



Highlights

[U.S. Capitol Security](#)

[D.C. Mayor Bowser- Authority and Limitations](#)

[Identifying Rioters Using Social Media \(and Admissions\)](#)

[A Straight-Up, Non-Exhaustive List of Security Breaches at the U.S. Capitol on January 6, 2021](#)

[FBI Offers \\$50k Reward for Info Regarding Pipe Bomb Found in D.C.](#)

[G2M Research Multi-Vendor Webinar Series – 2021 Schedule](#)

Our AI & Cybersecurity Newsletter covers topics such as ransomware attacks, exploits, security issues facing major companies such as Zoom, and security breaches such as the Solarwinds attacks on Nuclear Labs, the U.S. Treasury, and Pentagon. The common thread in all of these attacks is that they occur in the dark, so to speak. The malicious actors are identified after the fact, and often remain unknown. The hackers take data, disrupt services, and exploits, such as ransomware attacks on hospitals, cause us to ponder the very real risk of loss of life in the event of an attack on power grids or computer management systems integral to infrastructure.

The January 6 riot was the first time the U.S. Capitol was overrun by a hostile force since [1814](#) when the British set the White House and Capitol building on fire. In this case of the January 6 breach of U.S. Capitol security, all events occurred in the open, with many actors self-identified via social media posts and livestreams. Five people died as a consequence of the several hour

takeover of the building, including a Capitol Police officer, [Brian Sicknick](#), who was struck by a rioter in the head with a fire extinguisher. At least [56 officers](#) were injured defending the Capitol.

Congress was in session at the time of the security breach. Legislators and staff were evacuated to secure locations. A group of rioters chanted "[Hang Mike Pence](#)" as they walked through the Capital. Others [ransacked](#) Speaker Nancy Pelosi's office and accessed her emails on a desktop computer. Senator Jeff Merkley reported his [laptop](#) was stolen. The Chief Administrative Officer's Office of Cybersecurity reportedly took [actions to secure](#) and protect sensitive information during the siege.

It is unclear what documents were removed from offices. Michael Sherwin, the acting U.S. attorney for Washington, D.C., [said](#) it will likely take "several days to flesh out exactly what happened, what was stolen, what wasn't," noting that "items, electronic items were stolen from senators' offices, documents and materials were stolen, and we have to identify what was done to mitigate that [damage]."

This newsletter examines a few of the security issues related to the events of January 6.

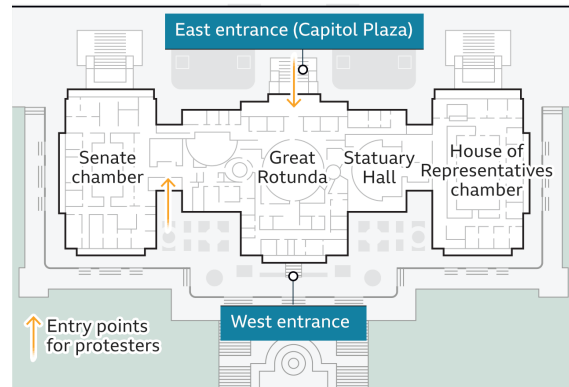
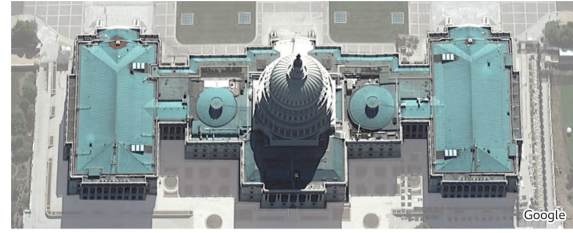
U.S. Capitol Security



The [United States Capitol Police \(USCP\)](#) includes 2,300 officers and civilian employees and has an annual budget of approximately \$460 million. The U.S. Capital has a floor area of [16.5 acres](#), five floors, and hosts 3-5M visitors per year (though tours are canceled due to the pandemic). More than 30k employees work in the 19 capitol buildings.

The USCP protects both the Senate and House, but each has its own [Sergeant at Arms](#) who oversees security. Because of that separation, there are situations where there could be a lockdown just for one or for both. Historically, Congress has treated its role as open and maintained that approach in availing its members to the public. However, over time, in response to threats and attacks, security measures have been added to secure the safety of members and constituents.

The [responsibility](#) of preparing for emergencies and disasters impacting the U.S. Capitol is shared by the Sergeant at Arms of the House and Senate, the Architect of the Capitol, the Chief Administrative Officer of the House, the Attending Physician, and the Chief of the United State Capitol Police. Each Congressional office has the responsibility of creating multiple plans, depending on the type of attack, to protect their staff and visiting constituents. The USCP serve the principal role during any partial or complete evacuation of any Capitol building.



In 1801, [John Golding](#) was appointed the first guard for the Capitol, during its construction, however; his role was really that of groundskeeper. In 1827, several incidents occurred that could have been prevented with sufficient security and surveillance. President John Quincy Adams asked that a regular Capitol Police force be established resulting in the creation of the United States Capitol Police by [Congressional Act](#) the following year.

With the passage of this Act, Congress brought the responsibility of policing the Capitol under the direction of the presiding officer of the House and Senate. Their area of authority did not exceed the neighboring walks and streets adjacent to the Capitol Building. In [1867](#) the responsibility of the Capitol Police was transferred from the Commissioner of Public Buildings to the Sergeants at Arms for the U.S. House of Representatives and the U.S. Senate. In [1873](#), the Capitol Police Board was established. By [1935](#), the Capitol Grounds footprint was expanded to 126 acres and the force was expanded.

Incidents of violence directed towards Members at the Capitol or the building itself include bombings such as in 1915 when [Erich Muentzer](#) planted dynamite near the Senate to protest our World War I policies. In 1971, [Weather Underground](#) detonated a bomb to protest the invasion of Laos resulting in the placement of metal detectors at the door and staff ID cards. In 1983, the [Resistance Conspiracy](#) planted a bomb in response to American military activities in Grenada and Lebanon. Additional security precautions were added, including closing the lobby outside the Senate Chamber. [The Containment and Emergency Response Team \(CERT\)](#) was created to handle dangers to the Capitol, like terrorism, or more peaceful events that require a high degree of security, like Presidential visits.

In [1954](#), four men shot and injured five U.S. Representatives. In [1998](#), a lone gunman killed two Capital Police officers, Jacob Chestnut and John Gibson. It was the first shooting in which any Capitol Police officer was killed while on duty. The shooting prompted government officials to review [security measures](#) for Federal buildings. Additional police officers were assigned to the entrances of the Capitol and to congressional leaders. The [Capital Visitors Center \(CVC\)](#) opened in [2008](#) and has security checkpoints to manage the flow of guests around the building.

The [attacks of September 11, 2001](#) resulted in permanent changes to security protocols. New measures were put in place to standardize protocol in the event of a large-scale evacuation. Over 200 additional police officers were hired. Streets were closed and trucks, cars, and even bicycles were rerouted in different areas around the complex. That same year, [anthrax spores](#) were mailed to congressional offices, leading to a number of new [security measures](#) to combat the threat of a biological attack. Mail for Congress was sent to offsite facilities for screening. The [D.C. National Guard](#) assisted in protecting the Capitol for several months.

Under normal circumstances, staff and visitors to Congress or the congressional office buildings go through at least one security checkpoint, perhaps two, if they are heading to the U.S. Capitol itself. The Capitol Visitor Center [website](#) lists items that tourists are [prohibited](#) from bring to the building, and there are additional restrictions for the Capitol itself.

D.C. Mayor Bowser – Authority and Limitations



Washington, D.C. is [unique](#) in that the mayor has some of the responsibilities generally allocated to governors, county executives and mayors of other states, such as overseeing public schools and running Medicaid, but does not have the full authority those positions typically have, such as the ability to deploy the National Guard. D.C. National Guard deployments must be [approved](#) by Secretary of the Army Ryan McCarthy, which is a slower process than having the governor declare the emergency and deploy the Guard directly.

[D.C. Homeland Security and Emergency Management Agency \(HSEMA\)](#) is responsible for ensuring the District of Columbia is prepared for all threats and hazards and serves the 700k residents in D.C.

[Mayor Muriel E. Bowser](#) safety initiatives around the City include installation of 1200 security cameras, providing officers with 1200 body-worn cameras, additional training and recruitment of law enforcement agents, and a [private security camera initiative program](#) for D.C. residents and businesses. Over 20k cameras have been funded through the initiative program.

The District of Columbia has [some of the most restrictive gun laws](#) in the U.S. All firearms [must be registered with the Washington D.C. Metropolitan Police](#). Registrants may be either residents or non-residents, must be 21 years of age, and not have disqualifying events on their records such a felony convictions, previous weapons offenses, or a variety of other conditions. Individuals may not possess ammunition unless they have a registered firearm.

Of particular note is the prohibition against “open carry” (carrying a non-concealed weapon in public areas). This extends to transportation of firearms within Washington D.C. as well, unless the person is going from one state to another if the firearm is licensed in both states, carried in the vehicle trunk in a locked case, and the person is not intending to stop in Washington D.C. [Concealed carry](#) of a pistol is allowed if the person has a concealed carry pistol license (CCPL) issued by the Metropolitan police (only 4,600 permits have been issued in D.C., which has a population of roughly 721,000 people), and there is no reciprocity agreements on CCPLs with any other jurisdictions and the District of Columbia. Additionally, many areas are off-limits for concealed carry even if the individual has a CCPL, including the National Mall and government buildings. Assault rifles and .50 caliber weapons chambering the Browning Machine Gun (BMG) are illegal in Washington D.C.

The [penalty for carrying a pistol](#) outside of one’s home without a CCPL (even a registered one) is a maximum of five years in prison and/or a fine of \$12,500. Possession of a firearm not registered in the District of Columbia adds one year in jail and/or a fine of \$2,500 to the above. If the weapon is in a person’s possession in a gun-free zone, such as the U.S. Capital, these penalties are doubled.

The National Park Service received [three separate applications](#) for pro-Trump rallies on Tuesday or Wednesday, with estimated maximum attendance at around 15,000 people.

Monday, January 4, [Enrique Tarrío](#), chairman of the Proud Boys, was [arrested](#) in Washington D.C. on a warrant for burning a Black Lives Matter banner taken from a historic church during a demonstration in December. He was also charged with possession of high-capacity ammunition feeding devices found during the arrest. Tarrío was released from jail on January 5 and banned

from Washington D.C. except for trial or meeting with his lawyers. Tarrío had planned to attend the rally on January 6 and posted on social media that the Proud Boys [would attend](#) in record numbers.

Downtown D.C. businesses [boarded up](#) their windows in anticipation of the rallies. Mayor Bowser [asked](#) that local area residents stay away from downtown D.C., and avoid confrontations with anyone who is “looking for a fight” and warned, “We will not allow people to incite violence, intimidate our residents or cause destruction in our city.” D.C. police [posted signs](#) throughout downtown warning that carrying any sort of firearm is illegal and asked area residents to warn authorities of anyone who might be armed.

[According to a U.S. defense official](#), Mayor Bowser put in a request on December 31 for a limited National Guard deployment on the streets from Tuesday, January 5 to Thursday, January 7, to support the Metropolitan Police Department during the scheduled rallies. 340 D.C. National Guard members were activated, with plans for around 115 guards to be on duty at any time and used for traffic and crowd control, unarmed and not wearing body armor. The defense official said that there would be no active duty military troops in the city and no D.C. Guard members on the National Mall or at the U.S. Capitol. According to [one AP article](#), the Pentagon asked Capitol Police on January 3 whether they would need additional National Guard support, and the Capitol Police declined.

President Trump [spoke](#) to supporters at the scheduled rally a couple of hours before Congress was scheduled to confirm the election results. His early remarks include, “We’re gathered together in the heart of our nation’s Capitol for one reason, to save our democracy.” He goes on to talk about theft of the election and says that after he finishes speaking “We’re going to walk down to the Capitol..” He continues to speak for over an hour and concludes, in part, by saying “We fight like Hell and if you don’t fight like Hell, you’re not going to have a country anymore.” As Congress convened, [a group of supporters](#), armed and angry, walked to the Capitol and chaos ensued. These rioters stormed the entrances to the Capitol, climbed walled, broke windows, and took over the U.S. Capitol for over four hours.

Rioters were able to enter the building with firearms. Many of the rioters were identified as the same individuals who entered the [Michigan State Capital on April 30, 2020](#), where it is legal to openly carry firearms. Many national security experts now believe that April 30 protests in Michigan were a [“dry run”](#) for the siege at the U.S. Capitol.

When the siege of the Capitol began, Mayor Muriel Bowser requested full deployment of the National Guard and assistance from the governors of [Virginia](#) and [Maryland](#) under EMAC. The Department of Defense said it took [30 minutes](#) to secure approval while others stated that approval took over [two hours](#).

Maryland Governor Larry Hogan [comments](#) regarding efforts to mobilize National Guard:

"We immediately offered support to the District of Columbia, which submitted a direct request for law enforcement support through the emergency management assistance compact," Hogan said, authorizing 200 Maryland State Troopers and the state's National Guard unit to be sent to D.C.

"I was ready, willing and able to immediately deploy [National Guard] to the Capitol, however we were repeatedly denied approval to do so."

Hogan received a phone call from House Major Leader Steny Hoyer, who Hogan said was calling from an "undisclosed bunker" where he, Speaker Pelosi and Senator Schumer had been taken during the evacuation. "The U.S. Capitol Police was overwhelmed, that there was no federal law enforcement presence and that the leaders of Congress were pleading with me, as the Governor of Maryland, for assistance from Maryland's National Guard and State Police."

President Trump [initially](#) "rebuffed and resisted requests to mobilize the National Guard." Department of Defense officials, however, say they were "merely being cautious about military involvement in election-related activities." Under Executive Order 11485, the Defense Department may approve a mayoral request for DCNG deployment "[s]ubject to the direction of the President as Commander-in-Chief." Defense officials ultimately approved the request after consultation with Vice President Mike Pence. Mayor Bowser issued an [order](#) extending her public emergency declaration to 15 days.

Identifying Rioters Using Social Media (and Admissions)

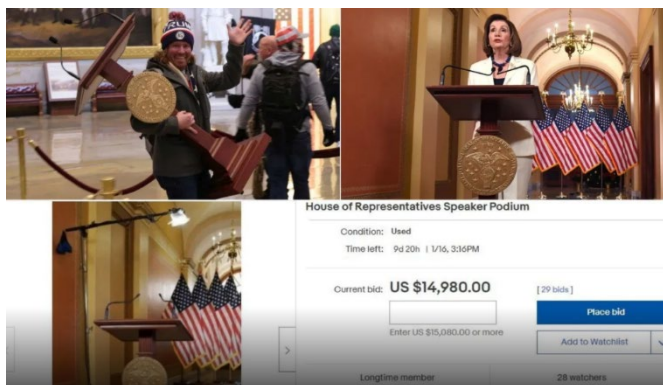


The ability to identify people is hampered, at least to some degree, with people wearing masks out in public to avoid contracting COVID-19. However, most of the people who stormed the US Capital on Wednesday were not wearing masks. And, in fact, many of the rioters posted [selfies](#)

during the hours they occupied the Capital. Some made phone calls to friends to announce they had successfully gained access and others livestreamed the attack, providing a play by play of their actions. Some spoke to the press, providing their names and home cities. Many posted their intent to go to the Capital on social media prior to January 6 and followed up with photos taken during the rally, inside the capital, and throughout the maylay. Many posted their intent to [kill](#), including killing police officers.



Media equipment was [destroyed](#), all while filmed by other rioters. A rioter [urinated](#) on the floor inside the Capitol and others smeared [excrement](#). One person was easily identified by his [work badge](#) hanging around his neck and was promptly terminated by his employer for cause. Fortunately, [staffers](#) had the presence of mind to secure the electoral votes. One protestor was identified, via social media, by his proud father, announcing [“THAT’S MY SON“](#), followed up with a post stating that the FBI had contacted him, then the account went offline.



Items were stolen, such as a [podium](#), which was promptly listed for sale on ebay, providing a second means of identifying the criminal.

Facial recognition software is often used by law enforcement to attempt to identify participants in criminal activity, but those efforts may be hampered by limited

surveillance, limited photo vantages, clothing intentionally obscuring the person's identity, and, inaccuracies in the software itself – in some cases, as we have written about previously, misidentifying the intended target. However, when the persons of interest self identify via social media platforms, tracking them, even across several state lines, becomes rather elementary.

[Elizabeth](#), who was maced in the face while trying to access the Capitol building, expresses her dissatisfaction with “the revolution.”



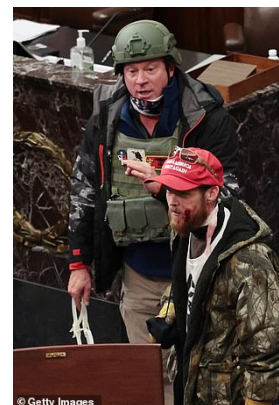
A Straight-Up, Non-Exhaustive List of Security Breaches at the U.S. Capitol on January 6, 2021

Access to the Building – Rioters gained access to the building by force directly through entrances, using scaffolding to hoist themselves up a floor or two in order to break windows, scaling the building by turning metal barriers on their side and climbing them like ladders, and climbing walls without assistance.

Lack of Firewalls inside the Building; Secure Access Points – Rioters gained access all over the Capitol building including the Chambers and Member offices, created an opportunity to plant listening devices, bombs, damage sensitive documents, read/access sensitive documents



Ability to Bring Anything Inside – Items brought into the building included guns, weapons, tools, backpacks, cellphones, video cameras, zip ties, cigarettes and lighters. There was an opportunity to bring in anything inside, creating enhanced security risks including risk of fire. Social media posts referenced the desire to take hostages.



Ability to Take Anything Outside – Rioters stole a laptop and podium. They made recordings while in the building which may include sensitive information. They had the ability to take photos of all items in Member offices. Rioters has the opportunity to take documents, laptops, access computers in offices including email.

Communications – Throughout the siege, rioters had the ability to communicate with anyone, including each other, inside or outside the building, via cellphones and livestreams. They were able to access the internal telephone system. They accessed emails in Speaker Nancy Pelosi's office and could have sent harmful mass email communications. Rioters could have coordinated and mobilized other violence and riots at the U.S. Capitol and anywhere in the world.

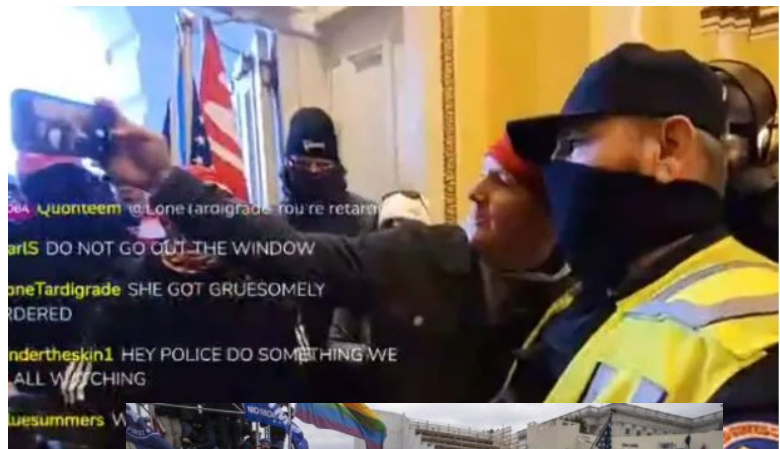
Area around the Capitol was Not Secure- Presence of pipe bombs, napalm, molotov cocktails

Damaging Items – Ransacked offices, threw media equipment into a pile outside and tried to light it on fire



(U//LES) Figure 3: Cooler filled with suspected IIDs. (Source: FBI WFO)

Capitol Police There were photos and videos of Capitol Police moving barriers out of the way, motioning rioters to enter the building, and taking selfies with rioters. There are other photos and videos showing Capitol Police pushing back and punching rioters trying to move past barriers.



Capitol Police Officer Brian Sicknick later died from injuries after a rioter hit him in the head with a fire extinguisher. Clearly, there were many officers fighting to protect the Capitol. There are questions regarding some members of the force and any effort to assist rioters.



FBI Offers \$50k for Info Regarding Pipe Bombs Found in D.C.



Reward:

The FBI is offering a reward of up to \$50,000 for information leading to the location, arrest, and conviction of the person(s) responsible for the placement of suspected pipe bombs in Washington, D.C. on January 6, 2021.

Details:

At approximately 1:00 p.m. EST on January 6, 2021, multiple law enforcement agencies received reports of a suspected pipe bomb with wires at the headquarters of the Republican National Committee (RNC) located at 310 First Street Southeast in Washington, D.C. At approximately 1:15 p.m. EST, a second suspected pipe bomb with similar descriptors was reported at the headquarters of the Democratic National Committee (DNC) at 430 South Capitol Street Southeast #3 in Washington, D.C.

Submit a Tip:

If you have any information concerning these incidents, please contact the FBI's toll-free tip line at 1-800-CALL-FBI (1-800-225-5324), or submit tips online at fbi.gov/USCapitol. You may also contact your [local FBI office](#) or the nearest [American Embassy or Consulate](#).

Additionally, the FBI is seeking help identifying "individuals making unlawful entry into the United States Capital Building" during the riots in D.C. There are pages of photos of individuals yet to be identified, including this [one](#). There have been over 80 arrests made (and probably many more at the time this newsletter is published). Investigators have received over 17k tips.

G2M Research Multi-Vendor Webinar Series

Our 2021 webinar schedule is ready! Click on any of the topics to get more information about that specific webinar. Interested in Sponsoring a webinar? Contact [G2M](#) for a prospectus.

Our November webinar "Implementing NVME™ & NVMe-oF™ for Cloud Service Providers" was sponsored by [Kioxia](#) (Joel Dedrick), [Lightbits](#) (Josh Goldenhar), and [Western Digital](#) (Mark Miquelon). [View the recording](#) and/or [download a PDF of the slides](#).

- Jan 19: Can Your Server Handle The Size of Your SSDs?
- Feb 23: Storage Architectures to Maximize the Performance of HPC Clusters
- March 23: One Year after COVID-19: How Did Storage Architectures Perform for Biotech AI Modeling & What Can We Learn From This?
- April 20: The Race to be Relevant in Autonomous Vehicle Data Storage (both On-Vehicle and Off-Vehicle)
- May 18: Responsive and Efficient Storage Architectures for Social Media
- June 15: It's 2021 - Where Has NVMe-oF™ Progressed To?
- July 13: Computational Storage vs Virtualized Computation/Storage in the Datacenter: "And The Winner Is"?
- Aug 17: AI/ML Storage - Distributed vs Centralized Architectures
- Sept 14: Composable Infrastructure vs Hyper-Converged Infrastructure for Business Intelligence
- Oct 12: Cloud Service Providers: Is Public Cloud, Private Datacenter, or a Hybrid Model Right for You?
- Nov 9: The Radiometry Data Explosion: Can Storage Keep Pace?
- Dec 14: 2021 Enterprise Storage Wrap-up Panel Discussion

