we care

From: Tsujii, Tim <tsujiidt@forsyth.cc>
Sent: Friday, August 19, 2022 8:43 AM

To: Phillip Spainhour <pwspainhour@fbi.gov>
Cc: James Kaylor <jmkaylor@fbi.gov>
Subject: Re: Forsyth County BOE

I appreciate the introduction and your help. I'll certainly reach out if anything comes up.

All the best,
Tim

Tim Tsujii
Director of Elections | Forsyth County Board of Elections
201 N. Chestnut Street | Winston-Salem, NC 27101
(336) 703-2801 desk | (336) 727-2893 fax
www.fcvotes.com
connect with us:

Forsyth County Government

From: Phillip Spainhour <pwspainhour@fbi.gov>
Sent: Thursday, August 18, 2022 7:14 PM
To: Tsujii, Tim <tsujiidt@forsyth.cc>
Cc: James Kaylor <jmkaylor@fbi.gov>
Subject: RE: Forsyth County BOE

Tim,

James and I have well established partnerships with Director Karen Brinson-Bell and the NCSBE over the last few election cycles. Please let us know if we can be of any assistance to you in Forsyth County.

Best regards,
Phillip

A/SSRA Phillip W. Spainhour
FBI – Charlotte Division,
Greensboro Resident Agency,
1801 Stanley Road, Suite 400,
Greensboro, NC, 27407
Desk: 336-855-2655
Fax: 336-855-2645
Cell: 336-207-3922

From: Kaylor, James Martin (CE) (FBI) <jmkaylor@fbi.gov>
Sent: Wednesday, August 17, 2022 5:05 PM

To: Tsujii, Tim <tsujiidt@forsyth.cc>; Spainhour, Phillip W. (CE) (FBI) <pwspainhour@fbi.gov>
Subject: Re: Forsyth County BOE

Thank you Tim, yes I will see you tomorrow and have added Phillip to this email.

Phillip, Tim is the Director of the Forsyth County BOE. I let him know we are here if they need anything.

Best,
James

James Kaylor
Special Agent
FBI Charlotte - Raleigh RA
704-942-8968

From: Tsujii, Tim <tsujiidt@forsyth.cc>
Sent: Wednesday, August 17, 2022 4:06:19 PM
To: Kaylor, James Martin (CE) (FBI) <jmkaylor@fbi.gov>
Subject: [EXTERNAL EMAIL] - Forsyth County BOE

James,

It was a pleasure speaking with you today and look forward to meeting you in person at tomorrow's DHS TTX event. I've included my contact information below. Please send me Philip's contact information as well and I'll get that added to my phone.

Thanks again.

Tim

Tim Tsujii
Director of Elections | Forsyth County Board of Elections
201 N. Chestnut Street | Winston-Salem, NC 27101
(336) 703-2801 desk | (336) 727-2893 fax
www.fcvotes.com
connect with us:

Forsyth County Government we care

Outlook

FYI: Justice Department to Monitor Polls in 28 States on Election Day

From Mulé, Michael (CRT) <Michael.Mule@usdoj.gov>
Date Mon 11/7/2016 10:27 AM
To tsujiidt@forsyth.cc <tsujiidt@forsyth.cc>

https://www.justice.gov/opa/pr/justice-department-monitor-polls-28-states-election-day

NORTH CAROLINA VOTER REGISTRATION APPLICATION

07

1 Are you a citizen of the United States? [X] Yes [ ] No

IF YOU CHECKED "NO" IN RESPONSE TO THIS QUESTION, DO NOT SUBMIT THIS FORM.

Will you be at least 18 years on or before Election Day? [X] Yes [ ] No

IF YOU CHECKED "NO" IN RESPONSE TO THIS QUESTION, DO NOT SUBMIT THIS FORM.

2

Last Name: YIN

First Name: SHUQIN

Middle Name:

[ ] Jr [ ] Sr [ ] I [ ] II [ ] III [ ] IV [ ] V [ ] VI [ ] VII [ ] VIII

3

Date of Birth: [redacted]

State of Birth:

Voter Registration Number:

NCID:

NCDL or Non-operators ID Number: [redacted]

Last 4 Digits - Social Security Number: [redacted]

[ ] I do not have a NC driver license, ID card or a SSN.

RESIDENTIAL ADDRESS INFORMATION – No P.O. Boxes or Rural Routes

4

Street Address where you live: 423 WISE CT

Apartment, Lot, or Unit Number:

City: WINSTON SALEM

State: NC

Zip Code: 27127

County: FORSYTH

Have you lived here for 30 days or more? [X] Yes [ ] No

If "No," date moved? _____

MAILING ADDRESS AND CONTACT INFORMATION

5

Mailing Address:

Phone:

Email Address:

Address Description:

6

GENDER

[X] Female

[ ] Male

RACE

[ ] African American/ Black

[ ] American Indian/ Alaska Native

[X] Asian

[ ] Multiracial

[ ] White

[ ] Other

ETHNICITY

[ ] Hispanic/Latino

[X] Not Hispanic/Latino

POLITICAL PARTY AFFILIATION

[ ] Democrat [ ] Republican [ ] Libertarian

[X] Unaffiliated [ ] Other _____

If you indicate a political party that is not currently qualified, or you do not indicate a choice you will be listed as "Unaffiliated".

PREVIOUS VOTER REGISTRATION (This information will be used to cancel your previous voter registration in another county or state.)

7

Last Name and Suffix used in Previous Registration:

First Name and Middle Name used in Previous Registration:

Previous Address:

Previous County:

Previous City:

Previous State:

Previous Zip Code:

I attest, under penalty of perjury, that in addition to having read and understood the contents of this form, that:
I am a United States citizen, as indicated above; I am at least 18 years of age, or will be by the date of the general election; I shall have been a resident of North Carolina, this county, and precinct for 30 days before the election in which I intend to vote; I will not vote in any other county or state after submission of this form and if I am registered elsewhere, I am canceling that registration at this time; and I have not been convicted of a felony, or if I have been convicted of a felony, I have completed my sentence, including any probation or parole. (Citizenship and voting rights are automatically restored upon completion of the sentence. No special document is needed.)

Fraudulently or falsely completing this form is a Class I Felony under Chapter 163 of the NC General Statutes.

X [redacted]

Sign

11/04/2016 06:48:16 PM

Date

86-119-20161104064816

SDR 102015