


TASK FORCE 1-6
Capitol Security Review

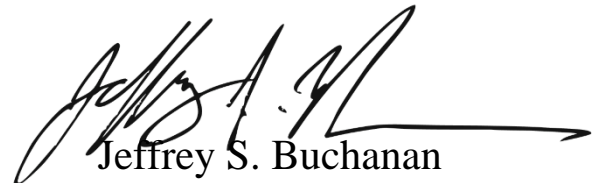


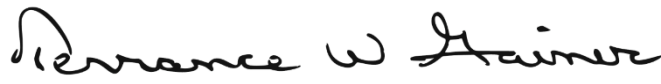
March 5, 2021




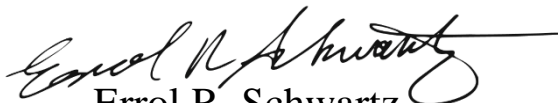
TASK FORCE 1-6 MEMBERS



Russel L. Honoré
LEAD


Jeffrey S. Buchanan
DEPUTY LEAD

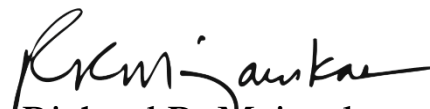

Terrance W. Gainer


Karen H. Gibson

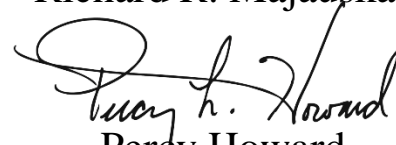

Errol R. Schwartz


Linda L. Singh


Samuel L. Kindred

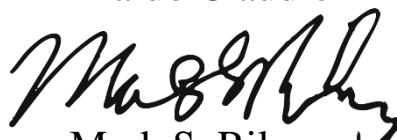

Richard R. Majauskas


Mary B. McCord



Percy Howard


Arnaldo Claudio


Karen F. Lloyd


Mark S. Riley


Steven Rotkoff


Joseph H. Albrecht


John K. Gordon



Task Force 1-6 Assessment

At the direction of the Speaker of the House, Lieutenant General Russel L. Honoré, USA (Retired) led an immediate forward-looking, non-partisan, six-week review for the purpose of identifying actions or decisions that could be taken immediately or in the near-term to improve the security of the Capitol, Members, and staff. To complete this review, a team of experienced professionals with law enforcement, legal, personal protection, intelligence, operational, and Congressional experience was assembled, hereafter referred to as Task Force 1-6. Specifically, the Task Force was directed to review and provide recommendations in the following areas: Capitol security operations, infrastructure physical security, and Member security in their Congressional districts, their residences, and during travel.* All findings were passed to the House Sergeant at Arms.

Given the immediacy of the review, the members of the Task Force met with the leadership, staff and members of the U.S. Capitol Police (USCP); the House and Senate Sergeants at Arms; the Architect of the Capitol (AOC); the Mayor of the District of Columbia; the Metropolitan Police Department (MPD); the Metropolitan Washington Council of Governments (MWCOG); numerous Federal Law Enforcement Partners (FBI, DHS, FPS); the Departments of Defense and the Army; the Pentagon Force Protection Agency; and the National Guard Bureau and relevant subordinate commands, such as the D.C. National Guard. The Task Force also met with Congressional Members and staff, both as individuals and as Congressional committee leaders for both the Senate and House.

*Although the facts and circumstances that led to the events of January 6 remain under investigation by others, we make our recommendations based on what we were able to learn and observe within the compressed timeframe of our review.

While the review focused on the House side of the Capitol, many of the security recommendations necessarily have broader applicability. There are several institutional challenges unique to securing the Capitol. Most evident is the inherent tension between public access and physical security. Any security measure that reduces physical access to the Capitol Complex makes it less accessible to the public it serves. As representatives of the people, Members understandably seek to be available to their constituents and transparent about their travel and activities, yet such openness can create physical security vulnerabilities. As such, a bicameral approach to security improvements is essential to reducing vulnerabilities and safeguarding Members in the Capitol and in their Districts. This may require Members to overcome institutional reluctance to appropriate tax dollars to fund necessary security improvements in support of the legislative branch. The Task Force recognizes that implementation of its recommendations will ultimately be shaped by political, budgetary, and other considerations.

OPERATIONAL REVIEW

Intelligence

Intelligence Focus. Threats against the Capitol and Members have shifted dramatically, both in volume and nature. Today's threats are not only more numerous but increasingly come from domestic elements. Individuals and groups advocating extremist views actively use the internet to propagandize, recruit, radicalize, and organize political violence such as the Capitol Attack. Some also target Members with threats of violence. The USCP is not postured to track, assess, plan against, or respond to this plethora of threats due to significant capacity shortfalls, inadequate training, immature processes, and an operating culture that is not intelligence-driven.

Intelligence Capacity. Only a handful of people in the USCP have significant intelligence training. The understaffed Intelligence and Interagency Coordination Division (IICD) lacks the experience, knowledge, and processes to provide intelligence support against emerging domestic threats. It urgently requires a modest increase of trained analysts to support USCP threat intelligence requirements. This larger team must standardize its intelligence processes and will require regular professionalization training, modern analytic tools, secure workstations, and classified workspace to function capably.

Intelligence Awareness, Assessment, and Sharing. Decades of experience with foreign terror threats prove that success comes through close collaboration across the intelligence and law enforcement communities to obtain early warning and gain collective understanding. The USCP has liaison officers at the Joint Terrorism Task Force and elsewhere, but very few are trained intelligence analysts. The IICD must sustain routine, analyst-level interaction with organizations that look at similar threats in the NCR or to Congressional Members and staff. The USCP would also be well served by placing intelligence specialists in the Washington Joint Terrorism Task Force and accepting augmentation or liaison officers from the NCR Threat Identification Center.

Intelligence – Operations Integration. Threat identification and understanding is not the sole responsibility of the intelligence staff. Leaders across the USCP have a responsibility to demand that the intelligence team look beyond imminent events to confirm or deny developing threats and to inform operational training and preparation across the USCP. Command Center staffing should include an IICD representative and threat briefings to the broader team should be a daily routine. USCP leadership must actively integrate intelligence functions into the USCP's daily operations, force protection decisions, and future planning. This will require additional intelligence research specialists and supervisory analysts, training on analytic methodologies and software tools, and the procurement of equipment to accommodate a more robust team. Just as critically, however, this will require a dramatic, consistent, leader-driven shift in the USCP's cultural mindset toward threat-based operations and decision-making.

Capitol Police Board Decision-making During Emergencies

The Capitol Police Board's (CPB) deliberate decision-making process proved too slow and cumbersome to respond to the crisis in January, delaying requests for critical supplemental resources. We recommend revisions to 2 U.S. Code §§ 1970 and 1974 to give the USCP Chief the authority to request external law enforcement and National Guard support without CPB preapproval in extraordinary emergency circumstances, when necessary to prevent the loss of life or wanton destruction of property and to restore governmental functions and public order. Moreover, when conducting crucial advance planning for mass demonstrations and NSSEs, the USCP Chief should have an avenue to appeal denial of requests for support or inaction by the CPB on such requests to House and Senate leadership. We also recommend an independent

review of the necessity for, and command and control effectiveness of, the Capitol Police Board's authority over the USCP.

Dedicated Quick Reaction Force to the District of Columbia

Our national capital is a prominent tourist destination, venue for many peaceful First Amendment activities, and a high-value target for foreign terrorists or domestic extremists, yet it has no dedicated QRF for response to crises. The USCP relies on augmentation from other civilian law enforcement agencies for emergency support, but we recommend establishment of a robust, dedicated QRF, not only for the USCP, but to serve the nation's capital writ large. Mobilized National Guard forces currently supplement the USCP, which is temporarily sufficient but not a permanent solution. We propose three long-term options for consideration, all of which involve the Executive Branch. The first would be to establish a QRF from existing federal law enforcement entities with appropriate legal authorities and appropriations to staff, train and equip such a force. The second would be to build a QRF under the command of the D.C. National Guard. This could be done by mobilizing military police from Guard elements across the U.S. on rotations of three to six months. Another option would be to create a QRF that permanently resides within the D.C. Guard by reestablishing a military police battalion and staffing it with Active Guard Reserve troops who live in or near the city year-round, perpetually on active duty.

The U.S. Capitol Police

USCP Force Structure. The USCP were understaffed, insufficiently equipped, and inadequately trained to secure the Capitol and Members when violently attacked by a large mob. To remedy personnel shortfalls, the Task Force recommends several changes. First, the USCP should hire sufficient officers to fill all current vacancies; this is now 233 officers. The Task Force identified several specific areas for additional capacity, as detailed throughout the report. Due to a lack of available personnel and increasing demands, the USCP has employed a vast amount of overtime to meet mission requirements (nearly 720,000 overtime hours in Fiscal Year (FY) 2020 and over 55 percent of enacted overtime in just the first five months of FY 2021). Not only is this model unsustainable, it leaves the force with no ability to pull officers from the line to train at the individual, leader, or collective level or to prepare for evolving threats. As such, the Task Force recommends the USCP receive an additional 350 authorizations to reduce

overtime costs and adequately fulfill its assigned missions. We further recommend the USCP receive 424 additional authorizations to fill assessed capability gaps, which includes intelligence specialists, operational planners, supervisors, Civil Disturbance Unit (CDU) personnel and trainers, and dignitary protection agents, to name just a few. This results in a total “plus-up” of 854 authorizations to the USCP. These personnel increases will require adequate appropriations to meet USCP recruiting objectives and initial training and onboarding requirements. The Task Force recommends consideration of alternative recruitment methods such as inclusion of lateral hiring practices to achieve recruiting goals.

USCP Force Training and Leader Development. The USCP has a sound system for training new officers so they are fully qualified before assuming their duties. Once they enter the force, however, the officer utilization rate is so high that they cannot step out of their operational roles for follow-on or refresher training. Addressing manpower issues should resolve this problem, but the USCP should also reexamine and upgrade its training curricula to incorporate the most modern police tactics. There are even greater shortcomings when it comes to collective training, i.e. training together as teams. Collective training is imperative for elements that operate as units, like CDUs or Quick Reaction Forces (QRF), but there is tremendous value in collective training for the rest of the force as well. Prior to NSSEs, leaders from security elements across the NCR come together to prepare as a group and conduct table-top rehearsals. USCP leadership participate in these collective training events but must follow up with similar rehearsals with the rest of the USCP. We recommend the USCP plan and execute a collective training event every quarter against a different contingency situation, wrapping in members of the CPB and interagency partners to ensure collective readiness in a crisis.

The USCP usually selects leaders from its own ranks but offers little in the way of leader development training after promotion to supervisor. Leader development is especially critical in organizations that may operate in crisis situations or are charged with saving lives. Well-prepared leaders can operate with agility and confidence in complex situations, making sound decisions under pressure. An active training and progressive leader development program and schooling to include a transition course from Private First Class to Sergeant will enhance every USCP leader’s ability to perform in a crisis. The USCP must also institute a deliberate program of After-Action Reviews following every significant operational event or training exercise in

order to leverage organizational and individual experience while it is fresh to maximize learning, address deficiencies, and sustain excellence.

USCP Implementation of the National Incident Management System. On January 6th, the USCP were challenged to effectively incorporate reinforcing elements from external units. We recommend they develop and practice standardized procedures for employing outside law enforcement in accordance with the National Incident Management System's Incident Command System. Such practices include operating a staging area for receipt of supplemental forces, administrative onboarding, assignment of tasks, and initial deployment of supporting personnel. These processes are essential for providing the Incident Commander with an awareness of arriving assets, their numbers and capabilities, specialized equipment, specifically trained personnel, and other vital information. They also provide a means to rapidly brief new arrivals on the situation and establish communications within the radio network. Without such processes, integration is less effective and is not driven by an overarching operational command.

USCP Operations and Equipment Requirements. Internal communications were a problem during the attack in part because the USCP failed to use "talk groups" on the radio, which would have allowed leaders to bypass the constant, high-volume tactical chatter to communicate without the interruption of other radio traffic. The USCP must take full advantage of its highly capable radio system to prevent confusion and establish clear command and control. Without earpieces, many officers were also unable to hear or understand radio communications due to overwhelming noise from the crowd. Every officer must be equipped with earpieces as part of his or her uniform and directed to wear them. This should not be optional. We also recommend the USCP be equipped with Body-Worn Cameras (BWC), an item not currently in their inventory, to improve police accountability and protect officers from false accusations of misconduct. BWC also provide visual and audio evidence that can independently verify what happened in any given situation, leading to better investigations and prosecutions when needed.

USCP Force Capability Enhancements

Civil Defense Units (CDU). CDUs are specially trained and can be activated and assembled to monitor and respond to illegal activities that present themselves during First Amendment assemblies, mass demonstrations, or civil unrest. USCP CDU are currently only available when planned for in advance, limiting the USCP's ability to react immediately to spontaneous threatening events. We recommend the USCP maintain dedicated CDU platoons on duty any time Congress is in session. Additionally, all USCP Uniformed Services Bureau officers should receive basic civil disturbance training and be issued essential riot gear, including less-lethal equipment, for situations in which additional manpower is needed to back up CDU platoons.

Explosive Detection Dog (EDD). EDD teams play a key role in providing comprehensive security. With an ability to detect explosive odors down to parts-per-trillion, their utility in providing a first line of defense cannot be overemphasized. Unfortunately, the USCP K9 unit is challenged to meet increasing operational requirements due to unfilled positions, non-mission capable teams, and aging dogs. Besides filling existing vacancies, the USCP should consider increasing the size of the EDD force so they may also be employed more broadly. The USCP should recruit and hire additional EDD handlers, equip them with civil disturbance equipment, and procure additional K9s where vacancies and K9 retirements are needed.

USCP Mounted Unit. The USCP should also consider reestablishing a mounted unit, recognized elsewhere as providing a less lethal law enforcement force multiplier. Best used in high pedestrian and dense crowd areas, a well-trained horse and rider can assist in controlling crowds or quelling disturbances with few serious injuries to demonstrators. They increase mobility, allowing officers to reach a scene more efficiently than on foot or in a vehicle. A rider's elevated position allows them to better assess a crowd and its actions, eliminate or curtail face-to-face confrontations, and provide a calming effect on a crowd in tense situations. Police horses can also serve as "moving walls" capable of shifting large crowds or separating antagonistic groups. Mounted units have been reestablished in other jurisdictions such as Tampa, Chicago, and Atlanta due to their operational effectiveness. The USCP's former Mounted Unit, disbanded in 2005, was prepared to provide immediate emergency response,

assist in searches for lost or wanted persons, assist in crowd management, and perform in ceremonial details.

National Capitol Region Integrated Security Plan

There is no overarching integrated security plan for the NCR, which consists of the District of Columbia and six counties in Maryland and Virginia. Some law enforcement elements, like the U.S. Park Police and USCP, have geographic jurisdictions. Others, such as the U.S. Secret Service, are functional. Reporting chains are even more complex, with various entities reporting to different governors, the D.C. mayor, or federal agencies. Cooperation is built on mutual aid agreements through the MWCOG, which works well for fire, emergency services, and NSSEs, but daily or emergency coordination can be challenging. We recommend a federal agency such as DHS lead a collaborative effort inclusive of the CPB and designees from the Office of the Governor for the states of Maryland and Virginia, and the Mayor of the District of Columbia. The collective planning effort would be key to developing a shared understanding for any response effort and better enable unity of effort. This plan should be exercised quarterly through table-top exercises and reinforced in daily operations.

Clarification of DoD Directive 3025.18 Concerning the Commander, D.C. National Guard

Procedures that delay requests for and approval of USCP augmentation by law enforcement and military personnel should be modified to facilitate a rapid response in extremis. DoD Directives are one area where clarity could be improved. We recommend DoD Directives be amended to make clear that, notwithstanding any restrictions on employment of the D.C. National Guard in non-emergency situations, the Commanding General of the DC National Guard shall retain “emergency authority” as defined in DoD Directive 3025.18 “in extraordinary emergency circumstances where prior authorization by the President is impossible and duly constituted local authorities are unable to control the situation, to engage temporarily in activities that are necessary to quell large-scale, unexpected civil disturbances” when necessary “to prevent significant loss of life or wanton destruction of property and are necessary to restore governmental function and proper order.”

PHYSICAL INFRASTRUCTURE

The Task Force recommendations listed hereafter require immediate action and appropriations where appropriate to enable the AOC or the USCP to initiate contracting actions and begin work on much-needed security improvements as soon as possible.

Capitol Fencing and Infrastructure Improvements

In securing the Capitol grounds, competing desires for maximum public access and guaranteed security create a situation where neither goal is achieved. No fence presents an insurmountable barrier. Obstacles do not prevent penetration by themselves, but serve to slow or canalize intruders, allowing security forces to focus a response to specific sites as necessary. For full effectiveness, obstacles also require unblinking observation from human eyes, cameras, or other sensors. The current, temporary security fence surrounds such a tremendous area that it requires significant personnel resources to monitor its entire length. As the fencing comes down, we recommend it be replaced with a mobile fencing option that is easily erected and deconstructed and an integrated, retractable fencing system in the long term to secure both the Capitol Building and Congressional office buildings. Such a solution could enable an open campus while giving security forces better options to protect the complex and its Members should a threat develop.

Due to previous piecemeal or incremental modernization efforts, many facets of the Capitol's physical security infrastructure are neither interoperable nor integrated. For instance, there are numerous cameras in the Capitol Complex, but they are not entirely integrated or linked. The Capitol Complex needs a fully integrated system of obstacles, cameras, sensors, and alarms and we recommend the USCP in collaboration with the AOC contract with the U.S. Army Corps of Engineers' Electronic Security System Mandatory Center of Expertise to help develop and build such an integrated system.

Mobility Within the Capitol During Emergencies

The evacuation of the Capitol was an extraordinary event in which USCP and U.S. Secret Service leveraged accessible, unimpeded routes to move Members and staff to safety. Such evacuations should be adequately rehearsed. Appropriate improvements to infrastructure and the procurement of relevant technologies should be expedited to enable wayfinding during

emergencies, as outlined in our report. Lastly, the AOC should install means to selectively compartmentalize areas of the Capitol Complex, also detailed in our report.

Capitol Complex Screening Procedures, Tools, and Infrastructure

Background Checks. The Capitol Complex must review its screening procedures and its use and application of background checks for identification card holders, and must expand employment of modern tools throughout the complex to enhance the safety of all Members, staff, and legislative employees. Requiring background checks for identification card holders and employing card readers more widely throughout the complex would decrease insider threat risks and enhance the safety of all Members, staff, and legislative employees.

Screening Portals and Access Points. Screening portals for visitors and staff should provide guards sufficient time to observe approaching individuals at a distance and provide sufficient space for processing workers and visitors. The AOC is procuring screening vestibules for the Capitol's south and north entrances that will more appropriately serve the building's needs. This work should be expedited and expanded to other buildings where needed. The Architect should also expedite repair and hardening of vulnerable windows and doors, prioritizing this work based on assessed vulnerabilities.

House Information Technology Systems and Cybersecurity

Although the House has centralized portions of information technology management (IT), the current oversight model results in a decentralized cybersecurity strategy that could lead to gaps in security and privacy throughout the organization. Centralizing IT authority would ensure best practices are utilized to minimize cybersecurity risk and provide comprehensive oversight of IT systems, administrators, and processes.

USCP Command Center and Infrastructure Requirements

The USCP headquarters and Command Center facilities are subpar and require substantial renovation or replacement to accommodate adequate primary and alternate command, control, and coordination functions, and provide sufficient secure office space and resources to support

officer training, equipment storage, and daily work. The Task Force also recommends improvements to address continuity of operations considerations.

MEMBER SECURITY WHILE TRAVELING AND IN THEIR DISTRICTS

Member Security During Travel

Dignitary Protection Services. The Member threat environment is not confined to the Capitol Complex. Although the USCP's Dignitary Protection Division (DPD) provides adequate security to House leadership, other Members, faced with varying threat levels, have limited or inconsistent protection at their homes, in their districts, and while in transit. When the threat warrants, the DPD assigns a dignitary protection team to a Member for a period, but this process is not standardized or evenly applied. The DPD should develop a threat-based protection model that can be consistently applied to non-leadership, allocating protection resources based on an evaluation of risk to Members and their families. With communicated threats against Members tracking at nearly four times last year's level, the DPD should also increase in size to viably handle growing demand for Member security. Admittedly, not every threat is credible, but every threat warrants attention and must be taken seriously. Upon investigation, some percentage of threats will shape a change in travel plans or warrant extra security precautions.

Member Security Systems and Tools. Member travel security is not handled efficiently. The process is largely manual, labor intensive, and fails to fully leverage federal, state, and local partnerships along the transit route, in the home district, and near the Member's residence. The Task Force recommends the House Sergeant at Arms establish a modestly staffed, technology-enabled Member Travel Operations Center (MTOC) to centrally manage Members' travel security needs. A regional focus within the MTOC and close collaboration with the House Sergeant at Arms District Service Centers would facilitate consistent relationships between Members' offices, MTOC facilitators, and the supporting state and local law enforcement communities.

Member Security in their Congressional Districts and Residences.

Security is also inconsistent across the approximately 900 Congressional district offices. The HSAA contracts security systems for many of these offices, but should establish a plan to cover

all of them through the same process. Installing and monitoring security systems for 100-percent coverage will require additional funds. Members presently use personal resources and campaign funds to procure security systems for their homes. Members' home security needs and their ability to finance security requirements vary considerably. We recommend Congress appropriate sufficient funds to the HSAA to manage a Member allowance for installation and monitoring of a standard residential security system.

Conclusion

The breach of the U.S. Capitol on January 6 brought into stark relief the need to immediately improve the security of the Capitol Complex and the security of Congressional Members and staff. Immediate action is therefore required:

- The Congress must immediately fund infrastructure contracts managed by the Architect of the Capitol to repair or replace doors and windows, authorize mobile fencing design and procurement, and authorize U.S. Army Corps of Engineers' assessment of long-term improvements to perimeter fencing and security surveillance and sensing systems.
- The Congress and the Capitol Police Board must immediately amend relevant statutory and internal Board policies to better enable crisis decision-making and empower the USCP Chief to initiate timely augmentation in emergencies.
- The Capitol Police Board must immediately approve the U.S. Capitol Police Chief's outstanding request for security augmentation from the National Guard.
- The Congress must direct the USCP to take immediate action to eliminate personnel shortfalls, currently 233 officers, through enhanced recruiting and incentive programs.
- The Congress must immediately authorize a USCP force structure increase and appropriate sufficient funding to hire the additional 350 officers needed to buy-down the long-standing and well-documented overtime problem within the USCP.
- The USCP must immediately:
 - Improve intelligence integration, develop daily intelligence summaries, and disseminate relevant and needed intelligence to front-line leaders.
 - Conduct necessary individual training and leader development, rehearsals, and After-Action Reviews.

- Participate in the MWCOG Police Chiefs Group and approve appropriate Mutual Aid Agreements.
- Implement the National Incident Management System and rehearse the Incident Command System.
- The Congress must immediately authorize appropriations to enable the Sergeants at Arms to procure security systems for all Member district offices and residences; this includes appropriations for design and procurement of technologies and software applications to improve coordination for Member security needs.

In the coming days, against the backdrop of inquiry and investigation, Congress will engage in spirited debate over the Capitol's current security arrangements and the change necessary to better secure the Capitol and safeguard its Members, staff, and employees. As you consider the recommendations of this Task Force, we must not forget it was the riotous actions of an angry mob that laid bare the vulnerabilities of the Capitol Complex. We must not long endure any discourse that prevents or delays efforts necessary to strengthen the security of the U.S. Capitol Complex and enhance the safety of those who serve the American people in Congress.