Physical Security: Personal Safety

The 60 Second Security Series is intended to help election officials quickly identify, and address, potential security issues. Each topic includes a brief description, a list of security measures, and potential funding sources for making these improvements. More information about election security can be found at www.eac.gov.

About Personal Safety

Election officials continue to receive violent threats and intimidating statements, and this is an increasing reality for offices across the country. It is a priority of election officials to ensure the physical security of themselves and staff. There are proactive steps election officials can take to improve their personal security, and it is critically important to document and report every threat and develop a working relationship with federal, state, and local law enforcement. Some security measures and tools may be funded through federal grant programs that are administered by the states. More information about grant funding for election security can be found at the end of this guide. **If you have experienced threats, harassment, or intimidation in your capacity as an election official, contact your local FBI Election Crimes Coordinator or submit a report to the FBI at 1-800-CALL-FBI (225-5324), prompt 1, then prompt 3, or online at tips.fbi.gov.** For more information about how to improve your personal security as an election official, go to: www.eac.gov/election-officials/election-official-security

Definition: Personally Identifiable Information (PII)

PII is information that can be used to distinguish or trace an individual's identity. This information is often maintained by both government agencies and private businesses and may include an individual's name, social security number, date and place of birth, mother's maiden name, biometric records, or any other records that can be linked to an individual, such as medical, educational, financial, and employment information.

Security Measures

There are several important steps that you can take to improve your personal security while at work or online. These include:

Personal Security

○ **Documenting Threats:**

If you receive abusive messages, it is critically important to save all voicemails, emails, screenshots, text messages, or any other communications. Some key tips for documenting evidence of abuse include:

- Log the time, date, and phone number (if possible) for any harassing phone calls.
- Retain any call recordings or transcripts, if available and permissible by state law.
- Save any voicemails, including the date and time they were received.
- If the caller provides any identifying information (name, location, etc.), document these details.
- Capture screenshots of any threatening text messages, emails, or social media posts.
- Take contemporaneous notes to provide evidence of a threat or demonstrate a pattern of abuse.

○ **Protecting Yourself Online:**

Prevent hacking of your accounts and devices by using strong passwords, turning on two-factor authentication, and reporting any phishing emails. You can also request to have your information removed from appearing in Google searches. More information on removing PII

U.S. Election Assistance Commission

633 3rd Street NW, Suite 200 | Washington, D.C. 20001

www.eac.gov

June 2023 v 1.0

from a Google search can be found here:
eac.gov/sites/default/files/electionofficials/security/Memo_Removing_PII_from_Google_508.pdf

Office Security

○ **Facility Security:**

Before accessing an office or facility, elections staff should be required to have a name badge, ID, or other credential that shows they are authorized to enter the facility. Any visitors to the office should be required to sign in before entering the facility, and they should be identified as visitors with a name badge or other credential. All visitors should always be escorted by a credentialed staff member, and staff members should not allow anyone inside a facility unless they have been given official access. Offices and facilities should also consider the physical security of the location. This may include conducting a security assessment to determine if upgrades might need to be made to the structure to ensure the safety and security of staff and the public.

○ **Alarm Systems:**

Alarm systems can deter vandalization and alert elections staff and law enforcement of unauthorized access to a facility. For staffed offices and facilities, consider installing panic buttons that can alert law enforcement immediately in case of an emergency.

○ **Security Presence:**

Due to specific threats, or during critical times, it may be necessary to provide additional security services. Consider working with local law enforcement to provide extra security patrols at highly sensitive facilities, or during critical times. These may include the elections office, an equipment warehouse, polling locations during voting hours, or in-person polling locations where voting equipment is being stored outside of voting hours.

Funding Opportunities

HAVA Election Security Funding

Since 2018, Congress has appropriated $955 million in HAVA Election Security grant funds to the states for the administration of elections, including cybersecurity enhancements, and many local elections offices have been able to use these funds to reimburse the cost of security improvements. Check with your state elections office to find out how to apply for HAVA grant funding in your state. Additionally, the EAC has published FAQs and other information about how HAVA grant funding may be used. Allowable expenses may include costs associated with the purchase, installation, and maintenance of security equipment, provided they are benefiting elections. Physical security services and social media threat monitoring may also be allowed if these services are necessary for the protection and security of election facilities and personnel. Any non-election benefit may be allocated accordingly to non-HAVA sources. States can reach out to the EAC Office of Grants Management via email to clarify any concerns about allowability and allocability for specific activities and costs. For more information about the EAC Office of Grants Management and HAVA Election Security funds, go to https://www.eac.gov/payments-and-grants/election-security-funds or email grants@eac.gov.

Other Federal Grant Programs

Other federal grant funds may be available to improve election security. Grants through the Department of Homeland Security (DHS) and the Department of Justice (DOJ) may be used by election officials or partner agencies to provide security services for election officials and improve the security of election infrastructure. More information about these programs can be found here: www.eac.gov/other-federal-grants.