



July 26, 2024

IT Outage from CrowdStrike's Update: Impacts to Certain Public Safety Systems and Considerations for Congress

On July 19, 2024, CrowdStrike, a U.S. cybersecurity firm, [released](#) a software update to their customers. The update caused certain systems to crash, disrupting services across several industries, including [airlines](#), banks, hospitals, government agencies, and public safety systems.

CrowdStrike reported that the incident was [caused by](#) “a defect found in a single content update of its software on Microsoft Windows operating systems” and was not a cyberattack. Though the update affected [less than 1%](#) of all Windows machines, the impacts were [widespread and global](#). The incident illustrates the vulnerabilities of information technology (IT) systems, increased dependence and risks in relying on third-party vendors for critical IT services, and lack of protocols and backup systems in the event of IT system failures.

This In Focus discusses the incident's impact on certain U.S. public safety communications systems and services.

Impact on Public Safety Systems

The incident affected public safety agencies that use CrowdStrike's cybersecurity software on their computer systems. This included some 911 systems; police and fire agency systems; fire alarms; and [broadcast networks](#), some of which play a role in emergency alerting. It also affected the computers and operations of some federal agencies that support public safety agencies and emergency response.

Selected 911 Systems and Services

The CrowdStrike update reportedly affected public safety systems and services in certain jurisdictions across several states. In some areas (examples below), 911 centers were able to receive voice calls, but their computer systems were not operational.

- In Phoenix, AZ, the police department [reported](#) the outage affected their computerized 911 dispatch center—people could still call the 911 center and calls were being answered, but caller information was recorded manually rather than through the computerized dispatch system.
- In Portland, OR, the mayor's office [announced](#) some of the city's computers and servers were affected, including the Bureau of Emergency Communication [computer-aided dispatch \(CAD\) system](#)—people could still make voice calls to the 911 center, but the center had to switch to taking calls manually rather than answering calls using its computerized system.

In other areas (examples follow), the update reportedly affected 911 calling.

- In Alaska, state troopers [announced](#) 911 systems were not operating correctly due to the incident and posted alternative phone numbers to call in lieu of 911.
- In Middletown, OH, police issued a notice to the public of its [inability](#) to receive 911 calls and offered alternative phone numbers.

Other jurisdictions [reported no impacts](#) to 911 services.

Other Public Safety-Related Systems

In some areas (examples below), the faulty CrowdStrike update affected other public safety-related systems.

- In Columbus, OH, police [reportedly](#) were unable to access data from terminals in their vehicles, including law enforcement data systems and license plate information, and firefighters were unable to receive dispatch information in their vehicles.
- In Ocean City, MD, fire alarms that automatically contact the fire department upon detection of a fire [reportedly](#) were affected.

Federal Agencies Supporting Public Safety

- A Department of Homeland Security (DHS) manager [reported](#) that some staff encountered issues logging into desktop computers but were able to work through phones, virtual desktop, or web-based applications.
- DHS's Federal Emergency Management Agency (FEMA) [reported](#) some issues with its systems, but an agency spokesperson said, “there are no impacts to FEMA's critical or immediate lifesaving and life-sustaining operations. There is also no evidence of any data loss.” FEMA's Integrated Public Alert and Warning System (IPAWS) and the Emergency Alert System were [reportedly](#) working normally; however, some [broadcasters](#) whose stations may play a role in distribution of alerts and warnings were affected.

Impact on Telecommunications Systems

Public safety agencies rely on commercial telecommunication networks as an additional means of communications, for [prioritization of calls](#) for officials, and for 911 calling and emergency alerting. Telecommunication networks seemingly were not affected by the incident. People were able to make calls and communicate on landline and cell phone networks. IT systems of [some](#) telecom providers who use CrowdStrike's service were affected, leading to some disruption of business operations and customer service, but networks remained operational.

The incident was similar to a February 22, 2024, outage of the [AT&T wireless network](#) in that both were caused by a faulty software update, and both affected public safety systems. The events were different in that AT&T was updating its own network, whereas CrowdStrike—a third-party vendor that provides cybersecurity services to companies and government agencies—was updating its client-end software on its customers' computers.

Future Public Safety Considerations

In a 2017 [white paper on telecommunications security](#), Oracle, a U.S.-based computer networking technology company, explained that telecommunication networks were “designed in a different era,” where a small set of operators managed the physical interconnection of networks and network security. The emergence of Internet Protocol (IP)—the set of rules for addressing and routing data over the internet—enabled interconnectivity between many networks, creating the global internet and the ability for IP-based networks and devices to interconnect. With the adoption of IP-based devices (e.g., smartphones, smart TVs), Oracle reports, “now virtually anyone can purchase or gain access to networks,” creating new risks.

The telecommunications and public safety sectors have been migrating to IP-based networks and [software-defined networks](#) to enhance network management and performance and enable interconnectivity. One example is Next Generation 911 (NG911), which allows for advanced capabilities, such as text-to-911 and other multimedia communications (e.g., videos), improved call routing, enhanced location-finding, and interconnection with other 911 centers. While NG911 enables interconnectivity between 911 centers, enhancing [redundancy and resiliency](#), it also introduces new vulnerabilities, including cyber risks.

Some companies address cyber risks internally, protecting their devices, networks, and data through their own IT solutions. Others adopt third-party vendors to protect their systems. CrowdStrike is a third-party vendor providing such services. Use of third-party vendors for critical IT services creates another risk for network operators in that any outage caused by or to a third-party provider or supplier also presents risks. In this case, dependence on CrowdStrike, a large cybersecurity firm that offers its services globally, explains the widespread outage.

The incident demonstrates the need for cybersecurity detection and services as well as the heavy reliance that entities, including public safety agencies, may have on one vendor. The risk is that when the vendor releases a software update over the internet, it can affect many computers and many entities at once, including public safety agencies. As more public safety systems move toward IP-based systems, more entities may rely on network-based, third-party services to address cyber risks. In this context, it may be important for public safety agencies to increase attention to and investment in backup protocols and systems that allow entities to maintain continuity of service during outages.

Executive Branch Response

The White House [reportedly](#) has been assessing the impact of the incident on federal IT, critical infrastructure, and

public safety systems and to industry. DHS's Cybersecurity and Infrastructure Security Agency (CISA) [announced](#) that it was working closely with CrowdStrike and with federal, state, local, tribal, and territorial partners, as well as with critical infrastructure and international partners to assess impacts and support remediation efforts. The Federal Communications Commission (FCC) [reported](#) it was working with other federal agencies to assist with the disruptions and assess the extent of the impact on 911 services.

Congressional Response

Some Members and committees have responded to the CrowdStrike incident. The chair and a subcommittee chair of the House Committee on Homeland Security [wrote a letter](#) requesting that CrowdStrike schedule a hearing with the subcommittee. Some Members of the House Oversight and Accountability and House Energy and Commerce Committees reportedly have separately requested briefings from CrowdStrike.

Considerations for Congress

Congress may seek to assess and address potential new risks and backup considerations for public safety agencies, particularly as Congress considers funding for the transition to NG911. For instance, Congress could direct

- DHS's CISA to work with public and private partners to identify and assess risks to public safety systems and recommend mitigation methods and best practices to avoid outages of public safety systems.
- National Institute of Standards and Technology to develop recommendations for minimum standards for testing and release protocols for software updates [as it does](#) for software testing and security.

Congress also could provide or prioritize funding for critical infrastructure resiliency, including for public safety backup systems.

While the FCC [regulates](#) telecommunications service providers and requires reporting of outages that may affect 911 services, it has [limited regulatory authority](#) over internet service providers or IT service providers that support public safety communications (e.g., 911, alerting). The FCC recently has [sought comment](#) on a proposal to require broadband internet access providers to report on outages during disasters; the FCC cited public safety dependencies on the internet. Congress may consider policies to ensure internet outages, such as telecommunications outages, are timely reported and communicated to public safety system operators (e.g., 911 centers, alerting agencies, police and fire departments).

See also CRS Report R48135, *IT Disruptions from CrowdStrike's Update: Frequently Asked Questions*.

Colby Leigh Pechtoll, Specialist in Telecommunications Policy

Jill C. Gallagher, Specialist in Telecommunications Policy

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.