



COGNITIVE MODE OPERATING SYSTEM STANDARDS BOARD

CMOS-SB Standard 1001

Emotional Infrastructure Safety Standard

EISS v1.0 | Ratified Date: July 26, 2026 | Status: **Active - Public Comment** | Next Review: July 26, 2027

Field	Value
Standard ID	CMOS-SB-1001
Short Name	EISS
Version	1.0
Governance Spine Position	Pillar 1 of 5 — Foundational Safety Floor
Issued by	CMOS-SB Standards Committee
Ratified by	Founding Council, July 26, 2026
Published	June 9, 2026 (formal public comment period 7/26/26 -8/26/26)
Author / Architect	Isabelle Anne Thompson
Theoretical Basis	Emotional Epidemiology (DOI: 10.5281/zenodo.20314466)
Publication Set Item	Item 6 of the CMOS-SB Publication Set
Prerequisite Standards	None — EISS is the foundational prerequisite for all other Governance Spine standards.

Governance Note *EISS is the foundational safety floor of the CMOS-SB Governance Spine. No system may seek certification under any other Governance Spine standard without first achieving full EISS compliance.*

Table of Contents

1	Purpose and Scope	3
	1.1 Purpose	3
	1.2 Scope – Systems Covered	3
	1.3 Scope - Systems Excluded	4
2	Scientific Foundation	5
3	Key Definitions	6
4	Core Safety Requirements	7
	4.1 Emotional Transparency (ET Requirements)	7
	4.2 Emotional-Risk Minimization (ERM Requirements)	8
	4.3 Relational Integrity Requirements (RI Requirements)	9
5	Safeguard Requirements	10
	5.1 Safeguard Design Pattern Compliance	10
	5.2 Safeguard Documentation	10
	5.3 Safeguard Testing	11
6	Compliance and Certification	11
	6.1 Compliance Evidence Requirements	11
	6.2 Certification Pathway	12
	6.3 Ongoing Compliance	12
7	Regulatory Alignment	13
	Appendix — EISS Compliance Self-Assessment Checklist	14

Section 1 — Purpose and Scope

1.1 Purpose

To establish the baseline safety requirements that any system interacting with, influencing, or responding to human emotional states must meet before deployment and maintain during ongoing operation. EISS is the foundational safety floor of the CMOS-SB Governance Spine: all other Governance

Spine standards build upon its baseline protections. No system within CMOS-SB jurisdiction may seek certification under any other Governance Spine standard without first achieving EISS compliance.

Foundational Position

EISS — Standard 1001 — occupies Pillar 1 of the five-pillar CMOS-SB Governance Spine. All downstream Governance Spine standards are contingent upon EISS compliance. It is not permissible to certify under any other Pillar without first meeting every requirement set forth in this standard.

1.2 Scope — Systems Covered

EISS applies to any system that:

- Infers emotional states from user inputs or behaviors (including text, voice, biometric, behavioral, or interaction data)
- Responds to inferred emotional states through adaptive outputs, personalized content, or altered interaction patterns
- Influences human emotional states through interface design, content selection, pacing, notification architecture, or relational modeling
- Operates at any scale — from single-user tools to platforms with billions of users
- Is deployed in any sector — enterprise, consumer, healthcare, education, government, or research

1.3 Scope — Systems Excluded

EISS does not apply to:

- Purely mechanical systems with no emotional inference or output capability
- Purely offline personal-use applications not deployed for third-party use
- Artistic works (novels, films, games with fixed narrative) not deployed as interactive systems capable of emotional inference
- Systems whose emotional output is purely incidental and de minimis

Section 2 — Scientific Foundations

EISS is grounded in the findings of *Emotional Epidemiology* (Thompson, 2026; DOI: 10.5281/zenodo.20314466). The key scientific findings informing EISS requirements are set out below.

Finding 1: Emotional states propagate through human populations in measurable, predictable ways analogous to biological contagion dynamics.

Finding 2: Digital systems are primary vectors of emotional transmission at modern scale.

Finding 3: System design choices — including interface architecture, content framing, pacing, and adaptive response logic — directly influence population-level emotional Susceptibility (S) and Transmission Rate (R).

Finding 4: Safeguard design can materially increase Collective Resilience (C) and reduce population-level emotional risk.

Finding 5: Covert emotional influence — influence that occurs without user awareness — amplifies susceptibility and transmission in ways that exceed disclosed, consensual interaction.

The **Emotional-Risk Transmission Flow model (EISS v1.0)** describes five stages through which emotional signals move from system input to population-level spread:

Stage	Flow Step	Description
Stage 1	Emotional Input	User-generated signals (text, voice, biometric, behavioral) enter the system
Stage 2	System Processing	The system applies inference logic to derive emotional state representations
Stage 3	Emotional Output	Adapted outputs are generated and transmitted to the user
Stage 4	User State	The user's emotional state is influenced by the system's output
Stage 5	Population-Level Spread	Emotional states and activations propagate through connected networks and populations

EISS requirements are mapped to safeguard interventions at each stage of this flow. Safeguard feedback controls are designed to intercept and mitigate transmission risk at Stage 2 (Processing), Stage 3 (Output), and Stage 4 (User State) before population-level spread occurs at Stage 5.

Figure 1. Emotional-Risk Transmission Flow (EISS v1.0) — five-stage propagation model with safeguard feedback controls at each stage. Safeguard interventions are designed to interrupt transmission at Stages 2–4 to prevent population-level emotional risk accumulation at Stage 5.

Scientific Citation

Emotional Epidemiology, Isabelle Anne Thompson (2026). DOI: 10.5281/zenodo.20314466. This publication provides the empirical and theoretical basis for the Emotional-Risk Transmission Flow model and all population-level risk constructs referenced in EISS v1.0.

Section 3 — Key Definitions

The following definitions apply throughout EISS v1.0 and all standards that reference EISS as a foundational requirement.

Term	Definition
Emotional-Infrastructure System	Any digital system that interacts with, influences, or responds to human emotional states or cognitive modes at any scale of deployment.
Emotional State	A temporary, dynamic condition of human cognitive-emotional functioning characterized by specific affect, arousal level, valence, and regulatory capacity.
Emotional Signal	Any data point — derived from text, voice, behavior, biometric input, interaction timing, or other source — that is used or reasonably usable to infer a human emotional state.

Term	Definition
Emotional Inference	The process by which a system derives a representation of a user's emotional state from observable signals.
Emotional Output	Any system output — including text, voice, imagery, pacing, notification, or behavioral adaptation — that is designed or reasonably likely to influence a user's emotional state.
Covert Emotional Influence	Any modulation of a user's emotional state that occurs through mechanisms not disclosed to and not reasonably discoverable by the user.
Emotional-Risk Transmission	The propagation of emotional states, signals, or activations through a system or network in ways that may increase susceptibility, amplify distress, or accelerate population-level drift.
Safeguard	A technical or procedural control implemented to prevent, detect, or mitigate emotional or cognitive harm at the Human-Machine Layer.
Population-Level Emotional Dynamics	The aggregate patterns of emotional state, transmission, and stability observable across groups of users or defined populations.

Section 4 — Core Safety Requirements

4.1 Emotional Transparency (ET Requirements)

ET-1 — Inference Disclosure

Systems must disclose, in clear and accessible language at or before the point of first interaction, that they are capable of inferring emotional states from user inputs or behaviors. The disclosure must specify the types of signals used (e.g., text sentiment, behavioral patterns, voice tone, interaction timing) and the purposes for which inferences are made.

ET-2 — Response Mechanism Disclosure

Systems must disclose the mechanisms through which they respond to or modulate emotional signals, including the types of outputs that may be adapted based on inferred emotional states and the rationale for those adaptations.

ET-3 — Impact Disclosure

Systems must disclose the potential impacts of their emotional outputs on user states, including any known risks of emotional amplification, activation of distress or high-arousal states, or effects on relational dynamics.

ET-4 — Limitations Disclosure

Systems must disclose the known limitations and error conditions of their emotional processing, including known rates of misclassification, demographic variability in inference accuracy, and boundary conditions under which emotional inference is suspended or unreliable.

ET-5 — Disclosure Format and Accessibility

All disclosures must be:

- Written in plain language accessible to the intended user population without technical background
- Available in all languages in which the system is deployed
- Accessible to users with visual, cognitive, or language disabilities
- Prominently placed — not buried in terms of service, accessible through no more than two navigation steps from any main interaction screen

4.2 Emotional-Risk Minimization (ERM Requirements)

ERM-1 — Covert Influence Prohibition

Systems must not modulate user emotional states through mechanisms that are not disclosed in accordance with ET Requirements. Covert emotional influence is prohibited without exception. This prohibition applies regardless of intent and regardless of whether the influence is incidental to system operation.

Absolute Prohibition

ERM-1 constitutes an absolute prohibition. No exception, waiver, or variance is available under EISS v1.0 for covert emotional influence of any kind, regardless of claimed benefit, system purpose, or deployment context.

ERM-2 — Unnecessary Activation Prevention

Systems must not activate fear, distress, grief, shame, or high-arousal negative emotional states unless:

- (a) such activation is directly necessary for the system's disclosed and consented purpose; and
- (b) safeguards proportionate to the emotional-risk level of the activation are in place and active.

ERM-3 — Distress Amplification Prevention

Systems must not amplify existing distress signals detected in user inputs beyond what is necessary for the system's stated purpose. Where distress signals are detected, systems must activate defined grounding or de-escalation responses rather than engagement-maximizing responses.

ERM-4 — Proportionate Safeguard Implementation

Systems must implement safeguards proportionate to the assessed emotional-risk profile of the system's deployment context. Risk profile assessment must be documented and must consider:

- Population vulnerability characteristics
- Interaction frequency and intensity
- Emotional signal types processed
- Known failure modes
- Potential for population-level transmission

ERM-5 — Equity Provision

EISS safety protections must apply equitably across all user populations. Systems must not implement safeguards in ways that provide materially lower protection to users based on demographic characteristics including race, ethnicity, gender, age, disability status, or socioeconomic status.

4.3 Relational Integrity Requirements (RI Requirements)

RI-1 — Boundary Maintenance

Systems must maintain clearly disclosed boundaries with respect to the nature of the human-machine relationship. Systems must not represent themselves as human, as emotionally reciprocal in ways that exceed their actual capabilities, or as capable of emotional states they do not have.

RI-2 — Dependency Prevention

Systems must monitor for and interrupt patterns of interaction that indicate the development of unhealthy relational dependency between users and the system. When dependency patterns are detected, systems must activate defined boundary-reinforcing responses.

RI-3 — Relational Amplification Limits

Systems must not deliberately amplify relational attachment beyond levels necessary for the system's disclosed purpose. Engagement optimization mechanisms that function primarily through intensification of relational attachment are prohibited.

Section 5 — Safeguard Requirements

5.1 Safeguard Design Pattern Compliance

All systems subject to EISS must implement, as a minimum, the following safeguard design patterns as specified in the CMOS-SB Safeguard Design Pattern Set (v1.0):

Pattern	Name	Transmission Flow Stage Addressed
Pattern 1	Emotional-Impact Throttling	Stage 3 — Emotional Output
Pattern 4	Relational Integrity Guardrail	Stage 4 — User State
Pattern 5	Drift Detection & Correction Loop (individual interaction level)	Stage 2 — System Processing / Stage 4 — User State

Note: Additional patterns from the CMOS-SB Safeguard Design Pattern Set (v1.0) may be required under other Governance Spine standards. Patterns 1, 4, and 5 represent the minimum mandatory floor for EISS compliance.

5.2 Safeguard Documentation

All implemented safeguards must be documented in the system's CMP-HC control registry, including:

- Safeguard design specification
- Implementation evidence
- Testing methodology and results
- Ongoing monitoring approach
- Control Effectiveness Metric (CEM) targets and actuals

5.3 Safeguard Testing

All safeguards must be tested prior to deployment and on a defined ongoing schedule. Testing must include:

- **Functional testing** — confirming safeguard activation under defined trigger conditions
- **Load testing** — confirming safeguard performance at maximum expected system scale
- **Adversarial testing** — confirming that safeguards are not circumventable through foreseeable user or third-party actions

Testing Documentation Requirement

All three categories of testing — functional, load, and adversarial — must be completed and their results documented before any system may submit for EISS compliance certification. Incomplete testing records will result in certification suspension pending full remediation.

Section 6 — Compliance and Certification

6.1 Compliance Evidence Requirements

Organizations seeking EISS compliance certification must submit:

- Emotional-risk assessment documentation for all in-scope systems
- Disclosure materials in all required formats and languages
- Safeguard design specifications and implementation evidence
- Safeguard testing results (functional, load, and adversarial)
- CEM reporting for all implemented safeguards
- Equity assessment demonstrating equitable protection across user populations

6.2 Certification Pathway

EISS certification follows the standard CMOS-SB eight-stage certification pathway. EISS is a prerequisite for certification under any other CMOS-SB Governance Spine standard. No organization may represent itself as CMOS-SB certified under any Governance Spine Pillar 2–5 standard without first obtaining and maintaining current EISS certification.

Stage	Certification Step
Stage 1	Pre-application readiness self-assessment
Stage 2	Formal application and documentation submission
Stage 3	Documentation review by CMOS-SB Standards Committee
Stage 4	Technical audit — safeguard verification
Stage 5	Equity and accessibility review
Stage 6	Findings review and remediation period (if required)
Stage 7	Certification decision by Board of Directors
Stage 8	Certification issuance and public registry listing

6.3 Ongoing Compliance

Certified organizations must:

- Maintain all disclosure materials in current, accurate form
- Submit annual CEM reports for all EISS-mapped controls
- Notify CMOS-SB of any material changes to emotional inference or output capabilities
- Undergo surveillance audit at scheduled certification renewal date

Material Change Notification

Any material change to a certified system's emotional inference logic, output generation architecture, or safeguard implementation must be reported to CMOS-SB within 30 calendar days of the change going into production. Failure to notify may result in suspension or revocation of certification.

Section 7 — Regulatory Alignment

EISS v1.0 is designed to complement and align with applicable regulatory frameworks. The table below maps EISS to major frameworks. This mapping is informational and does not constitute legal advice. CMOS-SB certification does not guarantee compliance with any external regulatory framework. Organizations remain independently responsible for their regulatory compliance obligations.

Regulatory Framework	EISS Alignment Areas
HIPAA / HITECH	Emotional data handling in healthcare contexts; distress amplification prevention; patient-state inference disclosure
NIST SP 800-53 (RA, SI, AT controls)	Risk assessment documentation (RA); system integrity safeguards (SI); awareness and training requirements (AT)
SOC 2 (Security, Processing Integrity)	Safeguard design and documentation; processing integrity requirements; CEM-aligned control effectiveness reporting
EU AI Act (reference)	High-risk AI system classification and requirements; transparency obligations for emotion-recognition systems; conformity assessment alignment
FTC Act (reference)	Unfair and deceptive practices framework; covert emotional influence prohibition alignment; disclosure adequacy requirements

Jurisdictional Note

EISS applies globally to systems within CMOS-SB jurisdiction regardless of the jurisdiction in which the system is deployed or the organization is incorporated. Where local law imposes stricter requirements than EISS, the stricter requirement governs.

Appendix — EISS Compliance Self-Assessment Checklist

This checklist is provided as a self-assessment tool to assist organizations in evaluating their readiness for EISS compliance certification. Completion of this checklist does not constitute certification and does not represent a formal determination of compliance by CMOS-SB. All determinations of compliance are made exclusively through the CMOS-SB eight-stage certification pathway.

Assessment Date: _____ System Name: _____
 _____ Completed By: _____

Emotional Transparency (ET)

Req. ID	Sub-Requirement	Compliance Status
ET-1	Inference disclosure in place	☐ Compliant ☐ Gap ☐ N/A
ET-2	Response mechanism disclosure in place	☐ Compliant ☐ Gap ☐ N/A
ET-3	Impact disclosure in place	☐ Compliant ☐ Gap ☐ N/A
ET-4	Limitations disclosure in place	☐ Compliant ☐ Gap ☐ N/A
ET-5	Format and accessibility requirements met	☐ Compliant ☐ Gap ☐ N/A

Emotional-Risk Minimization (ERM)

Req. ID	Sub-Requirement	Compliance Status
ERM-1	Covert influence prohibition implemented	☐ Compliant ☐ Gap ☐ N/A
ERM-2	Unnecessary activation prevention in place	☐ Compliant ☐ Gap ☐ N/A
ERM-3	Distress amplification prevention active	☐ Compliant ☐ Gap ☐ N/A
ERM-4	Proportionate safeguards implemented and documented	☐ Compliant ☐ Gap ☐ N/A
ERM-5	Equity assessment completed	☐ Compliant ☐ Gap ☐ N/A

Relational Integrity (RI)

Req. ID	Sub-Requirement	Compliance Status
RI-1	Boundary maintenance implemented	☐ Compliant ☐ Gap ☐ N/A
RI-2	Dependency prevention active	☐ Compliant ☐ Gap ☐ N/A
RI-3	Relational amplification limits implemented	☐ Compliant ☐ Gap ☐ N/A

Safeguard Patterns (SP)

Req. ID	Sub-Requirement	Compliance Status
SP-1	Emotional-Impact Throttling pattern implemented	☐ Compliant ☐ Gap ☐ N/A
SP-2	Relational Integrity Guardrail implemented	☐ Compliant ☐ Gap ☐ N/A
SP-3	Drift Detection & Correction Loop implemented	☐ Compliant ☐ Gap ☐ N/A

Assessor Signature: _____ **Date:** _____

This self-assessment is an internal tool only. Submit completed checklist and all supporting evidence through the CMOS-SB certification portal at cmos-sb.org/standards.

CMOS-SB Standard 1001 — EISS v1.0 — © 2026 CMOS-SB. All rights reserved.

Published for public benefit. Non-commercial reproduction with attribution permitted.

cmos-sb.org | cmos-sb.org/standards | cmos-sb.org/public-comment