SmartSuite

Framework / Cybersecurity / Other

SSA Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies (TSSR), Version 8.50

SSA's Electronic Information Exchange Security Requirements (TSSR, v8.50 of 2019) set the controls, certification and compliance reviews state and local agencies meet to receive SSA data.



What it is

The Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration, known throughout its own text as the Technical Systems Security Requirements (TSSR), is the Social Security Administration document that every Electronic Information Exchange Partner (EIEP), meaning a state or local agency with a data exchange agreement with SSA, must meet to receive SSA-provided information. The page name's v8.0 was the draft of June 21, 2018; the current readable edition is Version 8.50 of October 10, 2019, which states that all previous versions are superseded and obsolete, and SSA maintains the TSSR as a living document.

At a glance

PUBLISHER
Social Security Administration, Office of Information Security

TYPE
Standard

VERSION
Version 8.50 (October 10, 2019); v8.0 was the June 21, 2018 draft

EFFECTIVE
October 10, 2019 (Version 8.50)

DOMAIN
Cybersecurity

FAMILY
Other

REGION
United States

INDUSTRY
Government & Public Sector

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: ssa.gov/dataexchange/security.html

Why it matters

- **A named gate before access (section 6)** SSA certifies an EIEP in two phases, the SEQ and an onsite certification review, before online access to SSA-provided information begins, and a new SEQ is needed for a new platform or after SSA revokes an approval.
- **Audit trail with no exceptions (section 5.4)** A fully automated audit trail system must record every query of and every view of SSA-provided information, with user, workstation, action, business purpose and timestamp, each entry stored as a separate record.
- **A one-hour incident clock (section 5.9)** A suspected breach or loss of SSA-provided information goes to the state official responsible for systems security, who notifies the SSA contacts in the agreement; if that cannot be done within one hour, the National Network Service Center is called.
- **Named roles on both sides (section 3)** SSA's Office of Information Security, Regional Data Exchange Coordinators and the state official responsible for systems security named in the agreement carry the certification, review and reporting duties.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports SSA EIESR v8.0

TSSR Requirement Library

Load sections 5.2 to 5.13 and section 6 as requirements with owners, implementation status and the NIST SP 800-53 family each heading cites, linked to policies and evidence.

SEQ Preparation and Versioning

Draft, review and version the Security Evaluation Questionnaire against the 6.2.1 triggers (new access, new platform, changes since the last approval, revocation) and keep every submitted version with SSA's approval.

Access Authorization Records

Record who is designated to authorize access to SSA-provided information, each user's need-to-know basis, removals after adverse action and remote access approvals under section 5.3.

Incident Reporting Workflow

Route a suspected breach or loss of SSA-provided information to the state systems security official with the one-hour escalation to the SSA contacts or the National Network Service Center, the agreement's worksheet and the follow-up updates section 5.9 requires.

Training and Sanctions Evidence

Track section 5.10 security awareness training and acknowledgments for every employee, contractor and agent with access, and the sanctions applied for misuse such as employee browsing.

Compliance Review Readiness

Schedule the triennial or 3 to 5 year compliance review and any ad hoc review trigger, assemble the SEQ, audit trail samples, exception reports and data center evidence, and track findings to closure in Internal Audit Management.

Common framework mappings

CIS Controls v8.1 · FedRAMP Rev. 5 · HIPAA (NIST SP 800-66 Rev. 2) · ISO 27001:2022 · ISO 27002:2022 · NIST CSF 2.0 · NIST 800-53 Rev.5 · SOC 2

Official resources

SSA TSSR Version 8.50 (October 10, 2019), partner-hosted copy

The Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies (TSSR) v8.50, as hosted by the Illinois Department of Healthcare and Family Services, an SSA data exchange partner; ssa.gov blocks automated fetchers.

hfs.illinois.gov/content/dam/soi/en/web/hfs/sitecollectiondocuments/ieafattachment4tssrv850final10022019.pdf

Frequently asked questions

What is the SSA TSSR, and is v8.0 the current version?

The Technical Systems Security Requirements is SSA's name for the Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration. Version 8.0 was a draft completed on June 21, 2018; the revision history shows 8.1 in November 2018, 8.20 in January 2019 and Version 8.50 on October 10, 2019, whose cover note says all previous versions are superseded and obsolete. SSA describes the TSSR as a living document, so partners should confirm the current edition with their Regional Data Exchange Coordinator.

Who has to comply with the TSSR?

Every Electronic Information Exchange Partner, meaning a state or local agency that has a Computer Matching and Privacy Protection Act agreement or Information Exchange Agreement with SSA, together with the contractors and agents that process, maintain, transmit or store SSA-provided information on its behalf (sections 1, 3, 5.11). Section 1 states that an EIEP must comply with SSA's most current TSSR to gain electronic access, and section 6 applies the compliance review program to both online and batch access.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How do SSA's certification and compliance reviews work?

Section 6.1 describes a two-phase security certification for EIEPs seeking online access: Phase 1 is the Security Evaluation Questionnaire, a formal written plan of the agency's management, operational and technical controls, and Phase 2 is SSA's onsite certification review; SSA does not allow transactions to start until both are satisfied. Section 6.4 describes the compliance review program, in which the SEQ is resubmitted on an agreed timeline and SSA verifies the safeguards; section 3 calls these reviews triennial and section 6.4 says SSA attempts to follow a 3 to 5 year schedule, with ad hoc reviews after a platform change, a TSSR violation or an unauthorized disclosure.

What does the TSSR require for audit trails?

Section 5.4 requires a fully automated audit trail system capable of creating, storing, protecting and retrieving records that identify the individual user who initiates a request for or accesses SSA-provided information, with date and time stamps, the device or workstation, the action and the business purpose, each entry stored as a separate record. The system must record read-only views and access events that do not change data; the document states that all viewing of SSA-provided information requires an audit trail, with no exceptions.

How must a breach of SSA-provided information be reported?

Under section 5.9 an agency that experiences or suspects a breach or loss of PII or a security incident involving SSA-provided information notifies the state official responsible for systems security designated in the agreement, who notifies the SSA Regional Office contact or SSA Systems Security contact. If that cannot be done within one hour, the official reports the incident to SSA's National Network Service Center, and as a last resort to SSA's Security Operations Center. If SSA or another federal investigator decides that individuals must be notified, the agency agrees to absorb all notification and remediation costs.

License included / downloadable: Yes The TSSR is a U.S. government document that SSA distributes to its exchange partners through the data exchange agreements; a partner-hosted copy of Version 8.50 is publicly available from the Illinois Department of Healthcare and Family Services, and the platform links to SSA's data exchange security page.

Full framework page and mappings: smartsuite.com/frameworks/us-ssa-eiesr-v8-0-electronic-information-exchange-security