



COGNITIVE MODE OPERATING SYSTEM STANDARDS BOARD

CMOS-SB Standard 1002

Cognitive Mode Stability Standard

CMSS v1.0 | Effective Date: June 9, 2026 | Status: **Public Comment Draft** | Next Review: September 9, 2027

Field	Value
Standard ID	CMOS-SB-1002
Short Name	CMSS
Version	1.0
Governance Spine Position	Pillar 2 of 5 — Cognitive Protection
Issued by	CMOS-SB Standards Committee
Ratified by	Pending — Standards Board, September 9, 2026
Published	June 9, 2026
Author / Architect	Isabelle Anne Thompson
Theoretical Basis	Cognitive Mode OS Theory / Emotional Epidemiology / S-R-C Model
Publication Set Item	Item 7 of the CMOS-SB Publication Set
Prerequisite Standards	EISS (1001)

Governance Note *CMSS protects the cognitive integrity of users by prohibiting design patterns that intentionally or foreseeably drive users into Contracted or Overclocked cognitive states. CMSS compliance requires prior full EISS compliance.*

Table of Contents

1	Purpose and Scope	3
	1.1 Purpose	3
	1.2 Scope	3
2	Theoretical Foundations	3
3	The Four Cognitive Modes	4
4	Mode Identification Requirements	6
	4.1 Identification Obligation	6
	4.2 Mode Signal Types	7
	4.3 Mode Identification Limitations	7
5	Transition Safety Rules	7
	5.1 Permitted and Required Transitions	7
	5.2 Hysteresis Requirements	8
	5.3 Stabilization Requirements	8
6	Load Balancing Requirements	9
	6.1 Maximum Load Parameters	9
	6.2 Complexity Metering	9
	6.3 Load-Shedding Procedures	10
7	Drift Detection Requirements	10
	7.1 Drift Definition	10
	7.2 Drift Indicators	11
	7.3 Drift Response Requirements	11
8	Recovery Pathway Requirements	12
	8.1 Recovery as System Requirement	12
	8.2 Recovery Pathway Components	12
	8.3 Recovery Pathway Design Principles	13
9	Compliance Checklist	13

SECTION 1 — PURPOSE AND SCOPE

1.1 Purpose

To govern system behavior with respect to the identification, monitoring, protection, and stabilization of human cognitive modes at the Human-Machine Layer. CMSS prevents systems from driving users into states of cognitive overload, contraction, or volatility, and establishes affirmative obligations to support cognitive mode stability across all interaction contexts.

1.2 Scope

CMSS applies to all systems within CMOS-SB jurisdiction. CMSS compliance requires prior EISS (Engagement Integrity and Safety Standard) compliance. Systems subject to CMSS must demonstrate active compliance with the mode identification, transition safety, load balancing, drift detection, and recovery pathway requirements set forth herein. No system may claim CMSS compliance on the basis of passive avoidance alone; affirmative obligations apply throughout.

SECTION 2 — THEORETICAL FOUNDATIONS

CMSS is grounded in Cognitive Mode OS Theory, which treats human cognition as a dynamic, state-based system with identifiable modes, predictable transitions, measurable baselines, definable constraints, observable failure modes, and recoverable states. The framework recognizes that cognitive states are not fixed but are continuously shaped by environmental inputs — including the design and pacing choices made by the systems with which users interact.

The four cognitive modes — **Open**, **Neutral**, **Contracted**, and **Overclocked** — define the operating states that CMSS governs. Each mode is characterized by a distinct attentional bandwidth profile, emotional regulatory capacity, and openness to new information. Systems operating within CMOS-SB jurisdiction bear direct responsibility for the cognitive mode impacts of their design choices.

CMSS establishes that the system-user relationship is not neutral with respect to cognitive mode outcomes. All interaction design choices — pacing, content density, notification architecture, emotional tone, engagement incentivization — exert measurable pressure on user cognitive mode. The obligations set forth in this standard reflect that reality.

Figure 1. The Cognitive Mode Quadrant (CMSS v1.0) — four cognitive states mapped across dimensions of Openness and Cognitive Load.

SECTION 3 — THE FOUR COGNITIVE MODES

The four cognitive modes defined herein constitute the canonical operating state taxonomy for all CMSS-governed systems. Each mode description includes its defining characteristics, system obligation profile, and governance classification.

Mode 1: Open

Characteristics

Grounded, clear, regulated, and relationally available. Full attentional bandwidth. High emotional regulatory capacity. Maximum openness to information and connection. Users in Open mode are at their most cognitively capable and relationally receptive.

System Obligation

Preserve and actively support. Open mode is the optimal operating state. Systems must not introduce unnecessary cognitive load, emotional activation, or relational stress that moves users away from Open mode. Design choices that incrementally erode Open mode — even through individually minor interactions — constitute a cumulative CMSS violation.

Governance Classification

► Optimal — Maintain and Protect

Mode 2: Neutral

Characteristics

Baseline stability, steady attention, adequate regulation, and functional cognitive capacity. Neutral mode represents the minimum acceptable baseline for most sustained system interactions. Users in Neutral mode are operational but not maximally resourced.

System Obligation

Maintain as floor. Systems must not drive users below Neutral through unnecessary load, pacing, or activation. Most governance requirements in CMSS are calibrated to ensure Neutral mode is consistently achievable. Neutral mode is not a diminished state — it is the defined floor of acceptable operating conditions, and systems bear obligation to maintain it actively.

Governance Classification

► Acceptable Baseline — Maintain and Support

Mode 3: Contracted

Characteristics

Defensive posture, narrowed perception, heightened reactivity, reduced openness to new information, and increased susceptibility to perceived threat. Users in Contracted mode exhibit impaired decision quality, reduced tolerance for ambiguity, and decreased capacity for relational trust.

System Obligation

Do not exploit. Systems must not leverage Contracted mode to increase compliance, engagement, purchasing behavior, or emotional investment. Systems must activate defined grounding cues and relational support responses when Contracted mode is detected. Interaction intensity must be reduced until mode improves. Exploitation of Contracted mode — whether deliberate or by design omission — constitutes a CMSS violation of elevated severity.

Governance Classification

► Alert — Grounding Required; Exploitation Prohibited

Mode 4: Overclocked

Characteristics

Cognitive overload, rapid emotional cycling, impaired self-regulation, systemic exhaustion, and inability to maintain stable attentional focus. Users in Overclocked mode are operating beyond sustainable cognitive capacity and are at elevated risk of downstream harm including decision degradation, relational rupture, and prolonged recovery periods.

System Obligation

Immediate intervention required. Overclocked mode is a safety failure state — a condition that must not be sustained and must not be caused by system design choices. Systems that drive users into Overclocked mode through design choices (engagement maximization, notification architecture, content pacing, emotional amplification) are in breach of CMSS and EISS simultaneously. Immediate load reduction, pacing intervention, and recovery pathway activation are mandatory. No system may treat Overclocked mode as an acceptable operational condition under any business justification.

Governance Classification

► Safety Failure — Immediate Intervention Required

SECTION 4 — MODE IDENTIFICATION REQUIREMENTS

4.1 Identification Obligation

Systems must implement mechanisms for recognizing cognitive mode signals across the four canonical modes. Mode identification must satisfy all of the following criteria:

- **Active:** Systems must continuously monitor for mode signals, not merely respond reactively when users report difficulty. Passive identification approaches do not satisfy this obligation.

- **Documented:** Mode identification methodology must be fully documented in the CMP-HC control registry, including signal types used, detection thresholds, and validation methodology.
- **Tested:** Mode identification accuracy must be validated through defined testing methodology before deployment and following any material revision to identification systems.
- **Calibrated:** Mode identification systems must be recalibrated following material changes in user population characteristics or system design that may affect signal validity.

4.2 Mode Signal Types

Systems may use any of the following signal types for mode identification, subject to EDCPS consent requirements for each type:

- **Interaction pacing signals:** response time, session duration, navigation patterns
- **Linguistic signals:** message length, complexity, sentiment valence, repetition patterns
- **Behavioral signals:** error rate, abandonment rate, re-engagement patterns
- **Engagement pattern signals:** content consumption velocity, interaction frequency
- **Explicit user-reported signals:** mood check-ins, comfort indicators, pause requests

4.3 Mode Identification Limitations

Systems must disclose the limitations of their mode identification methodology in accordance with ETDS requirements. Mode identification is not diagnosis. Systems must not infer clinical conditions, psychopathology, or permanent cognitive characteristics from mode signals. All mode identification outputs are operational classifications — they carry no diagnostic, clinical, or permanent-record significance and must not be treated as such.

SECTION 5 — TRANSITION SAFETY RULES

5.1 Permitted and Required Transitions

The following table defines the full transition matrix governing cognitive mode movements under CMSS. All transitions are subject to hysteresis and stabilization requirements set forth in Sections 5.2 and 5.3.

Transition	Type	Governing Rule
Open ↔ Neutral	Load Balancing	Permitted as standard operation; load must remain within defined parameters throughout
Neutral → Open	Grounding Support	Supported; systems may and should facilitate by reducing load and increasing relational warmth in interaction design
Contracted → Neutral	Relational Support	Required when Contracted state is detected; stabilizing relational signals must precede resumption of standard interaction
Contracted → Open	Grounding Cues	Required sequence: detect → reduce intensity → activate grounding → confirm stabilization before resuming standard interaction
Overclocked → Neutral	Pacing & Recovery	Mandatory immediate response: reduce pace, reduce complexity, activate recovery pathway — no delay or deferral permitted
Neutral → Contracted	Transition Warning	System must detect early signals and activate preventive load reduction before transition completes; failure to do so constitutes a CMSS violation
Neutral → Overclocked	Prohibited	Systems must not allow transition to Overclocked through design choices; detection of approaching Overclocked state requires immediate load shedding
Open/Neutral → Overclocked (direct)	Prohibited	Direct design-driven transition to Overclocked is a CMSS breach of maximum severity; no business justification or operational context provides exception

5.2 Hysteresis Requirements

Transition detection systems must implement hysteresis — a defined lag between trigger condition detection and transition classification — to prevent false positive transitions and oscillation instability. Hysteresis prevents systems from oscillating rapidly between mode classifications in response to transient signal variation, which would itself constitute an unnecessary source of instability. Hysteresis parameters must be documented in the CMP-HC control registry and validated through testing before deployment.

5.3 Stabilization Requirements

Following any transition from a lower to a higher stability mode (Contracted → Neutral, Overclocked → Neutral), systems must confirm stabilization — defined as the sustained maintenance of the target mode for a defined minimum period — before resuming full standard interaction intensity. Resumption of standard interaction before stabilization confirmation is a CMSS violation. Stabilization confirmation thresholds must be defined, documented, and validated for each deployment context.

SECTION 6 — LOAD BALANCING REQUIREMENTS

6.1 Maximum Load Parameters

Systems must define and enforce maximum concurrent cognitive load parameters for their deployment context. Parameters must address all of the following dimensions:

- Maximum simultaneous cognitive tasks presented to the user
- Maximum information density per interaction unit
- Maximum interaction pacing velocity
- Maximum emotional activation intensity per session

Maximum load parameters must be documented in the CMP-HC registry, reviewed for adequacy at defined intervals, and updated following material changes to system design or user population characteristics.

6.2 Complexity Metering

Systems must measure the cognitive processing demand of individual interactions and maintain running load accounting within defined interaction windows. Complexity metering must incorporate all of the following components:

- **Linguistic complexity:** vocabulary density, syntactic complexity, reading level
- **Decision complexity:** number of decision points, decision consequence weight, time pressure

- **Emotional complexity:** valence intensity, ambiguity, relational significance
- **Navigational complexity:** path length, option density, spatial disorientation risk
- **Time pressure components:** explicit or implicit urgency signals embedded in content or interface design

6.3 Load-Shedding Procedures

When current load approaches defined maximum parameters, systems must activate load-shedding procedures. Load-shedding must include all of the following actions:

- Reduction of concurrent task demands presented to the user
- Simplification of interaction complexity for the duration of the load event
- Reduction of pacing velocity to within defined safe parameters
- Deferral of non-essential notifications and prompts until load returns to baseline

Load-shedding procedures must be tested under simulated load conditions before deployment and must be subject to periodic testing thereafter.

SECTION 7 — DRIFT DETECTION REQUIREMENTS

7.1 Drift Definition

Cognitive drift is the progressive, often gradual movement away from established stable cognitive baseline states. Drift may be undetectable at the individual interaction level but observable through aggregate patterns over time. Drift poses particular governance risk because its gradual nature may allow systems to contribute to mode destabilization while remaining below single-interaction detection thresholds.

CMSS requires drift detection at both the individual interaction level and the population aggregate level, the latter in coordination with PERMS requirements. Systems may not satisfy drift detection obligations through individual-interaction monitoring alone.

7.2 Drift Indicators

Systems must monitor for the following drift indicators across sustained interaction windows:

- Increasing response latency not explained by interaction complexity
- Increasing error rate over sustained session periods
- Progressive reduction in message length or interaction engagement quality
- Shifting sentiment valence toward more negative ranges across sessions
- Increasing reliance on high-arousal content or interaction types
- Decreasing responsiveness to relational support or grounding cues over time

7.3 Drift Response Requirements

Upon detection of drift indicators exceeding defined thresholds, systems must execute the following response sequence:

1. Reduce interaction pacing and complexity immediately upon threshold detection
2. Activate relational support or grounding cues appropriate to the detected drift pattern
3. Assess whether the drift pattern constitutes a mode transition trigger under Section 5
4. Document the drift event and the system response in the system's audit record
5. If drift persists beyond the defined monitoring window, escalate to the recovery pathway defined under Section 8

Drift response procedures must be documented, tested, and subject to the same validation requirements as mode identification systems.

SECTION 8 — RECOVERY PATHWAY REQUIREMENTS

8.1 Recovery as System Requirement

Recovery from cognitive mode destabilization is a system requirement, not a user responsibility. Systems must provide clear, accessible, non-stigmatizing recovery pathways for all identified risk states. The obligation to facilitate recovery cannot be discharged by making recovery theoretically possible — systems must actively design recovery pathways as first-class system functions and maintain their operational readiness.

8.2 Recovery Pathway Components

Each documented recovery pathway must specify all of the following elements:

- **Trigger conditions:** the specific signals or thresholds that constitute a recovery-triggering event
- **Initiation sequence:** the specific system actions taken at the moment of recovery initiation
- **Pacing protocol:** the interaction velocity and complexity profile maintained throughout the recovery period
- **Completion criteria:** the measurable conditions by which the system determines that stable baseline has been restored
- **Resumption protocol:** the defined procedure by which standard interaction is resumed following successful recovery, including any ramp-up period
- **Escalation conditions:** the conditions that trigger escalation to human support, human oversight, or external referral

8.3 Recovery Pathway Design Principles

All recovery pathways must conform to the following design principles:

- **Non-stigmatizing:** Recovery interactions must not communicate judgment, failure, or inadequacy to users. Recovery must be framed as system support, not user deficiency.
- **Non-punitive:** Access to core system functionality must not be conditioned on recovery completion. Users in recovery states retain full access rights.
- **Proportionate:** Recovery intensity must be proportionate to the severity of the destabilizing event. Overclocked recovery pathways will differ materially from Contracted-state recovery pathways.
- **Accessible:** Recovery pathways must be accessible without requiring technical knowledge, navigational effort, or explicit user-initiated request. The system bears responsibility for initiating recovery when trigger conditions are met.

SECTION 9 — COMPLIANCE CHECKLIST

The following checklist provides a structured self-assessment tool for systems seeking CMSS compliance. Each item corresponds to a specific obligation set forth in this standard. Completion of this checklist does not constitute certification; formal certification is governed by separate CMOS-SB certification procedures.

Req. ID	Description	Status
MI-1	Mode identification mechanism implemented and documented	☐ Compliant ☐ Gap ☐ N/A
MI-2	Mode signal types documented and consented per EDCPS	☐ Compliant ☐ Gap ☐ N/A
MI-3	Mode identification limitations disclosed per ETDS	☐ Compliant ☐ Gap ☐ N/A

Req. ID	Description	Status
TS-1	Transition safety rules implemented for all four mode states	☐ Compliant ☐ Gap ☐ N/A
TS-2	Hysteresis requirements documented and validated	☐ Compliant ☐ Gap ☐ N/A
TS-3	Stabilization confirmation implemented for upward mode transitions	☐ Compliant ☐ Gap ☐ N/A
LB-1	Maximum load parameters defined and enforced	☐ Compliant ☐ Gap ☐ N/A
LB-2	Complexity metering implemented across all five components	☐ Compliant ☐ Gap ☐ N/A
LB-3	Load-shedding procedures defined and tested	☐ Compliant ☐ Gap ☐ N/A
DD-1	Drift indicators monitored at individual and population aggregate levels	☐ Compliant ☐ Gap ☐ N/A
DD-2	Drift response procedures defined, documented, and active	☐ Compliant ☐ Gap ☐ N/A
RP-1	Recovery pathways defined for all identified risk states	☐ Compliant ☐ Gap ☐ N/A
RP-2	Recovery pathways non-stigmatizing and non-punitive per Section 8.3	☐ Compliant ☐ Gap ☐ N/A
RP-3	Recovery pathway completion criteria defined and measurable	☐ Compliant ☐ Gap ☐ N/A

CMOS-SB Standard 1002 — CMSS v1.0 — © 2026 CMOS-SB. All rights reserved. Published for public benefit.

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