Congress of the United States

Washington, DC 20515

March 4, 2026

Orice Williams Brown
Acting Comptroller General of the United States
Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Brown:

We write to request that the Government Accountability Office (GAO) conduct an investigation of the serious national security threat described in the attached unclassified report produced by the Congressional Research Service (CRS). As the CRS report notes, GAO conducted a prior review related to this issue in 1986, but that GAO review did not assess the efficacy of the government's efforts to counter this threat, nor has GAO conducted a follow-up review since.

The surveillance methods described in the CRS report do not just pose a counterintelligence threat to the U.S. government, but these methods can also be exploited by adversaries against the American public, including to steal strategically-important technologies from U.S. companies. Moreover, as the CRS report also notes, some of these methods have been rediscovered and published by academic researchers, broadening the adversaries that can potentially exploit them beyond foreign intelligence agencies to include criminals, surveillance mercenaries, and private investigators.

Although the surveillance methods described in the CRS report are more than 80 years old, and have been described in a National Security Agency (NSA) report from 1972, declassified by NSA in 2007 and published on its website, and which is cited by the CRS report, the U.S. government has neither warned the public about this threat, nor imposed requirements on the manufacturers of consumer electronics, such as smartphones, computers and computer accessories, to build technical countermeasures into their products. As such, the government has left the American people vulnerable and in the dark.

It has been nearly 40 years since GAO last reviewed this issue. Accordingly, we urge GAO to conduct a follow-up investigation to review:

1. The scale of the threat to the U.S. government, to the private sector, and to the public.
2. The effectiveness of the U.S. government's efforts to mitigate this threat, to classified and unclassified information held by the government.
3. Whether there is additional information that can be released by the U.S. government, consistent with the protection of sources and methods, that could assist the public and the private sector in addressing this threat.

4. The feasibility and cost of device manufacturers adding surveillance countermeasures to consumer electronics, such as smartphones, computers, and computer accessories.
5. Potential policy options to mitigate this threat against the public, including mandating device manufacturers add countermeasures to their products.

Thank you for your attention to this important matter.

Sincerely,

Ron Wyden
United States Senator

Shontel M. Brown
Member of Congress

Congressional Research Service
Informing the legislative debate since 1914

MEMORANDUM January 27, 2026

To: Senator Ron Wyden
[redacted]

From: [redacted]

Subject: **Background on TEMPEST**

This memorandum responds to your request for information on TEMPEST—the code name the National Security Agency (NSA) gave to a security risk whereby an attacker could observe the nonradioactive radiations or other emanations from an information technology (IT) device and reconstruct what that device was processing. Specifically, you requested: (1) background information and a history of TEMPEST; (2) details on how the United States government has responded to this threat; (3) a list of ongoing concerns about TEMPEST today; (4) a description of the ways in which TEMPEST attacks may be mitigated today; and (5) a list of authorities that the U.S. government could use to compel equipment manufacturers to mitigate against TEMPEST attacks.[1]

Information in this memorandum may be of general interest to Congress and may appear in other CRS products. Your confidentiality will be maintained in this event. CRS is available to follow up, in person or remotely, at your convenience.

TEMPEST Background

The National Institute of Standards and Technology (NIST) recognizes the definition of TEMPEST from the Committee on National Security Systems (CNSS) Instruction 4009-2015 as "a name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment."[2]

The Federal Information Processing Standard on *Security Requirements for Cryptographic Modules* further elaborates:

> TEMPEST attacks involve the remote or external detection and collection of the electromagnetic signals emitted from a cryptographic module and associated equipment during processing. Such an attack can be used to obtain keystroke information, messages displayed on a video screen, and other forms of critical security information (e.g., cryptographic keys). Special shielding of all components,

[1] Much about TEMPEST remains classified. CRS based information in this memorandum on unclassified government documents, declassified government documents, and academic research papers.

[2] National Institute of Standards and Technology, "TEMPEST," webpage, https://csrc.nist.gov/glossary/term/tempest. CNSSI 4009-2015 itself is not publicly available.

including network cabling, is the mechanism used to reduce the risk of such an attack. Shielding reduces and, in some cases, prevents the emission of electromagnetic signals.[3]

At their core, TEMPEST attacks are analog-based observations of information technology that allow the attacker to detect what is being processed or sent by that technology and determine the message (without reading the contents of the message directly).

Attack Examples

For computing devices, the input (e.g., sound emanating from typing on a keyboard) or processing of information (e.g., a hard drive spinning or a light flashing) creates an emanation that could be detected. These emanations can be observed by some sensors and logged. That logged data can then be studied and analyzed, and reconstructed to its original state (or close enough to its original state so as to leak sensitive data).

Some ways this can be accomplished are:[4]

- **Acoustically** – microphones could be employed near a device (e.g., covertly installed or a telephone may be left off the hook) to record the sounds coming from the device. The attacker then studies the recording to recreate data. For example, a recording of a user typing in their password could lead an attacker to discover the keystrokes necessary to recreate that password.
- **Radio Frequency –** antennas could be employed as far as a mile away from a device (if oriented correctly and assuming minimal interferences) to observe signal emanations from a device. This is different from the intended broadcast of radio frequencies related to Wi-Fi or cellular connectivity. Instead, a component of a device may radiate a radio frequency during its operation, which could indicate the power load under that device and could assist in the processing of signal data to recreate plaintext data.
- **Electromagnetically** – sensors could be placed near a device to observe the electromagnetic emanations of a device. Device components generate and emanate electromagnetic energy as electric currents flow through those devices or the cables connecting components. Software-defined radios (i.e., a computer with an analog signal to digital converter, and radio frequency antenna) could be employed to acquire and process the signal coming through an electromagnetic emanation. For such attacks to be successful, one would likely need to know the type of device generating the content, where the emanation is being detected, and where the observed information is going since knowledge of the origination and destination components would key attackers into how the data is structured.

History

The potential for TEMPEST attacks was discovered by Bell Labs during World War II. At the time, Bell made cryptographic equipment to encrypt sensitive information for the U.S. Army and Navy. In testing one of their teletypewriters, engineers observed a reaction in a distant oscilloscope (a testing instrument that graphically displays the voltage of an observed signal in wave form). Upon further study, the

[3] National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, FIPS PUB 140-2, May 25 2001 (superseded), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf.

[4] Justin Markland, "TEMPEST: Electronic Spying and Countermeasures," March 25, 2025, https://greydynamics.com/tempest-electronic-spying-and-countermeasures/#h-2-understanding-tempest.

engineer found that he could read the plaintext of the teletypewriter by studying the oscilloscope information.[5]

TEMPEST attacks appear to have ebbed and flowed since this discovery. Knowledge of the attacks became largely dormant following World War II.[6] In the 1960s, however, U.S. military officers noticed technical surveillance (e.g., microphones and antenna) inside or nearby sensitive government facilities.[7] In subsequent years, TEMPEST attacks were a tool used by intelligence services to discover sensitive information from various technology devices.

Government Response

Since World War II, there have been four primary ways the U.S. government has employed to combat TEMPEST attacks:

- **Distancing** – creating a safe zone of many hundreds of feet from a device to limit the ability of its emanations to travel through space and be detected by a sensor.[8]
- **Shielding** – sometimes called *hardening,* refers to the blocking of a device's emanations (e.g., electromagnetic radiation). This can be done on the device itself (e.g., ferrite balls attached to a cable to interfere with magnetic fields), or by insulating the room containing that device (e.g., rooms insulated with metal cages). Government secure compartmented information facilities (SCIFs) employ shielding.[9]
- **Masking –** involves operating many devices simultaneously to create enough signal noise so that malicious sensors have difficulty in identifying single streams of data.[10]
- **Filtering –** attempting to add information (e.g., additional radiation or acoustic sound) to, or remove information from, the emanation of a single or multiple devices so as to interfere with its ability to travel through space.[11]

In 1981, the Reagan Administration's National Communications Security Committee released the *National Policy on Control of Compromising Emanations* and established a Subcommittee on Compromising Emanations. The policy at the time was for the head of each federal agency to manage the TEMPEST risks, take corrective actions, and ensure compliance with the policy by contractors to the agency. Guidance for mitigating TEMPEST risks was to be shared by the NSA, which was also responsible for technical analysis of TEMPEST threats.[12]

Based on publicly available information, the applicability and implementation of this policy are unclear. Technical specifications for controlling TEMPEST risks are not publicly available. Publicly available information indicates some acknowledgment of the risks of TEMPEST, but does not prescribe mitigating

[5] National Security Agency, *TEMPEST: A Signal Problem*, approved for release on September 27, 2007, https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/tempest.pdf.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] National Counterintelligence and Security Center, "Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities," IC Tech Spec – For ICD/ICS 705 version 1.5, March 13, 2020, https://www.dni.gov/files/Governance/IC-Tech-Specs-for-Const-and-Mgmt-of-SCIFs-v15.pdf.

[10] National Security Agency, *TEMPEST: A Signal Problem*, approved for release on September 27, 2007, https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/tempest.pdf

[11] Ibid.

[12] Central Intelligence Agency, *National Policy on Control of Compromising Emanations (U)*, approved for release on February 8, 2008, https://www.cia.gov/readingroom/docs/CIA-RDP96M01138R000900020034-2.pdf.

strategies. It also appears that TEMPEST program applicability was focused on communications security (COMSEC, e.g., cryptographic devices) and not general-purpose information technology. For example, although the 2001 Federal Information Processing Standards Publication (FIPS PUB) 140-2—*Security Requirements for Cryptographic Modules*—mentions TEMPEST, TEMPEST references were dropped from the current 2019 version (FIPS PUB 140-3).

Despite the variety of federal agencies with COMSEC equipment, the applicability of policies across government, and the discovery of sensors near federal facilities, CRS was unable to find any information about uniform TEMPEST-mitigation policies across the federal government. The Department of Defense refers to TEMPEST in the department's acquisition regulation.[13] The Department of Energy also acknowledges TEMPEST risks in the department's Technical Security Program.[14] In both cases, however, it is unclear the extent to which policies have been adopted. Nor is it clear whether these departments are ensuring compliance with TEMPEST mitigation policies.

In 1986, the General Accounting Office (since renamed the Government Accountability Office [GAO] in 2004) reviewed the Department of Defense TEMPEST protection countermeasure program. GAO recommended that DOD clarify its policies, which DOD did—so, GAO closed their recommendations.[15] From the unclassified report, it does not appear that GAO evaluated the efficacy of the countermeasure program, nor has GAO followed up with a new TEMPEST review of any agency since.

TEMPEST Today

Early TEMPEST exploitations occurred against analogue devices. Spinning hard drives on computers and mechanical switches on cryptographic teletypewriters emitted a lot of capturable data.[16] As devices became more digital, (e.g., solid state hard drives and touchscreen keyboards) the exploitation potential of the emanations of such devices changed.

Information processing has also evolved. The push for cloud computing, as a side benefit, has included many TEMPEST mitigation tactics: many computing resources operate simultaneously masking emanations, and data centers are physically distanced and hardened. Mobile computing has also changed how attackers think about deploying sensors. Since devices are constantly in transit, and sensors are not, the intelligence gain-loss calculations related to the opportunity costs for an attacker have shifted.[17]

Security research of emanation-based exploitation is still occurring. Today, many of these attacks are referred to as *side-channel* attacks (rather than TEMPEST).[18] These attacks do not directly compromise a device, nor do they directly read data. Instead, they use secondary information from the target device or nearby devices to reconstruct data.

---

[13] Department of Defense – Defense Federal Acquisition Regulation, "Acquisition of Information Technology: Compromising emanations—TEMPEST or other standard," *DFAR 239.7102-2*, https://www.acquisition.gov/dfars/part-239-acquisition-information-technology.

[14] Department of Energy, "Technical Security Program," *DOE Order 470.6*, September 2, 2015, https://www.directives.doe.gov/directives-documents/400-series/0470.6-BOrder/@@images/file.

[15] U.S. Government Accountability Office, *DOD Tempest Protection: Better Evaluations Needed to Determine Required Countermeasures*, NSIAD-86-132, July 27, 1986, https://www.gao.gov/products/nsiad-86-132.

[16] Thomas M. Donahue, "Static Magic, or The Wonderful World of TEMPEST, or One Man's Statis is Another Man's Treasure," *CRYPTOLOG*. November 1983, https://media.defense.gov/2021/Jul/01/2002754916/-1/-1/0/CRYPTOLOG_84.PDF.

[17] For a further discussion, see Alex Arno, "TEMPEST Countermeasures: Safeguarding Against Unintentional Data Leakage," blog post, March 12, 2025, https://www.spgsecure.com/post/tempest-countermeasures-safeguarding-against-unintentional-data-leakage.

[18] David Temoshok, Diana Proud-Madruga, Yee-Yin Choong, et. al., Digital Identity Guidelines, *NIST SP 800-63-4*, July 2025, p. 80, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.pdf.

In 2009, researchers found ways to capture the electromagnetic emanations from wired and wireless keyboards to recover keystrokes.[19] Similar to the earlier methods of conducting acoustic-based attacks to capture keystrokes, researchers in 2011 figured out a way capture data from the accelerometer of a nearby smartphone to decode the inputs of a keyboard.[20] In 2013, a researcher found ways to exploit the frequency, timing, and emanations from liquid-crystal display (LCD) televisions to reconstruct the image shown on the screen.[21] In 2020, researchers showed ways to measure the emanations from digital video display cables to expose the objects being shown on display units.[22] In 2022, researchers discovered a way to read the extremely small variations in air pressure on a lamp bulb to recover what was spoken in the same room as the bulb.[23]

Counterintelligence professionals are aware of the risk posed by existing vulnerabilities to TEMPEST (or side-channel) attacks.[24] Equipment necessary to detect emanations is easily acquired. Less is understood about the knowledge and skill necessary to successfully execute an attack, and how applicable proofs of concepts are to real-world emanations collection and processing.

In today's risk space, traditional cyberattacks are very successful in providing attackers direct access to data, negating the need to indirectly collect information, except in the most unique circumstances. A side-channel (or TEMPEST) attack may be a preferable attack technique for a foreign intelligence service to employ against targets in certain situations since it allows an adversary to passively collect intelligence, thereby avoiding the need to place a sensor nearby or malware on a device and risk detection.

Mitigating TEMPEST Threats Today

The U.S. government has employed *hardening* strategies against TEMPEST threats in the past. These strategies included distancing, shielding, and filtering—which are all implemented in the design and construction of a SCIF. Hardening relies on creating physical security around the devices processing information.[25]

Physically securing a device protects all three states of associated data—storage, process, and transit—against TEMPEST threats. Physical security is not always practical, however. It is expensive to harden devices and the spaces they operate in, and modern devices may move about (e.g., removed from the SCIF), thereby nullifying the protections provided by the space.

[19] Marting Vuagnoux and Sylvian Pasini, "Compromising Electromagnetic Emanations of Wired and Wireless Keyboards," *18th Usenix Security Symposium,* August 12, 2009, https://www.usenix.org/legacy/event/sec09/tech/full_papers/sec09_attacks.pdf.

[20] Philip Marquardt, Arunabh Verma, Henry Carter, et al, "iPhone: Decoding Vibrations from Nearby Keyboards Using Mobile Phone Accelerometers," *Association for Computing Machinery,* October 17, 2011, https://dl.acm.org/doi/10.1145/2046707.2046771.

[21] Markus G. Kuhn, "Compromising Emanations of LCD TV Sets," *IEEE Transactions on Electromagnetic Compatibility,* June 2013, https://ieeexplore.ieee.org/document/6488807.

[22] Pieterjan De Meulemeester, Bart Scheers, and Guy A. E. Vandenbosch, "A Quantitative Approach to Eavesdrop Video Display Systems Exploiting Multiple Electromagnetic Leakage Channels," *IEEE Transactions on Electromagnetic Compatibility,* June 2020, https://ieeexplore.ieee.org/document/8751145.

[23] Ben Nassi, Yaron Pirutin, Raz Swissa, et al., "Lamphone: Passive Recovery from a Desk Lamp's Light Bulb Vibrations," 31st *Usenix Security Symposium,* August 10-12, 2022, https://www.usenix.org/system/files/sec22-nassi.pdf.

[24] Defense Intelligence Agency, "Terms and Definitions of Interest for DOD Counterintelligence Professionals," glossary, May 2, 2011, https://www.dni.gov/files/NCSC/documents/ci/CI_Glossary.pdf.

[25] National Counterintelligence and Security Center, "Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities," IC Tech Spec – For ICD/ICS 705 version 1.5, March 13, 2020, https://www.dni.gov/files/Governance/IC-Tech-Specs-for-Const-and-Mgmt-of-SCIFs-v15.pdf.

Another way to mitigate against TEMPEST threats is to transform the data being observed.[26] A common way to do this is to encrypt the data. When encrypted, data may lay at rest on a storage device or be in transit to another device (by wireless signal or wireline) and be unintelligible to observers. By changing the data (e.g., by encrypting it) the emanations detected by the attacker will lead to cipher text rather than the plaintext of the message itself. There are also ways to process data while it is encrypted (e.g., homomorphic encryption). The benefits of encryption (especially homomorphic encryption), however, carry a computational cost.[27]

Federal Authority to Address TEMPEST Threats in Consumer Goods

There is no federal statutory authority directed to comprehensively mitigating TEMPEST threats in all consumer goods or equipment manufacturing. Depending on the goods, however, some federal statutes may provide authority to mandate certain activities that mitigate some relevant threats.

One example is the Federal Trade Commission (FTC) Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce," among other things.[28] The FTC, in some cases, has interpreted this authority to require some companies to use encryption or similarly effective security methods to protect certain data.[29] In its enforcement actions, the FTC has pointed to a failure to encrypt customers' data in allegations that a company's data security measures amount to an unfair act or practice.[30] In cases where companies advertise their products' security, the FTC has again pointed to encryption failures in allegations of deceptive acts or practices.[31] Accordingly, when a consumer good records data about its customers, the FTC Act may impose certain data security requirements, and those requirements could help mitigate TEMPEST threats.[32]

The Federal Communications Commission (FCC) also has potentially relevant authority. The FCC can, for example, issue "reasonable regulations . . . establishing minimum performance standards for home electronic equipment and systems to reduce their susceptibility to interference from radio frequency energy."[33] The agency has used this and related authorities to impose security requirements on certain devices,[34] such as those compatible with the Citizens Broadband Radio Service.[35]

None of these authorities are expressly directed at mitigating TEMPEST threats though. An FTC action that results in a company agreeing to encrypt "in transit and at rest" all "home security recordings" made

[26] Alex Arno, "TEMPEST Countermeasures: Safeguarding Against Unintentional Data Leakage," blog post, March 12, 2025, https://www.spgsecure.com/post/tempest-countermeasures-safeguarding-against-unintentional-data-leakage.

[27] For further information, see CRS Report R44642, *Encryption: Frequently Asked Questions*, by Chris Jaikaran

[28] 15 U.S.C. §45(a).

[29] See, e.g., F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 240, 256 (3d Cir. 2015) (affirming the FTC's authority to regulate cybersecurity under the unfairness prong of 15 U.S.C. §45(a) in a case where the FTC alleged that a company "did not use *any* encryption for certain customer files").

[30] See, e.g., ibid.; Complaint ¶¶48, 62–64, F.T.C. v. Ring LLC, No. 1:23-cv-1549 (D.D.C. May 31, 2023).

[31] See, e.g., *Wyndham*, 799 F.3d at 241; Complaint ¶¶48, 56–58, F.T.C. v. Ring LLC, No. 1:23-cv-1549 (D.D.C. May 31, 2023); Complaint ¶¶9, 19–23, Henry Schein Practice Solutions, Inc., No. C-4575 (F.T.C. May 20, 2016).

[32] See *supra* "Mitigating TEMPEST Threats Today" (explaining that encrypting data can help mitigate TEMPEST threats).

[33] 47 U.S.C. §302a(a).

[34] Cybersecurity Labeling for Internet of Things, 39 F.C.C. Rcd. 2497, at ¶160 (Mar. 14, 2024).

[35] 47 C.F.R. §96.39(f)–(g); see also Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band, 30 FCC Rcd 3959, 4033-4034 (Apr. 17, 2015).

with a consumer device[36] may *incidentally* make the device less vulnerable to TEMPEST attacks. A determination of whether a company violates the FTC Act's unfair or deceptive acts or practices prohibition, however, will not necessarily include an evaluation of vulnerabilities to TEMPEST attacks specifically. That determination will turn on the meaning of "unfair or deceptive acts or practices," as used in the FTC Act.[37]

[36] Stipulated Order for Injunction and Monetary Judgment §III.E.7, F.T.C. v. Ring LLC, No. 1:23-cv-1549 (D.D.C. June 16, 2023).

[37] 15 U.S.C. §45(a); see also ibid. §45(n); *Wyndham*, 799 F.3d at 243–59 (applying the unfairness prong of the FTC Act to cybersecurity practices); CRS In Focus IF12244, *Unfair or Deceptive Acts or Practices (UDAP) Enforcement Authority Under the Federal Trade Commission Act*, by Eric N. Holmes (2022).