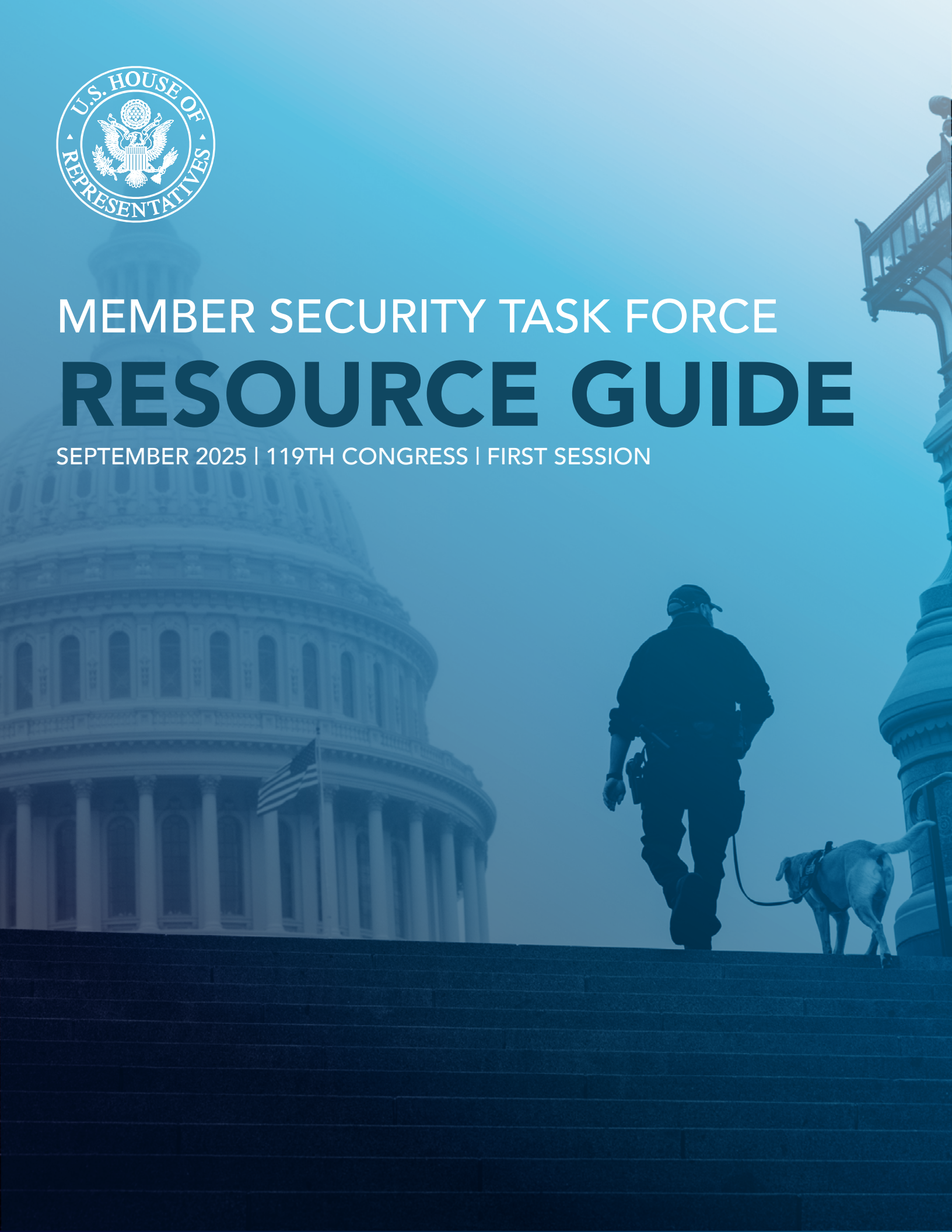

MEMBER SECURITY TASK FORCE

RESOURCE GUIDE

SEPTEMBER 2025 | 119TH CONGRESS | FIRST SESSION

Table of Contents

Introduction

This guide details the key security resources currently available to Members of Congress, their families, and staff. These resources build on lessons learned from prior incidents and combine physical protective measures with technology, cybersecurity and privacy protections, intelligence sharing, and training. Together, they form a layered security strategy that is essential to mitigating risk and maintaining continuity of congressional operations. The programs described in this guide are designed to be as unobtrusive as practicable, enabling Members to continue meeting with constituents, holding public events, and carrying out their constitutional duties with reduced risk.

The guide serves as both an overview of existing programs and a practical guide for their implementation. Members and staff will find detailed information about program offerings and best practices developed through years of operational experience. Members and staff are encouraged to familiarize themselves with these resources and work with their designated office emergency and law enforcement coordinators, as well as the House's institutional security partners, to fully utilize the available protective measures and services. Regular consultation of these materials and any subsequent updates to the resources described—as well as those provided by U.S. Capitol Police, House Sergeant at Arms, and Chief Administrative Officer—will help mitigate risk and enhance the security of the House community.

The Office Emergency Coordinator Program

Background

The Office Emergency Coordinator (OEC) Program was created in 2002 to assist in the dissemination of emergency information after biological attacks on the offices of Senators Patrick Leahy and Tom Daschle. Every DC and district office, including committee and support offices, selects an OEC from a member of its senior staff, as well as a backup OEC in case of emergency. The OEC's primary responsibilities focus on facilitating emergency preparedness training for staff and ensuring that offices have an open line of communication with the House Sergeant at Arms (HSAA) Emergency Management Division (EMD) in matters relating to emergency preparedness.

Planning and Personnel

- Develop and maintain the Occupant Emergency Plan (OEP) and Continuity of Operations Plan (COOP)
- Develop and maintain office-specific emergency information, including lists of emergency contacts and important phone numbers and documents
- Ensure all office staff are trained on how to respond to emergencies and receive a copy of the OEP
- Identify staff with special needs and establish an emergency assistance system by requesting a volunteer to serve as an emergency evacuation assistant, and informing HSAA EMD that the office has a special needs staff member
- Obtain and maintain up-to-date staff emergency contact information
- Ensure the office participates in emergency training and drills
- Inspect office emergency response equipment on a regular basis to ensure functionality and adequacy (e.g., annunciator, Go Kit)

Emergency Response and Coordination

- Serve as the office point-of-contact with the HSAA EMD and the United States Capitol Police (USCP) regarding emergency planning, preparedness, and response
- Ensure the Chief of Staff and/or other designated office staff are notified whenever information about actual or potential emergencies is received or when directed to take a protective action (e.g., evacuation, shelter in place, etc.)
- Acquire, maintain, and bring (or designate someone in the office to bring) the Office Emergency Go Kit and annunciator pager during evacuations, when told to go to an internal relocation site, or moving to a shelter in place location
- Ensure staff accountability and reporting to USCP at their request during emergency events

Equipment Provided by the House Sergeant at Arms

The HSAA supports Member offices by providing the following equipment free of charge for use in the case of emergencies. One of the OEC's most important responsibilities is, in partnership with HSAA EMD, ensuring that the Member and staff are properly trained to use this equipment, and that all items are accessible and maintained for use in an evacuation:

Duress Buttons[1, 2]	Wireless Emergency Annunciators[3]
Escape Hoods[4]	Victim Rescue Units (VRUs)[5]
Go Kits[6]	

Member Security Best Practices

Two critical resources for every DC, district, Member, committee, or support Office are Office Emergency Plans (OEP) and Continuity of Operations Plans (COOP). When an office's OEC completes the advanced stages of their training, they will have designed or revised that office's OEP and COOP to help Members and staff navigate periods of disruption where every moment matters.

Office Emergency Plan (OEP)

As part of basic certification, OECs complete one of the following worksheets, which guides them through the process of creating an OEP for their office, along with three in-person Staff Academy Trainings to prepare them for a leadership role in emergency management.

[1] House of Representatives, *Duress Buttons,* HouseNet, https://housenet.house.gov/page/3911?SearchId=0.
[2] House of Representatives, *Duress Button User Guide,* HouseNet, https://housenet.house.gov/page/3473?SearchId=150163.
[3] House of Representatives, *Wireless Emergency Annunciators,* HouseNet, https://housenet.house.gov/page/4027?SearchId=0.
[4] House of Representatives, *Escape Hoods,* HouseNet, https://housenet.house.gov/page/4029?SearchId=0.
[5] Victim Rescue Units are available for staff identified with special needs and their assistants. VRU caches are also available at emergency elevator staging areas for use by mobility impaired visitors, staff and their emergency evacuation
[6] House of Representatives, *Go Kits,* HouseNet, https://housenet.house.gov/page/4028?SearchId=0.

Continuity of Operations Plan (COOP)

To complete the advanced certification process, an OEC attends two additional crisis response trainings and designs a COOP, which can be activated at the direction of a member or their designee.
The COOP lays out the actions, capabilities, essential staff, and physical resources needed to continue operating when an emergency makes the primary workspace uninhabitable or inaccessible.

Level	OEP Worksheets	Trainings
Basic Certification	DC OEP Worksheet[7]	"Emergency Procedures and Escape Hood Training."
	District OEP Worksheet[8]	"OEC Roles and Responsibilities."
		"How to Respond to an Active Shooter."
Advanced Certification	Member Office COOP Worksheet[9]	"CPR and AED Training."
	Committee Office COOP Worksheet[10]	"Stop the Bleed."
	Support Office COOP Worksheet[11]	

[7] House of Representatives, *D.C. Office Emergency Plan Worksheet – 119th Congress,* HouseNet, https://housenet.house.gov/page/3092.
[8] House of Representatives, *District Office Emergency Plan Worksheet - 119th Congress*, HouseNet, https://housenet.house.gov/page/3207.
[9] House of Representatives, *Member Office COOP Plan Worksheet – 119th Congress*, HouseNet, https://housenet.house.gov/page/3079.
[10] House of Representatives, *Committee COOP Plan Worksheet – 119th Congress*, HouseNet, https://housenet.house.gov/page/3078.
[11] House of Representatives, *Support Office COOP Plan Worksheet – 119th Congress*, HouseNet, https://housenet.house.gov/page/3059.

Emergency Planning Resources

Planning for emergencies is a critical function of Member offices, committees, and support offices. HSAA EMD has created several resources to assist House offices in planning for emergencies:

Bomb Threats	Evacuations	Concerning Callers/Visitors	Government Emergency Telecommunications Service (GETS)
• Search all written and electronic communications for bomb threats • Do not touch or move suspicious packages • If a bomb threat is suspected, do not pull the fire alarm; await instructions from the authorities • If a threat is received via phone call or in person: o Remain calm and keep caller on the phone o Write down all details about the threatener o Ask questions about the bomb, including where it is and when it will go off o Do not hang up the call, even if the caller hangs up o Write down the phone number, if possible	• Evacuation notices in the Capitol complex will be noticed when there is a life safety threat, such as a fire or bomb threat, or a hazardous material threat • Prior to an evacuation, all offices should designate a primary and secondary OEC who will be responsible for ensuring that all staff evacuate properly • When evacuating make sure to: o Lock all safes o Close, but do not lock, office doors o Bring the Emergency Annunciator Page and other items required o Help all staff exit the building safely o Once evacuated, the OEC should account for all staff and remain in place until further notice	• Stay calm and write down as many details as possible • If a threat is issued, ask for specifics on their plan, including when, where, and how they plan to attack • Note the caller/visitor's name, appearance, speech pattern, emotional state, and accent or dialect • Utilize the panic button if necessary • Fill out the LEC form for a Concerning Visitor/Concerning Caller afterward	• The GETS program is offered by the Department of Homeland Security and provides authorized users with improved call completion on public landline networks • The program allows authorized personnel priority calling during an emergency or when landlines are congested • Authorized users are provided with a GETS calling card with a universal number and unique pin for accessing the system • All Members are automatically provided with a GETS card, but staff can be added with permission from the Committee on House Administration

The District Office Security Program

Background

The HSAA administers the District Office Security Program through its District Security Service Center (DSSC), an office which emerged in 2017 as a one-stop-shop for Members' in-district security needs. By centralizing security services and standardizing protective measures, such as mail screening hoods and secure communications capabilities, the DSSC helps Members select and secure appropriate spaces for constituent service while providing essential security equipment, training, and coordination with local law enforcement partners.

Figure 1: DSSC Regional Security Specialist Coverage

The DSSC assigns dedicated regional Security Specialists to assist Members and security coordinators in navigating the complex challenge of balancing security with constituent accessibility. These specialists help Members assess potential office locations, implement appropriate protective measures, and maintain security protocols tailored to their district's unique circumstances. The District Security Program has become increasingly vital as district staff bear the brunt of confrontations with individuals emboldened by inflammatory, conspiratorial rhetoric.

Security Assessment and Site Selection

The DSSC's Security Specialists play a vital role in the district office selection process, from security awareness briefings, which HSAA provides to district staff upon request, to providing guidance on existing security infrastructure at a potential office site and coordinating law enforcement support for public appearances. Federal buildings, courthouses, and other government facilities can make ideal locations for district offices, offering built-in protection such as security screening, surveillance systems, and law enforcement at rates generally unattainable at commercial locations. For Members who must select commercial spaces, Security Specialists can identify properties with essential security features like multiple emergency exit routes, secure reception areas, and spaces suitable for safe rooms and secure mail processing.

Security Systems and Support

Once a suitable location is identified, the DSSC provides standard security packages including intrusion detection systems, wireless duress buttons, motion sensors, and video intercoms for each Member's flagship (primary) district office. The program covers $150 in monthly monitoring fees for district office security systems while also facilitating the installation of supplemental security features through approved vendors, though additional measures must be funded through the MRA. The DSSC is also available to provide security awareness briefings to Members, staff, and law enforcement partners as needed.

Member Security Best Practices

Carefully evaluating potential office locations is one of the most important security decisions Members make. The right location can provide built-in security features that would be cost-prohibitive to install in commercial spaces. But regardless of the type of space chosen, maintaining strict control and monitoring over access points is essential.

The DSSC also provides complimentary protective gear for staff, such as mail safety hoods, along with security awareness trainings and individualized support for district offices.

When selecting and securing a district office, the DSSC recommends the following:

Office Location	Access and Crowd Control	Mail and Gift Processing
• Prioritize space in federal buildings, courthouses, or local government facilities with existing security screening and law enforcement presence. • Contact your state or territory's GSA Congressional Services Representative to acquire federal space for District offices.[12] • If government space is unavailable, look for commercial properties with controlled access points, a reliable telecommunications connectivity, multiple exits, and spaces suitable for secure reception areas. • Opt for proximity to local law enforcement and emergency services when evaluating locations. • Assess your location's surroundings for risk factors such as dimly-lit streets or parking areas, elevated neighborhood crime, and visibility from public spaces. • Verify building infrastructure can support necessary security technology installation.	• Prioritize offices with layouts that create clear separation between public and private spaces. • Control office access and monitor potentially concerning activity by requiring visitors to sign in upon arrival. • If a facility with screening or on-premises security is not available at your location, or local threat levels are elevated, discuss options for on-premises security or patrols with local law enforcement. • Secure all doors and windows with locks and alarms vetted by HSAA.	• Designate your office's mail processing area in a room separate from the rest of the office with a closeable door, operational telephone, and away from air vents. • Wear a mask, gloves, and use mail hoods when processing any mail sent to District offices. • If you find white powder or another suspicious substance when opening mail, place the mail hood down, remove your gloves, leave your mask on, notify office leadership and local authorities, and remain where you are until help arrives. • Use the protective equipment supplied by DSSC and contact HSAA Police Services Division to request additional protective equipment if needed. • Post emergency procedures provided during Security Awareness Briefings

[12] General Services Administration, *Contact information for congressional services representatives,* https://www.gsa.gov/about-us/contact-us/contact-by-topic/contact-information-for-congressional-services-representatives.

Guidance for Interacting with Law Enforcement

On June 4, 2025, Committee on House Administration Ranking Member Joe Morelle issued a Dear Colleague letter providing guidance to Members and staff who interact with law enforcement in the execution of their office's constitutional duties. The letter stated:

> As the Trump Administration continues to engage in efforts to intimidate Members of Congress into silence and capitulation, it is important that you and your staff are aware of their rights when interacting with law enforcement, particularly in district offices. The vast majority of law enforcement officers are honorable professionals; however, the Trump Administration has weaponized agencies to obstruct us from carrying out our constitutional duties. Accordingly, we want to remind you of some key principles that can assist in protecting you and your staff against any unlawful encroachment on the constitutional rights and responsibilities of Members of Congress. While no two situations are identical, it is useful to keep in mind these general principles when interacting with law enforcement.
>
> As a threshold matter, law enforcement can only access your space with consent, a valid warrant (e.g., search warrant, arrest warrant), or if there are exigent circumstances. Exigent circumstances include a relatively narrow set of circumstances when people are in imminent danger, where evidence of a crime could be imminently destroyed, or when a suspect could immediately escape from law enforcement. Absent these conditions, law enforcement has no right to enter a congressional office.
>
> If a law enforcement agency's presence is a surprise, out of the ordinary (i.e., they weren't called for assistance or it is an agency that would not normally have a reason to be at the office) or appears pretextual (i.e., you have reason to believe have an ulterior motive beyond the safety of your office for wanting access to your space), you should exercise caution in your interactions with them.
>
> To the greatest extent possible, exercise control of your physical space and limit access to it. One way to do this is requiring the scheduling of appointments in advance and maintaining control of entry with devices like door buzzers or buttons. While this kind of controlled access serves as a general safety precaution for you and your staff, it also allows for "arm's length" conversations with law enforcement to help ascertain the reason for their presence and whether it's legal or justified.
>
> If law enforcement asks or demands to be let in, you can respond by asking to see a warrant. Without a warrant, your consent, or an exigent circumstance of the kind described above, law enforcement has no right to enter the premises. If the agents claim they are there to perform a welfare or safety check, but no one in the office requested such a check, you can respond that staff will perform the check and report back to them with any issues.
>
> While the principles outlined above are most directly applicable to situations when there is uncertainty about a law enforcement agency's presence and intentions, it is important to recognize that there may be legitimate reasons for law enforcement or other first responders to access your office. If your district office is located in a federal building with a federal protective agency, that agency may need to access your office in an emergency or threat situation. It is encouraged to try to establish an agreed upon protocol with the agency in advance for when and under what conditions they may enter the space.
>
> Controlling your physical space and knowing your rights are key to the peaceful resolution of incidents and to protecting your staff and your office's interests and prerogatives.

The Residential Security Program

Background

HSAA's Residential Security Program was established in 2022 due to the escalating series of threats to elected officials and their families that have proliferated in recent years. That same year, the vicious attack on Paul Pelosi, husband of Speaker Nancy Pelosi, in their San Francisco home further highlighted the urgent need for members and their families to harden their residences from malicious actors.[13]

The increasing frequency and severity of threats against Members of Congress has necessitated a multi-layered approach to residential security. The current Residential Security Program provides up to $20,000 for security system equipment and installation and $150 monthly for monitoring services. This program complements other resources available both through the House and other entities, including the Federal Election Commission's 2021 guidance allowing campaign funds to be used to hire security personnel.[14]

Residential Security Equipment

HSAA-funded residential security systems include: Control Panels, Keypads, Motions Sensors, Door/Window Contacts, Duress Buttons / Fobs, Intercom Sets.[15]

MRA funds can be used to procure any of the following if not already provided by HSAA:

Intrusion Detection	CCTV Systems	Other Security Equipment and Fixtures
Control panels / keypads	Video recorder	Exterior/interior door locks
Duress buttons & key fobs	Monitors	Exterior lighting/wiring
Glass break & motion sensors	Indoor cameras	Smoke & carbon monoxide alarms
Door & window contacts	Outdoor cameras	Water leak sensors
Cellular & network communicator(s)	AI enhanced CCTV systems	Security film
		Video analytics

[13] Mychael Schnell, *Calls Grow for More Lawmaker Security After Shocking Attack on Paul Pelosi*, The Hill (Oct. 31, 2022), https://thehill.com/homenews/house/3716376-calls-grow-for-more-lawmaker-security-after-shocking-attack-on-paul-pelosi/.

[14] Federal Election Commission, *Letter from FEC Chair Shana Broussard to the Honorable Veronica Escobar,* Advisory Opinion 2020-06, https://www.fec.gov/files/legal/aos/2020-06/2020-06.pdf.

[15] House of Representatives, *Selecting Security Equipment for a District Office,* HouseNet, https://housenet.house.gov/page/3106?SearchId=0.

Monitoring and Alerting Services

Members should take a comprehensive approach when implementing residential security services through the program. This includes conducting an initial security assessment with the help of HSAA's Police Services Division, installing multiple layers of protection provided by approved vendors (intrusion detection, video surveillance, panic buttons), and ensuring all family members, staff, and hired security personnel are trained on operational and physical security protocols. The HSAA Police Services Division and USCP offer in-person security awareness briefings that provide detailed guidance on maximizing these security measures in a residential security context, but Members should also regularly review and update their security systems to address evolving threats and technological advances which introduce new vulnerabilities.

Personal Security Services

While physical security systems form the foundation of home protection, Members should also carefully consider their security personnel needs. In August 2025, the House established the Personal Security Pilot Program, which allows Members to hire licensed and insured individuals or companies to provide personal protective, residential, or event security**.** The Program provides up to $10,000 per month (an increase from the initial $5,000 limit) and is authorized through November 30, 2025 (extended from the initial September 30, 2025, end date).

Security personnel engaged under the Personal Security Pilot Program may not be used in Washington, D.C., nor may they be used for investigatory services. Members must review program guidelines and submit the Personal Security Attestation Form, available by contacting SAA_Residential_Security@mail.house.gov, to confirm insurance and licensing checks have been performed in order to be eligible for reimbursement.

Members may also utilize campaign funds for professional security staff, as permitted by Federal Election Commission guidelines.

Members with concerns or those facing specific threats should use the Member Secure Portal to coordinate with USCP TAS, who can help determine the appropriate deployment of additional security resources.

Member Security Best Practices

The safety of a residence is held in place by three rings of protection, all of which must be maintained to ensure effective and responsive protection for Members and their families. Home security that relies on one service, piece of equipment, or protocol leaves protectees vulnerable to a single point of failure, an inherently risky approach. But by establishing layers of security at the perimeter, exterior, and interior of residences, Members can ensure the safety of themselves, their loved ones, and their property.

The perimeter of a Member's residence forms their home's **outer ring of defense**, and it should be configured to deter, detect and delay potential threats without compromising situational awareness for any inhabitants or on-site security personnel. The exterior structure of Member residences, **the middle ring of defense**, should be hardened against intrusion, alert inhabitants and security personnel of impending intrusion, and include effective emergency exits.

A residence's living spaces are within **the inner ring of defense**, depending on the proper functioning of the other rings to maximize the protection, situational awareness, and emergency communication capabilities of Members and their families.

The Outer Ring	The Middle Ring	The Inner Ring
• Request a residential security assessment from an HSAA-vetted security firm • Coordinate patrols of residential perimeters and access points with USCP, local law enforcement, or a private security service. • Install motion-activated lighting covering shaded areas and access points, preferably featuring an independent power source or battery back-up. • Ensure clear lines of sight for CCTV and security personnel, evaluating surroundings for hiding spots • If property conditions permit, consider perimeter fencing or vehicle barriers from an HSAA-vetted security company. • Install HD outdoor cameras with night vision capability from an approved vendor to monitor all entry points and potential access routes. • Ensure street numbers are clearly visible and reflective for rapid emergency response in low-light conditions	• Install and maintain HSAA-approved intrusion detection systems incl. motion sensors; duress buttons; & glass break sensors. • Ensure that all doors and windows have properly installed locks and reinforcements, such as by using a "Charlie bar" in the bottom track of a sliding glass door to prevent opening. • Prevent a breach through a window or sliding glass door by applying security window film or by installing laminated security glass. • Position high-resolution, night vision-enabled cameras to capture face-level images at all entry points. • Establish a designated, monitored secure package delivery area away from main entrance. • Maintain multiple, fully-lit emergency evacuation routes. • Arrange periodic exterior security checks from HSAA or a vetted security company.	• Maintain an independent interior camera system a separate storage system from exterior cameras. • Keep a telephone, flashlight, and phone number of local law enforcement by your bed. • If you catch an intruder trying to break into your residence, do not challenge them or block their escape route. Make as much noise as possible. If the incident is happening at night, turn on all the lights you can. • Maintain updated emergency contact card information with the USCP Command Center for all Family members. • Designate a safe room in your home with reinforced entrances, no windows if possible, and redundant emergency communications equipment. • Conduct regular home security system tests in coordination with HSAA.

The Cybersecurity Program

Background

In 2023, the Residential Security Program expanded to include cybersecurity services for Members' residences. Cyber-attacks are becoming increasingly common and sophisticated, necessitating the expansion of the Residential Security Program to include cybersecurity upgrades. The loss of sensitive data regarding the Member, their family, or staff can increase the risk of physical attack, particularly when data related to addresses, locations, travel, and scheduling is put at risk.

Nation-state actors are increasingly using advanced cyber-attacks to gain access to the devices of Members. It is vital that Members work to secure their technology to ensure that their physical safety and sensitive data is not put at risk. To ensure the continued safety of Members in the wake of these new threats, the Residential Security Program was expanded to include cybersecurity services.

HSAA will assume the cost of certain residential cybersecurity upgrades that provide additional layers of security to protect sensitive personal information and online activity. HSAA will pay for the implementation and installation of cybersecurity services, up to a yearly total of $1000. Services available through this program include network security, antivirus and malware protection, virtual private networks (VPN), password managers, and data and privacy protections. These protections will help to secure devices, home networks, and accounts to safeguard sensitive House data.

Cybersecurity Stipend

In addition to covering $150 in subscriptions and fees for monitoring, alerts, and other security services under the Residential Security Program, the HSAA offers each Member a yearly $1,000 stipend for a wide and growing range cybersecurity services.

House Cybersecurity Services[16]

Software/Services	Installation
Network security	Software config. & setup
Antivirus/malware	Vendor supplied training
Virtual Private Network	
Password Manager	
Data and Privacy Protection	

In addition, the House has optional free services that provide additional protection. For example, the House offers dark web monitoring services that provide alerts when a Member's personal information is found on the dark web, giving Members an opportunity to remove such information via services covered by the Cybersecurity Program. Members may add their personal accounts and accounts of family members (i.e., their children or spouse) to this tool free of charge. The House also provides access to a free automatic threat monitoring app for the personal devices of a Member and their immediate family. For additional information on the House cybersecurity offerings, reach out to HSAA or the Chief Administrative Officer for assistance.

[16] Note: All cybersecurity services and products installed or operating on official devices must be vetted by CAO OCS

Cybersecurity Checklist for International Travel

Members should be proactive in securing their devices ahead of international travel, which exposes Member PII and other sensitive information to unique cybersecurity risks from foreign malicious actors. The Chief Administrative Officer (CAO) Office of Cybersecurity (OCS) recommends the following Checklist for International travel to safeguard Member data and maintain the security of the House Network.[17]

Before Departing	During Travel	After Returning
• Do not bring your personal or official devices; contact CAO Telecommunications for travel devices and guidance. • Set up temporary email and Active Directory accounts via CAO service requests. • Establish strong, unique passwords and device lock screens. • Obtain and use House-trusted USB data blockers (e.g., Portapow). • Use Radio Frequency Interference (RFI) Faraday bags to block signals. • Apply privacy screen protectors to devices. • Update operating systems and security applications; delete unnecessary apps. • Install cybersecurity apps like MTD for Work or Airwatch. • Disable automatic Wi-Fi connectivity.	• Keep devices/cables on you; never leave them unattended. • Lock or power off devices when unused. • Disable Wi-Fi/Bluetooth; enable only when necessary. • Avoid public Wi-Fi/local networks; use mobile hotspots securely. • Only Connect to the House network remotely via VPN. • Use USB data blockers; avoid unknown USB ports. • Charge devices with AC outlets using personal chargers/adapters. • Prevent screen exposure to "shoulder surfers." • Avoid online shopping or accessing banking accounts. • Reboot devices daily to reduce malware risks.	• Return borrowed temporary devices to their respective offices. • Factory reset all temporary devices before returning them. • Scan electronic gifts for malware via the Office of Cybersecurity; consider disposal. • Assess non-electronic gifts with HSAA House Security for safety.

[17] House of Representatives, *Cybersecurity Checklist for International Travel,* HouseNet, https://housenet.house.gov/page/3117?SearchId=149788.

Member Security Best Practices

HSAA Considerations for Social Media Use

Be mindful of information being published on social media platforms. An individual with malicious intent could use social media and online information to identify a Member's assets and whereabouts or to plan an encounter.

Open affiliation with a Member online may also make family members and staff targets for grievances and discontent. Keep the following in mind before posting, recognizing that information shared on social media and other online sources is often permanent:

- Avoid posting the specific time and date of public appearances and posting about non-public activities.
- Try to only post public event-related content after the Member has left the event.
- Avoid sharing sensitive personal information in your posts (e.g., employer, whereabouts, patterns in your routine).
- Maximize privacy settings on your personal accounts to only allow posts to be viewed by friends and family.
- If targeted by online threats or concerning posts:
    - Capture the image and report it to USCP.
    - Do not delete the post until advised by USCP. Include hyperlinks to the post in the report.
    - Please keep full URLs, timestamps and other identifying information.

Device and Account Management

OCS uses a defense-in-depth approach, maintaining layers of cyber protection from cyber threat monitoring and detection, to providing secure connectivity and devices to Members and staff on official travel and CODELs. But to ensure that personal and official information is not compromised, especially including sensitive data that could put the Members and staff in harm's way, it essential to follow guidance from OCS on the responsible use of House devices and House sensitive data and maintain situational awareness of cyber threats that increasingly target, harass, and threaten Members of Congress.

Personal Device, Account, and Network Protection	Protection Against Fraudulent Meetings	Phishing Protection	Monitor for Concerning Social Media Behaviors
• Regularly update software • Remove unnecessary services and software • Run antivirus software consistently • Install a network firewall • Regularly back up data • Install the OCS recommended LookOut App • Do not reuse passwords for multiple accounts • Add the Member's personal accounts, including those of family, to the Office of Cybersecurity's dark web monitoring list • Change default login passwords and usernames • Do not share Wi-Fi router username or password • Use a VPN to encrypt traffic to and from your devices	• Contact meeting requestors through a different communication channel to verify the sender's identity, and contact the Office of Cybersecurity if the sender seems suspicious • Reach out to the agency or embassy of the sender to verify their identity • If a Member believes that they are the victim of a fraudulent meeting, immediately: o End the call or meeting o Send the meeting information to the Office of Cybersecurity o Contact the State Department or FBI to help in determining if the meeting was legitimate	• Look out for signs of a phishing attempt, including cheap offers for goods and services, requests for personal information, suspicious senders, poor spelling and grammar, and suspicious links • Avoid clicking links, URLs, or attachments, especially from an unknown or untrusted sender • Report all suspicious communications to OCS and to the communication platform	• Use of or interaction with dehumanizing language, racial or misogynistic slurs, or violent content • Signs of mobilization, including efforts to secure weapons, travel to a location where a Member will be, detailed plans for attack, or doxing • Membership or interaction with extremist groups, including neo-Nazis, white supremacists, anti-government militias, and vigilante groups

The Law Enforcement Coordination Program

Background

The HSAA established the Law Enforcement Coordination (LEC) program to create and maintain critical partnerships between Members of Congress, their district staff, and local law enforcement agencies that serve their communities. This program emerged from a recognition that while the USCP maintains primary jurisdiction over the safety of Members, most security incidents occur far from Washington D.C., where local law enforcement must serve as first responders.

The LEC program provides a crucial bridge between federal and local law enforcement, enabling streamlined coordination of law enforcement coverage for events while facilitating information sharing on potential threat actors. By centralizing coordination through a dedicated LEC form that captures comprehensive contact information for Members, staff, and family members, the program ensures that local agencies can quickly verify the legitimacy of emergency calls and respond appropriately to security incidents.

LEC Services

The LEC program offers several unique services that complement other House security initiatives:

- Coordinates security briefings between Members' offices and local law enforcement leadership to establish protocols before emergencies arise.
- Provides local agencies with official points of contact to verify emergency calls and "swatting" attempts.
- Facilitates joint security planning for high-profile district events and public appearances.
- Maintains updated emergency contact information for Members, staff, and family members through a secure database.

Law Enforcement Partnerships

While the USCP maintains primary responsibility for Member security in the Capitol, local law enforcement agencies are often the first line of defense against threats in Members' districts. The LEC program helps forge these critical partnerships by:

- Conducting outreach to police departments, sheriffs' offices, and state law enforcement agencies in Members' districts.
- Providing local agencies with direct lines of communication to USCP TAS.
- Coordinating intelligence sharing between federal, state and local agencies regarding potential threats.
- Establishing protocols for emergency responses to Member residences and district offices.
- Facilitating joint training exercises between USCP, local law enforcement, and Member security teams.

Travel Security Program

When Members travel, especially via transit hubs such as airports or train stations, HSAA recommends that LEC Coordinators consider all operational security requirements from door to door, including proactive communication with USCP and local law enforcement. Members who have any reason to fear confrontation or harassment at airports should participate in the HSAA Travel Security Program by submitting a Member Travel Security Information Request Form through the Member Secure Portal.[18] House security personnel coordinate with the TSA and local law enforcement partners at destinations to arrange a police escort to accompany Members from arrival through TSA-secured portions of the airport. HSAA recommends the following best practices:

Driving Requirements	Pre-Travel Security Considerations	Travel Essentials	Special Member Security Considerations
• Search all written and electronic communications for bomb threats • Do not touch or move suspicious packages • If a bomb threat is suspected, do not pull the fire alarm; await instructions from the authorities • If a threat is received via phone call or in person: o Remain calm and keep caller on the phone o Write down all details about the threatener o Ask questions about the bomb, including where it is and when it will go off o Do not hang up the call, even if the caller hangs up o Write down the phone number, if possible	• Evacuation notices in the Capitol complex will be noticed when there is a life safety threat, such as a fire or bomb threat, or a hazardous material threat • Prior to an evacuation, all offices should designate a primary and secondary OEC who will be responsible for ensuring that all staff evacuate properly • When evacuating make sure to: o Lock all safes o Close, but do not lock, office doors o Bring the Emergency Annunciator Page and other items required o Help all staff exit the building safely o Once evacuated, the OEC should account for all staff and remain in place until further notice	• Prepare an all-purpose bag while traveling with the Member. The bag should contain, but not be limited to, the following: o Small first aid kit: bandages, gauze, burn gel, EpiPen, etc. o Over-the-counter medicines: e.g., Excedrin, Tylenol, Advil, etc. o Prescription medications, if appropriate. o Conduct a comprehensive sweep of Member and staff rooms prior to vacating the premises to ensure nothing is left behind (e.g., documents, suitcase, cell phone, wallet, passports, valuables in the safe, etc.).	• Research indicators of potential public and media reaction to the Member's travel location or reason for visit. • What is the current political climate? • Is there another event at the site or in close proximity that may impact the Member's visit? • Another dignitary, celebrity, etc. that may have security or a reason for concern • Determine if it will be necessary to secure the presence of local law enforcement. • Does the nature of an event, its location and participants require police support? • Does police intelligence and threat assessment information indicate a need for police support?

[18] Office of the Sergeant at Arms, *Member Travel Security Information Request Form,* https://saa.house.gov/member-travel-security-information-request-form.

Event Security

Event Security Planning

Public events demand close advance coordination with venue staff and law enforcement at all levels. Each gathering type presents specific vulnerabilities requiring targeted security measures.

- LEC Coordinators should submit all event details through LEC at least 72 hours ahead, preferably one week in advance, for comprehensive threat assessment and local agency coordination.
- Require RSVPs for events whenever the Member will be present, and share attendee lists with LEC as soon as possible to allow for proper vetting by USCP.
- Walk through and document safe room location, evacuation routes, and screening procedures with local law enforcement or other security personnel prior to the day of the event.

Member Security Best Practices

Build Strong Local Law Enforcement Partnerships

The success of Member security operations in district depends heavily on direct engagement with local law enforcement agencies who serve as first responders during emergencies or threats. Members who maintain active communication with police chiefs, sheriffs, and field office leadership consistently benefit from faster response times and more effective coordination during security incidents.

- Meet directly with law enforcement leadership with jurisdiction over district offices and residences to establish points of contact and emergency protocols.
- Begin discussions regarding supplemental security measures like patrols of residences/district offices or dedicated details, recognizing these may require additional funding arrangements.
- Maintain regular communication about protest activities, emerging threats, and concerning individuals even in the absence of specific incidents.
- Work with local agencies to map out specific response plans for security incidents at residences and district offices.

Engage with the Law Enforcement Coordination Program

The HSAA Police Services Division and USCP TAS provide essential intelligence gathering, threat analysis, and coordination support. Their effectiveness relies on rapid information sharing about potential threats and scheduled events.

- Update Law Enforcement Coordinator forms immediately when Member, staff, or family contact information changes.
- Contact USCP TAS as soon as staff identifies concerning behaviors or communication directed at Members, their families, or their staff.
- Share intelligence received from local law enforcement about planned protests or demonstrations.

Law Enforcement Coordinator Duties

An office LEC serves as the liaison with local law enforcement agencies and USCP. Each Member office should assign one senior district staff as primary LEC and one staff member as an alternate LEC.
Through the LEC program, HSAA and USCP empowers Emergency Coordinators to be the link between district staff, local law enforcement, and federal security resources—ensuring law enforcement support for Member movements, public engagements, and residential security.

- Only share Member schedules and travel details to authorized personnel through secure channels.
- Discuss the behaviors, communications, or online activity of local individuals exhibiting violent extremist tendencies with liaison officers of in-district law enforcement agencies.
- Keep emergency contact lists current and immediately accessible to all security partners including HSAA Police Services Division and local law enforcement.
- Document and report all threatening behaviors or communications, online or offline, to LECOR and local law enforcement with as much information about the incident and threatening individual(s) as possible.

Other Key Resources for Members and Staff

Sergeant at Arms Office of House Security (OHS)

The Office of House Security (OHS) serves as the central authority for protecting classified information and coordinating security measures across the House of Representatives. Working closely with the U.S. Capitol Police and intelligence community partners, OHS develops and implements comprehensive security protocols to safeguard Members, staff, and sensitive information.

OHS provides essential services including:

Foreign Travel Resources: The OHS equips Members and staff with critical security guidance and support for international travel through comprehensive pre-departure briefings, real-time threat monitoring, and standardized reporting mechanisms for foreign contacts and travel activities.

- Issues alerts and warnings from State Department and Embassy notifications.[19]
- Processes foreign national contact information reports for tracking interactions abroad.[20]
- Maintains standardized travel reporting forms for official international travel.[21]
- Provides training material on defensive tactics briefings for CODELs, STAFFDELs, and personal travel.[22]
- Coordinates with diplomatic security for travel threat assessments.
- Provides foreign travel briefings tailored to specific destinations.[23]

Technical Countermeasures & SCIF Services: OHS conducts sophisticated technical surveillance countermeasure sweeps (TSCM)[24] to prevent or detect the clandestine interception of sensitive, classified, or private information, while managing the House's Sensitive Compartmented Information Facilities (SCIFs) for classified meetings and materials.[25]

Security Clearances: OHS administers a rigorous security clearance program limited to two cleared staff per Member office.[26] The office's range of services includes managing SCIF access, clearance transfers between House offices, and processing visit authorization requests for staff attending a meeting, briefing, or hearing that requires a security clearance to be passed to other agencies.[27]

Sergeant at Arms Protocol and Special Events Division

The Protocol and Special Events Division coordinates security logistics for official ceremonies and VIP visits to the Capitol complex, ensuring the safety of Members, staff, and visitors via collaboration with Leadership offices and committees.[28]

---

[19] Department of Homeland Security, National Terrorism Advisory System, https://www.dhs.gov/national-terrorism-advisory-system; Overseas Security Advisory Council, Alerts & Travel Advisories, https://www.osac.gov/Content/Browse/Report?subContentTypes=Alerts%2CTravel%20Advisories; U.S. Department of State, Travel Advisories, https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/.
[20] House Sergeant at Arms, Foreign National Contact Information Form, https://saa.house.gov/_cache/files/d/9/d9de2ca8-e6bf-47dc-b8ed-64fb9e366919/63DB4DF0FA23DB718C374A1E308E025F.ohs-foreign-national-contact-information-form-v2-002-.pdf.
[21] House Sergeant at Arms, Foreign Travel Reporting Form, https://saa.house.gov/_cache/files/2/6/26937534-345e-4e9d-bc37-000855321414/B026A99FEF8419AAB597C724A07E9B47.ohs-foreign-travel-reporting-form-v2.pdf.
[22] House Sergeant at Arms, Defensive Tactics on International Travel, https://saa.house.gov/_cache/files/3/c/3c418fb4-265d-4b83-a379-dc5305ad41f9/1512DCEF0C7655E8A5F6F9159147C396.defensive-tactics-on-international-travel.pdf.
[23] House Sergeant at Arms, Foreign Travel Program Overview, https://saa.house.gov/foreign-travel.
[24] House Sergeant at Arms, Technical Surveillance Countermeasures (TSCM) Sweep Request, https://saa.house.gov/tscm-sweep.
[25] House Sergeant at Arms, Room Reservation Request, https://saa.house.gov/room-request.
[26] House Sergeant at Arms, Security Clearances, https://saa.house.gov/security-clearances.
[27] House Sergeant at Arms, Visit Authorization Request, https://saa.house.gov/visit-authorization-request.
[28] House Sergeant at Arms, Protocol and Special Events, https://saa.house.gov/protocol-and-special-events.

The division's primary responsibilities include:

- Planning for major House ceremonies, Joint Sessions and official memorial services.
- Coordinating security logistics for visits by Heads of State and dignitaries in partnership with USCP and other law enforcement entities.
- Serving as first point of contact for official business visitors through the HSAA's Appointments Desk system.[29]
- Maintaining protocol standards for official international delegations and serves as principal liaison with diplomatic missions and foreign embassies.

Sergeant at Arms Police Services Division

Police Services Division: The Police Services Division acts as the vital link between House security operations and law enforcement partners at all levels of government, providing specialized training, coordinating protective details, and facilitating unified command during major events. Through its embedded Security Awareness Training program and Law Enforcement Coordination services, the division ensures Members and staff receive current threat briefings while enabling consistent security coverage for official activities.

- Delivers customized security awareness briefings for Washington and district office staff.[30]
- Processes requests for USCP and local law enforcement coverage for Member events in the Washington D.C. Metro Area.[31]
- Facilitates threat assessment briefings and protective intelligence sharing.
- Maintains relationships with federal, state and local law enforcement partners.

House Office of Employee Assistance

The House Office of Employee Assistance (OEA) provides free, timely, and confidential assistance to Members, House employees, and their immediate family members with a variety of personal and work-related issues. OEA is staffed by professionals credentialed in behavioral health-related disciplines and familiar with the unique challenges associated with working in a congressional setting. OEA's free services include individual counseling, comprising comprehensive assessments, supportive counseling, and referral services, as well as adverse stress response services with 24/7 on-call coverage.

[29] House Sergeant at Arms, Appointments Desk, https://saa.house.gov/appointments-desk.
[30] House Sergeant at Arms, Security Awareness Briefing (Washington, DC or District Office), https://saa.house.gov/security-awareness-briefing-washington-dc-or-district-office.
[31] House Sergeant at Arms, U.S. Capitol Police Support in the Washington, DC Metro Area, https://saa.house.gov/u-s-capitol-police-support-washington-dc-metro-area.

Glossary of Terms and Acronyms

Related Security Entities

U.S. Capitol Police (USCP) – The federal law enforcement agency charged with protecting Congress, including Members, staff, visitors, and the Capitol Complex.
U.S. Capitol Police Threat Assessment Section (USCP TAS) – The division of USCP charged with investigating threats against Members and the Capitol.
House Sergeant at Arms (HSAA) – Chief law enforcement and protocol officer of the House of Representatives and is responsible for maintaining order in the House side of the United States Capitol complex.
Sergeant at Arms Emergency Management Division (SAA EMD) – HSAA group tasked with responding to and managing emergencies related to Capitol, Member, or staff security.
Sergeant at Arms Protocol and Special Events - The division of the House Sergeant at Arms responsible for coordinating official ceremonies, managing dignitary visits, and overseeing access procedures for official business visitors to the Capitol complex.
Sergeant at Arms Office of House Security (SAA OHS) - The office within the House Sergeant at Arms responsible for managing security clearances, providing foreign travel alerts and briefings, conducting security sweeps, and maintaining SCIF access for the House community.
Sergeant at Arms Police Services Division - The division that coordinates between House security operations and law enforcement partners, manages security awareness training, and facilitates law enforcement support for Member activities in both DC and district offices.
Chief Administrative Officer (CAO) – The administrative body of the House, responsible for human resources, information resources, cybersecurity, payroll, finance, procurement, and other business services.
Office of Cybersecurity (OCS) – An entity of the CAO responsible for ensuring the cybersecurity of the House network, devices, and IT systems.
Federal Bureau of Investigation (FBI) – The domestic intelligence and security service of the United States and its principal federal law enforcement agency.
Department of Homeland Security (DHS) – Federal executive department responsible for public security.
Law Enforcement Coordination Program (LEC/LECOR) – HSAA program to create and maintain partnerships between Members, district staff, and local enforcement.
District Security Service Center (DSSC) – HSAA office dedicated to providing security resources for district offices, including regional Security Specialists.
Government Services Administration (GSA) – Federal agency dedicated to procuring goods and services for the government; they own and lease space in 9,600 buildings in more than 2,200 communities nationwide.
Office Emergency Coordinator (OEC) – Staff member within an office charged with developing emergency plans, carrying out those plans in case of emergency, and designating tasks for other staff to carry out.
Office Emergency Plan (OEP) – Emergency plan developed by the Office Emergency Coordinator on how the office will respond to all types of emergencies, which includes the responsibilities of each staff member.
Office Continuity of Operations Plan (COOP) – A plan developed within each office that lays out the actions, capabilities, essential staff, and physical resources needed to continue operating when an emergency makes the primary workspace uninhabitable or inaccessible.
Virtual Private Network (VPN) – Encrypted connection over the internet, primarily used to protect sensitive data transmission.

Relevant Terms

Congressional Delegation (CODEL) – An official overseas trip by Members of Congress authorized by the Speaker of the House to conduct legislative activities, oversight, or fact-finding missions abroad.
Staff Delegation (STAFFDEL) - An official overseas trip by congressional staff members, typically to conduct advance work for Member travel or to gather information on behalf of committees or Member offices.
Sensitive Compartmented Information Facility (SCIF) - A specially constructed secure room or structure where classified materials can be securely accessed, discussed, and stored. Access is strictly limited to individuals with appropriate security clearances.

Personally Identifiable Information (PII) – Information that can identify an individual, including but not limited to credit card information, date of birth, driver's license information, financial information, mailing address, medical records, and social security number.
Members Representation Allowance (MRA) – The budget authorized by the Committee on House Administration for each Member of Congress to support official and representation duties in their district.
Mobile Threat Defense Application (MTD) – Preinstalled application on House devices that automatically scans device for cyber threats and vulnerabilities.
Doxing – The act of publicly providing personally identifiable information about an individual or organization, usually via the Internet and without their consent.
Swatting – The act of calling law enforcement authorities with the purpose of luring them to a location with a false claim of an ongoing crime or emergency.
Phishing – A form of social engineering and a scam where attackers deceive people into revealing sensitive information, such as PII or account information, or installing harmful software on to their device.

Security Equipment and Services

Duress Buttons – Devices placed within an office that, when activated, alert the USCP of an ongoing threat.
Wireless Emergency Annunciators – Communication devices that allow the USCP to disseminate information during emergencies. Annunciators are placed throughout the Capitol complex to ensure that all Members and staff can hear announcements, and it is portable.
Escape Hoods – A wearable tool designed to protect Members and staff from respiratory or airborne emergencies, providing the wearer with protection against inhalable particulates, such as chemical or biological weapons.
Mail Hoods – A device to protect against airborne pathogens or hazardous materials mailed to an office, which are provided free of charge to district office staff.
Victim Rescue Units (VRUs) – A self-contained protective breathing device or smoke hood, designed to provide the wearer with oxygen for 60 minutes in the case of a fire or smoke emergency.
Go Kits – A supply kit provided to offices for emergencies, and includes items such as maps, flashlights, blankets, water, a First Aid Kid, and batteries.