



## Privacy Impact Assessment of Video Surveillance Monitoring System “VSMS”

For Questions or Comments, please email: [privacy.comments@frb.gov](mailto:privacy.comments@frb.gov)

### Description of the IT system:

The Board of Governors of the Federal Reserve’s (Board) uses a third-party vendor to provide a digital security video surveillance monitoring system (VSMS) to view, record, and manage video cameras inside and outside the Board’s owned and leased buildings.

### 1. The information concerning individuals that is being collected and/or maintained:

The VSMS captures employees, contractors, visitors, and members of the public in view of cameras located in common areas inside and outside the Board’s owned and leased buildings (building perimeter entrances and exits, parking garages, hallways and corridors, courtyards, sidewalks, reception areas, and elevator lobbies). This includes individuals' facial features, physical characteristics, clothing, and personal belongings such as bags and packages, as well as date and time stamps of entry and exit activities. The system also records license plate numbers of vehicles, mobility aids (e.g., wheelchairs or walkers), interactions between individuals, and the presence of service delivery personnel and vendors. Notably, the system records only video, no audio is captured.

### 2. Source(s) of each category of information listed in item 1:

Board employees, contractors, visitors, and members of the public inside and outside the Board’s owned and leased buildings.

### 3. Purposes for which the information is collected:

The VSMS supports the Board’s security responsibilities by:

- *Enhancing security awareness.* VSMS is utilized across all owned and leased buildings to increase the Board's overall security posture.
- *Supporting investigations.* Provides video footage to aid security incident investigations.
- *Evaluating operations.* VSMS allows for the assessment and improvement of the Board's Law Enforcement Unit (LEU) operations.

*Responding to legal requests.* The system facilitates timely and accurate responses to lawful requests received by the Board (e.g., subpoenas, search warrants, and court orders).

**4. Who will have access to the information:**

Access to video footage is restricted to authorized staff with official business purposes. In particular, the Board's LEU and LEU-Technical Security (LEU-TS) are authorized to access both live and recorded video footage. The Protective Service Unit, Motor Transport Unit, and Facilities Control Center are authorized to access only live video footage.

The system owner or system manager must approve VSMS footage prior to sharing within the Board. Legal approval is required before sharing any videos outside the Board with state, local, and federal law enforcement for purposes of supporting lawful investigations. Disclosures may also be subject to the Freedom of Information Act (5 U.S.C. §552).

**5. Whether the individuals to whom the information pertains have an opportunity to decline to provide the information or to consent to particular uses of the information (other than required or authorized uses):**

Individuals do not have an opportunity to decline VSMS' recording or provide consent to the Board's use of the video content.

**6. Procedure(s) for ensuring that the information maintained is accurate, complete and up-to-date:**

VSMS does not have the capability to edit or alter its captured content.

**7. The length of time the data will be retained:**

Videos are saved for 30 days, in accordance with the National Archives and Records Administration's (NARA) General Records Schedule 5.6, Item 90, and then overwritten See, <https://www.archives.gov/files/records-mgmt/grs/grs05-6.pdf>.

**8. The administrative and technological procedures used to secure the information against unauthorized access:**

The Board applies applicable privacy and security controls in the National Institute of Standards and Technology's (NIST) Special Publication 800-53 (Rev. 5), Security and Privacy Controls for Information Systems and Organizations, at the moderate impact level, in accordance with the Federal Information Security Modernization Act (FISMA).

Access to VSMS is restricted to authorized Board staff who require access for official business purposes. The type of information staff are permitted to access is based on their job responsibilities. Periodic reviews are conducted to determine whether users still require access, have the appropriate role, and whether there have been any unauthorized changes in any information maintained in VSMS.

**9. Whether a new system of records under the Privacy Act will be created. (If the data are retrieved by name, unique number or other identifier assigned to an individual, then a Privacy Act system of records may be created):**

VSMS is not a system of records under the Privacy Act of 1974 since it is not searched by name or personal identifiers, so a system of records notice is not required.

**Reviewed:**

<u>//Signed//</u>	<u>01/05/2026</u>
Charles Young Senior Agency Official for Privacy	Date
<u>//Signed//</u>	<u>01/05/2026</u>
Jeff Riedel Chief Information Officer	Date