



COGNITIVE MODE OPERATING SYSTEM STANDARDS BOARD

CMOS-SB Standard 1005

Population-Level Emotional Risk Monitoring Standard

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

Field	Value
Standard ID	CMOS-SB-1005
Short Name	PERMS
Version	1.0
Governance Spine Position	Pillar 5 of 5 — Population-Level Risk
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	Cognitive Mode OS Theory / Emotional Epidemiology / S-R-C Model
Publication Set Item	Item 10 of the CMOS-SB Publication Set
Prerequisite Standards	EISS (1001) / CMSS (1002) / ETDS (1003) / EDCPS (1004)

Governance Note *PERMS is the fifth and final pillar of the CMOS-SB Governance Spine. It operationalizes Emotional Epidemiology at the governance layer, extending individual-level protections established in Standards 1001–1004 to the population level. PERMS compliance requires prior full compliance with all four predecessor standards.*

Cognitive Mode OS™ is a trademark of Isabelle Anne Thompson / Sugar Sands Publishing LLC. All rights reserved.

Table of Contents

1.	Purpose and Scope
1.1	Purpose
1.2	Scope
2.	Theoretical Foundations
2.1	Emotional Epidemiology and the S-R-C Model
2.2	Three Population-Level Risk Dynamics
3.	Population-Level Monitoring Architecture
3.1	Required Monitoring Infrastructure
3.2	Standard-Scale Systems (1,000–999,999 Users)
3.3	Large-Scale Systems (1,000,000+ Users)
4.	Baseline Establishment Requirements
4.1	Baseline Measurement
4.2	Baseline Components
4.3	Baseline Refresh
5.	Anomaly Detection Standards
5.1	Definition of Anomaly
5.2	Detection Requirements
5.3	Detection Windows
6.	Contagion and Drift Surveillance Requirements
6.1	Contagion Surveillance
6.2	Drift Surveillance
6.3	Cascade Risk Monitoring
7.	Alert Thresholds and Escalation Protocols
7.1	Level 1 Alert — Advisory
7.2	Level 2 Alert — Elevated Risk

1.	Purpose and Scope
7.3	Level 3 Alert — Critical
8.	Reporting Requirements
8.1	Internal Reporting
8.2	CMOS-SB Reporting
8.3	Public Reporting
8.4	Report Format Standards
9.	Remediation Obligations
9.1	Remediation Duty
9.2	Remediation Measures
9.3	Remediation Verification
10.	Data Governance for Population Monitoring Data
11.	Compliance Checklist

Section 1 — Purpose and Scope

1.1 Purpose

The Population-Level Emotional Risk Monitoring Standard (PERMS) is established by the Cognitive Mode Operating System Standards Board (CMOS-SB) to create binding requirements for the monitoring, detection, reporting, and remediation of population-level emotional risk events. For the purposes of this standard, a **population-level emotional risk event** is defined as any measurable pattern of emotional state degradation, cognitive mode instability, emotional contagion, or collective resilience failure that emerges across groups of users interacting with systems subject to CMOS-SB jurisdiction.

PERMS operationalizes the principles of Emotional Epidemiology at the governance layer. It extends the individual-level protections established under Standards 1001–1004 to the level of the population, requiring systems to treat population-level emotional outcomes as a core operational responsibility rather than an incidental or externalized consequence of system design and operation.

The animating principle of PERMS is that systems which interact with large populations of users at scale bear a proportional responsibility for the aggregate emotional health of those populations. Individual-level harm protections, while necessary, are insufficient when system design choices — including algorithmic amplification, content sequencing, notification architecture, and engagement optimization — produce emergent population-level effects that no individual-level monitoring system would detect in isolation. PERMS closes this governance gap.

Foundational Principle

Systems at scale function as emotional infrastructure. PERMS requires that this infrastructure be monitored with the same rigor applied to any critical operational system — with defined baselines, anomaly detection, escalation protocols, and mandatory remediation.

1.2 Scope

PERMS applies to all systems within CMOS-SB jurisdiction that serve active user populations of **1,000 or more users** at the time of assessment or at any point during a compliance cycle. Jurisdiction thresholds and applicability determinations shall be made in accordance with CMOS-SB jurisdictional guidance in force at the time of compliance review.

Full PERMS compliance requires prior demonstrated compliance with the following predecessor standards:

- **CMOS-SB Standard 1001 — EISS** (Emotional Impact Safety Standard)
- **CMOS-SB Standard 1002 — CMSS** (Cognitive Mode Safety Standard)
- **CMOS-SB Standard 1003 — ETDS** (Emotional Transmission Design Standard)
- **CMOS-SB Standard 1004 — EDCPS** (Emotional Data Collection and Protection Standard)

Systems that have not achieved compliance with all four predecessor standards are not eligible for PERMS certification. CMOS-SB may, at its discretion, grant provisional PERMS monitoring status to systems actively pursuing predecessor compliance, subject to enhanced reporting requirements during the provisional period.

Systems serving fewer than 1,000 users are encouraged to implement PERMS voluntarily and may seek voluntary PERMS recognition from CMOS-SB upon request.

Systems serving populations of **1,000,000 or more users** are subject to enhanced PERMS obligations as specified in Section 3.3 of this standard, including continuous real-time monitoring, automated anomaly detection with sub-24-hour alert capability, monthly internal reporting, and mandatory public annual disclosure.

Population Tier	PERMS Obligation Level	Key Distinguishing Requirements
Fewer than 1,000 users	Voluntary	Voluntary implementation; no mandatory compliance obligations
1,000–999,999 users	Standard-Scale PERMS	Baseline monitoring; anomaly detection; quarterly reporting
1,000,000+ users	Large-Scale Enhanced PERMS	Real-time monitoring; automated detection; monthly + public annual reporting; cascade risk modeling

Section 2 — Theoretical Foundations

2.1 Emotional Epidemiology and the S-R-C Model

PERMS is grounded in the theoretical framework of **Emotional Epidemiology**, as developed within Cognitive Mode OS Theory. Emotional Epidemiology applies the conceptual and analytical apparatus of population-level health science to the study of emotional state propagation, cognitive mode distribution, and resilience dynamics across user populations. Just as traditional epidemiology studies the spread, concentration, and mitigation of physical disease across populations, Emotional Epidemiology studies the spread, concentration, and mitigation of emotional states, cognitive mode patterns, and resilience vulnerabilities across socially connected human systems.

The foundational analytical model underlying PERMS is the **Susceptibility-Response-Contagion (S-R-C) Model**. The S-R-C Model describes the three-variable dynamic that governs population-level emotional risk:

- **Susceptibility (S)** — the degree to which individuals within a population are vulnerable to adverse emotional state changes, as influenced by baseline cognitive mode, prior emotional

history, unmet core needs, and current life context. Susceptibility is not static; it is continuously shaped by system interactions and external events.

- **Response (R)** — the nature, intensity, and direction of the emotional state change that occurs when a susceptible individual encounters an emotional stimulus, whether that stimulus originates from content, social signals, system design patterns, or real-world events.
- **Contagion (C)** — the process by which emotional states and cognitive modes propagate from individual to individual across social and system-mediated connections, potentially amplifying or attenuating as they travel through the population network.

PERMS requires systems to monitor all three S-R-C variables at the population level on a continuous basis. No single variable is sufficient in isolation: a population of low-susceptibility users may tolerate high contagion pressure without significant harm, while a population of high-susceptibility users may experience population-level harm even under conditions of low inherent contagion pressure.

2.2 Three Population-Level Risk Dynamics

PERMS identifies three specific population-level risk dynamics that systems must govern under this standard. These dynamics are not mutually exclusive and may co-occur or interact to produce compounding risk conditions.

2.2.1 Susceptibility Aggregation

Susceptibility Aggregation occurs when a system's user population exhibits a measurably elevated average Susceptibility Index relative to established baselines. Populations with elevated average susceptibility are at materially heightened risk of emotional contagion events: when a high proportion of users are simultaneously in elevated susceptibility states, even low-intensity emotional stimuli may propagate broadly and rapidly through the population network.

Susceptibility Aggregation can arise from system design choices that disproportionately attract or retain high-susceptibility users, from content patterns that systematically elevate susceptibility over time, or from external events that simultaneously elevate susceptibility across large segments of the user population. All three pathways are governed under PERMS and require monitoring regardless of origin.

2.2.2 Transmission Acceleration

Transmission Acceleration occurs when system design choices increase the effective rate at which emotional signals propagate through the user population. Design choices that can drive Transmission

Acceleration include, but are not limited to: algorithmic amplification of high-emotional-valence content; notification density and urgency patterns that increase user responsiveness to social emotional signals; engagement optimization strategies that favor emotionally activating content; and social graph structures that create high-density emotional transmission pathways between user clusters.

Critically, Transmission Acceleration can drive population-level emotional drift even in the absence of any individual-level harm trigger. A system may be fully compliant at the individual interaction level — no single interaction crossing any individual harm threshold — while simultaneously operating in a configuration that drives population-level drift through the cumulative effect of accelerated transmission across millions of users. PERMS exists, in part, to close this governance gap.

2.2.3 Collective Resilience Degradation

Collective Resilience Degradation occurs when the cumulative effect of individual emotional regulation capacity erosion across a population produces a measurable reduction in the population's aggregate capacity to manage future emotional challenges. Resilience is not a fixed trait; it is a dynamic resource that can be replenished or depleted by interaction patterns over time.

Systems that expose users to chronically elevated emotional activation, sustained Contracted or Overclocked mode states, or patterns of interaction that undermine self-regulatory capacity may produce Collective Resilience Degradation even if no acute harm event occurs. Degraded collective resilience increases the population's vulnerability to future contagion events, creating a compounding risk cycle that PERMS is designed to detect and interrupt at the earliest measurable stage.

Governance Rationale

All three risk dynamics — Susceptibility Aggregation, Transmission Acceleration, and Collective Resilience Degradation — may produce population-level harm in the complete absence of any individual-level harm event detectable under Standards 1001–1004. PERMS monitoring is therefore not redundant to predecessor standard compliance; it is structurally necessary to close the governance gap between individual-level and population-level protection.

Section 3 — Population-Level Monitoring Architecture

3.1 Required Monitoring Infrastructure

All PERMS-subject systems must design, implement, and maintain a population-level monitoring infrastructure capable of fulfilling the detection, reporting, and escalation functions required by this standard. The monitoring infrastructure must be operational at all times, subject only to planned maintenance windows not exceeding 4 hours per month, during which compensating monitoring procedures must be in place.

The required monitoring infrastructure must comprise at minimum the following four functional capabilities:

1. **Real-Time Population-State Monitoring Capability** — A continuous measurement function capable of tracking population-level distributions across defined emotional and cognitive mode metrics, producing current-state snapshots at intervals no greater than those specified by the applicable tier requirements (Section 3.2 and 3.3).
2. **Anomaly Detection System** — An automated detection system capable of identifying statistically significant deviations from established population baselines, as defined in Section 5. The anomaly detection system must be capable of detecting both acute spike events and gradual drift patterns, and must operate continuously without requiring manual initiation.
3. **Contagion Surveillance Function** — A capability dedicated to tracking the propagation of emotional signals and cognitive mode states across user population clusters, capable of identifying contagion events as defined in Section 6.1 and reporting propagation patterns for analysis and escalation.
4. **Escalation and Alert System** — A structured alert management function with defined thresholds corresponding to the three-tier alert levels specified in Section 7, capable of triggering internal and external notifications in accordance with the timelines required by this standard.

All four functional capabilities must be documented, version-controlled, and available for audit inspection upon CMOS-SB request. Monitoring infrastructure documentation must include: architecture diagrams, data flow descriptions, methodology statements, calibration records, and maintenance logs.

3.2 Standard-Scale Systems (1,000–999,999 Users)

Systems serving user populations between 1,000 and 999,999 users are classified as **Standard-Scale PERMS Systems** and are subject to the following monitoring architecture requirements:

- All four functional monitoring capabilities specified in Section 3.1 must be implemented and operational.
- Population-state snapshots must be generated at intervals no greater than **72 hours**.
- Anomaly detection must operate on a rolling basis with a maximum detection window of 72 hours (see Section 5.3).
- Contagion surveillance must be capable of detecting propagation events within the 72-hour detection window.
- Quarterly population monitoring summary reports must be prepared and submitted to system leadership and retained for CMOS-SB audit purposes.
- Annual compliance reports must be submitted to CMOS-SB in accordance with Section 8.2.

3.3 Large-Scale Systems (1,000,000+ Users)

Systems serving user populations of 1,000,000 or more users are classified as **Large-Scale Enhanced PERMS Systems** and are subject to the following enhanced monitoring architecture requirements, in addition to all Standard-Scale requirements:

- Population-state monitoring must operate in **continuous real-time**, with snapshot intervals not exceeding **1 hour** for Tier 1 and Tier 2 alert-relevant metrics.
- Anomaly detection must be fully automated with a maximum detection-to-alert window of **24 hours** (see Section 5.3).
- Cascade risk modeling must be implemented and maintained in accordance with Section 6.3.
- Monthly population monitoring summary reports must be prepared and submitted to senior system leadership.
- Annual compliance reports must be submitted to CMOS-SB in accordance with Section 8.2.
- An annual **Population-Level Emotional Impact Report** must be prepared and made publicly available in accordance with Section 8.3.

- Large-Scale Enhanced PERMS Systems must designate a named Population Monitoring Officer with defined accountability for PERMS compliance, reporting, and escalation.

Monitoring Requirement	Standard-Scale (1K–999,999)	Large-Scale Enhanced (1M+)
Real-time monitoring	72-hour snapshot interval	Continuous; 1-hour max interval
Anomaly detection	72-hour detection window	24-hour automated detection window
Contagion surveillance	Required	Required + cascade risk modeling
Internal reporting	Quarterly summary	Monthly summary + immediate alert reports
CMOS-SB reporting	Annual compliance report	Annual compliance report + immediate Level 2/3 notifications
Public disclosure	Not required	Annual Population-Level Emotional Impact Report
Named accountability	Designated monitoring lead recommended	Population Monitoring Officer required

Section 4 — Baseline Establishment Requirements

4.1 Baseline Measurement

All PERMS-subject systems must establish documented population-level emotional state baselines within **90 days** of PERMS implementation or the attainment of the applicable user-population threshold, whichever occurs first. Baselines established under this section serve as the reference standard against which all anomaly detection, contagion surveillance, and drift surveillance functions operate.

Baseline measurement must be conducted using consistent, reproducible, and documented methodologies. The measurement methodology must be recorded in sufficient detail that a qualified independent reviewer could replicate the baseline measurement process and arrive at materially equivalent results. Measurement methodologies must be approved by the system's designated

monitoring lead (Standard-Scale) or Population Monitoring Officer (Large-Scale Enhanced) prior to operationalization.

Systems may not substitute non-comparable historical data for prospective baseline measurement unless CMOS-SB expressly approves the substitution in writing. Where a system possesses historical population-level data that predates formal PERMS implementation, such data may be retained and used for trend analysis purposes but may not serve as the operative compliance baseline without explicit CMOS-SB approval.

4.2 Baseline Components

Population-level baselines must include, at minimum, the following four components, each measured at the population aggregate level:

5. **Mode Distribution Baseline** — The average distribution of users across the four cognitive modes of Cognitive Mode OS Theory: Open Mode, Neutral Mode, Contracted Mode, and Overclocked Mode. The Mode Distribution Baseline must capture both the mean distribution and the standard deviation of distribution, enabling meaningful statistical anomaly detection. Mode Distribution must be disaggregated by user cluster groupings where technically feasible, to enable contagion and drift surveillance at the sub-population level.
6. **Average Susceptibility Index (ASI)** — The population-level average of the individual Susceptibility Index scores as defined in CMOS-SB Standard 1002 (CMSS). The ASI must be computed using a consistent aggregation methodology and recorded with sufficient precision to enable detection of statistically significant shifts over time.
7. **Average Transmission Rate (ATR)** — The average rate at which emotional signals propagate between connected users within the system's population network, measured across representative interaction clusters. The ATR establishes the baseline against which contagion events, as defined in Section 6.1, are detected.
8. **Collective Resilience Score (CRS)** — A composite population-level metric reflecting the aggregate capacity of the user population to process, integrate, and recover from adverse emotional stimuli. The CRS methodology must be documented, consistent with Cognitive Mode OS Theory principles, and applied uniformly across compliance cycles.

Baseline Component	Abbreviation	What It Measures	Risk Dimension
Mode Distribution Baseline	MDB	Distribution across Open / Neutral / Contracted / Overclocked modes	Susceptibility Aggregation
Average Susceptibility Index	ASI	Population-mean susceptibility to adverse emotional state change	Susceptibility Aggregation
Average Transmission Rate	ATR	Rate of emotional signal propagation across user clusters	Transmission Acceleration
Collective Resilience Score	CRS	Aggregate population capacity for emotional recovery	Collective Resilience Degradation

4.3 Baseline Refresh

Population-level baselines established under this section are not permanent reference points. They must be recalibrated under the following conditions:

- **Annual Recalibration** — Baselines must be refreshed at least once per calendar year, regardless of whether any major system change has occurred, to account for natural population evolution and environmental shifts.
- **Major System Change Trigger** — Baselines must be recalibrated within 60 days following the deployment of any major system change that materially affects the features, algorithms, content selection systems, notification architecture, or user population composition that the original baseline was designed to reflect.
- **Post-Anomaly Event Recalibration** — Following any Level 2 or Level 3 alert event, baselines must be reviewed and, where warranted, recalibrated following successful remediation and restoration to normal operating parameters.

Recalibrated baselines must be documented with the date of recalibration, the triggering condition, and a comparison summary identifying material changes from the prior baseline. Historical baselines must be retained for a minimum of 5 years for trend analysis and audit purposes.

Compliance Note

The 90-day baseline establishment window begins upon the earlier of: (a) formal PERMS implementation, or (b) the date on which the system first meets or exceeds the applicable user-population threshold. Systems may not delay baseline establishment by deferring formal PERMS implementation after crossing the applicable threshold.

Section 5 — Anomaly Detection Standards

5.1 Definition of Anomaly

For purposes of this standard, a **population-level emotional anomaly** is defined as a statistically significant deviation from established population baselines in any monitored metric — including the Mode Distribution Baseline, Average Susceptibility Index, Average Transmission Rate, or Collective Resilience Score — that persists for a duration exceeding the applicable detection window defined in Section 5.3.

A deviation is considered statistically significant for PERMS purposes when it meets or exceeds a threshold of **two standard deviations** from the established baseline mean for the relevant metric, sustained over the applicable detection window. Systems may adopt more stringent significance thresholds, and are encouraged to do so where population vulnerability indicators warrant heightened sensitivity. More stringent thresholds adopted voluntarily must be documented and applied consistently across compliance cycles.

The following are specifically designated as anomaly-eligible conditions requiring immediate evaluation under this section:

- A shift of 10 percentage points or more in the proportion of users distributed in Contracted or Overclocked modes relative to the Mode Distribution Baseline.
- An increase in the Average Susceptibility Index of 15% or more relative to the established baseline.
- An increase in the Average Transmission Rate of 20% or more relative to the established baseline, sustained over the detection window.

- A decrease in the Collective Resilience Score of 10% or more relative to the established baseline.

These specific conditions are designated as *presumptive anomalies* and must be treated as anomaly events triggering the evaluation and potential escalation process defined in Section 7, absent documented evidence of a non-system causal explanation that satisfies the external event attribution standard specified in Section 5.2.

5.2 Detection Requirements

The anomaly detection system required by Section 3.1 must satisfy all of the following operational requirements:

9. **Automated Operation** — Anomaly detection must function automatically and continuously, without requiring manual initiation of detection runs. Human review of detected anomalies is required before escalation classification, but detection itself must not depend on human initiation.
10. **Dual Sensitivity** — The detection system must be sensitive to both acute spike events (rapid, high-magnitude deviations occurring within a single detection window) and gradual drift events (slow, cumulative deviations that individually fall below significance thresholds in any single window but represent sustained directional movement over multiple windows). Dual-mode detection must be documented separately in system architecture records.
11. **Causal Attribution Capability** — The detection system must include capability to support distinction between system-driven anomalies (those attributable to system design, content, algorithm, or operational changes) and external event-driven anomalies (those primarily attributable to real-world events such as major news events, natural disasters, or documented societal disruptions). Causal attribution determinations must be documented and are subject to CMOS-SB audit review. Attribution of an anomaly to external events does not relieve the system of monitoring, documentation, or escalation obligations; it affects only the remediation analysis.
12. **Methodological Documentation** — Full detection methodology documentation must be maintained, including: statistical model descriptions, threshold definitions, calibration parameters, version history, and validation records. This documentation must be made available to CMOS-SB within 5 business days of any information request.

5.3 Detection Windows

Detection windows define the maximum sustained duration that a deviation must persist before triggering formal anomaly classification. Detection windows are set by population tier as follows:

Population Tier	Maximum Detection Window	Rationale
Standard-Scale Systems (1,000–999,999 users)	72 hours	Proportionate to monitoring intensity requirement and operational capacity of standard-scale systems
Large-Scale Enhanced Systems (1,000,000+ users)	24 hours	Reflects both the heightened risk potential of large-scale propagation and the enhanced monitoring infrastructure required of large-scale systems

Detection windows represent maximum allowable periods, not targets. Systems are encouraged to configure detection sensitivity to identify anomaly conditions within detection windows shorter than the applicable maximum. Early detection is recognized by CMOS-SB as a compliance best practice indicator and will be reflected in compliance assessments.

Section 6 — Contagion and Drift Surveillance Requirements

6.1 Contagion Surveillance

All PERMS-subject systems must maintain an operational contagion surveillance capability dedicated to the detection of emotional contagion events within their user populations. For the purposes of this standard, an **emotional contagion event** is defined as the measurable propagation of an emotional state or cognitive mode across connected user clusters at a rate that meets or exceeds 120% of the established Average Transmission Rate baseline over the applicable detection window — that is, transmission occurring at a rate at least 20% above the established population norm.

Contagion surveillance must include the following functional elements:

- **Cluster-Level Tracking** — The capability to identify and monitor named or defined user clusters (social connections, shared content networks, notification cohorts, or other functionally

connected groupings) and to track emotional state or mode propagation pathways across cluster boundaries.

- **Propagation Rate Measurement** — Active, ongoing measurement of the rate at which defined emotional signals are propagating through the population network, benchmarked against the ATR baseline established under Section 4.2.
- **Source Identification Support** — Where technically feasible, the capability to trace a detected contagion event backward toward its originating source or content category, to support causal analysis and targeted remediation.
- **Event Documentation** — Systematic recording of all detected contagion events, including onset time, affected clusters, propagation rate, duration, and resolution status, retained for a minimum of 3 years for audit and trend analysis purposes.

Key Distinction

Contagion events differ from anomaly events in that they specifically concern the *propagation mechanism* — the pathway by which emotional states spread across users — rather than the aggregate population-level metric deviation. A contagion event may or may not coincide with a statistical anomaly. Both surveillance functions are required independently and serve complementary governance purposes.

6.2 Drift Surveillance

All PERMS-subject systems must maintain an operational drift surveillance capability capable of detecting emotional drift — defined as gradual, cumulative movement of population-level emotional state in a negative direction (toward Contracted or Overclocked modes, declining Collective Resilience Score, or rising Average Susceptibility Index) that does not trigger acute anomaly thresholds in any single detection window but represents sustained population-level degradation over multiple detection cycles.

Emotional drift is among the most governance-significant population-level risk conditions precisely because of its gradual nature. Drift may persist for weeks or months before producing an acute anomaly event, and systems that monitor only for acute anomalies may permit sustained drift to reach advanced stages before detection. PERMS requires dedicated drift surveillance to close this gap.

Drift surveillance requirements include:

- **Multi-Window Trend Analysis** — Automated analysis of metric trajectories across a rolling window of no fewer than 8 consecutive detection cycles, capable of identifying directional trends even where no individual cycle produces a significant deviation from baseline.
- **Drift Threshold Definition** — Documented drift detection thresholds, expressed as cumulative directional movement across the rolling analysis window, beyond which a drift alert is generated for internal review. Drift thresholds must be established at a level sensitive enough to identify meaningful population-level degradation trajectories before they produce acute anomaly conditions.
- **Drift Event Documentation** — All detected drift events must be documented with the same rigor required for contagion events, including onset trajectory, affected metrics, magnitude of cumulative movement, and remediation outcome.

6.3 Cascade Risk Monitoring

Large-Scale Enhanced PERMS Systems (1,000,000+ users) must implement and maintain an active **cascade risk modeling** function in addition to the contagion and drift surveillance requirements applicable to all PERMS-subject systems. Cascade risk modeling is defined as the ongoing analytical capability to identify conditions under which a localized emotional anomaly or contagion event could propagate through the population network to affect a materially larger population segment.

Cascade risk modeling must include:

- **Network Topology Analysis** — Maintained current-state mapping of the social and content-sharing network topology across the user population, sufficient to identify high-connectivity nodes and clusters that present elevated cascade propagation risk.
- **Scenario Stress Testing** — Periodic (at minimum quarterly) simulation or analytical stress-testing of cascade propagation risk under defined adverse scenarios, using current population baseline data and network topology maps.
- **Pre-Emptive Risk Flagging** — The capability to flag elevated cascade risk conditions before a cascade event occurs, based on the concurrent presence of defined risk factors (e.g., elevated

ASI + high network density + rising ATR), triggering heightened monitoring posture as specified in the Level 1 Alert protocol of Section 7.1.

Section 7 — Alert Thresholds and Escalation Protocols

PERMS establishes a three-tier alert system to govern the escalation of detected anomaly, contagion, and drift events. Each tier carries defined trigger conditions, notification requirements, and response obligations. All PERMS-subject systems must implement all three alert tiers as part of the escalation and alert system required by Section 3.1.

Alert tier classifications are assigned by the system's designated monitoring lead or Population Monitoring Officer upon detection of a qualifying condition. Tier classification decisions must be documented in writing at the time of classification, including the factual basis for the assigned tier and any alternative tier considered and rejected.

Alert Tier	Trigger Condition	Key Obligations	External Reporting
Level 1 — Advisory	Metrics approaching defined threshold; elevated cascade risk flagged; early drift trajectory detected	Internal team notification; enhanced monitoring posture	None required
Level 2 — Elevated Risk	Metrics breach defined threshold; confirmed anomaly, contagion, or drift event	Senior leadership notification; remediation assessment initiated	CMOS-SB notification within 72 hours
Level 3 — Critical	Sustained or severe breach; cascade event in progress; multiple concurrent breaches	Immediate remediation action; user notification if directly affected	CMOS-SB within 4 hours; public disclosure within 24 hours

7.1 Level 1 Alert — Advisory

A **Level 1 Alert (Advisory)** is issued when monitored metrics approach defined alert thresholds without yet breaching them, when an early drift trajectory is detected in drift surveillance analysis, or when cascade risk monitoring flags an elevated pre-event risk condition. A Level 1 Alert signals the need for

heightened operational vigilance and enhanced monitoring without yet indicating that a confirmed population-level harm event is underway.

Level 1 Alert obligations include:

- Immediate notification to the system's internal monitoring team and designated monitoring lead or Population Monitoring Officer.
- Enhancement of monitoring intensity, including reduction of detection window intervals where operationally feasible.
- Documentation of the Level 1 trigger condition, the current metric readings, the distance from threshold breach, and the planned monitoring response.
- Initiation of a Level 1 watch period: a defined period of heightened monitoring during which the developing condition is tracked to resolution (de-escalation) or escalation to Level 2.

No mandatory external reporting to CMOS-SB or public disclosure is required at Level 1. However, systems that subsequently escalate to Level 2 or Level 3 are required to include the Level 1 advisory record in the Level 2 or Level 3 notification to CMOS-SB, to establish the full event timeline.

7.2 Level 2 Alert — Elevated Risk

A **Level 2 Alert (Elevated Risk)** is issued when a monitored metric breaches its defined detection threshold, confirming a population-level anomaly, contagion event, or sustained drift condition. Level 2 represents a confirmed population-level risk event in progress and triggers mandatory escalation, disclosure, and remediation obligations.

Level 2 Alert obligations include:

- Immediate notification to senior system leadership, including at minimum the system's executive lead and, where applicable, the Population Monitoring Officer.
- Initiation of the remediation assessment process within 48 hours of Level 2 classification, in accordance with Section 9.1.
- Documentation of the Level 2 event, including: classification date and time, triggering metric and threshold breach data, preliminary causal attribution assessment, and initial remediation response status.

- Disclosure to CMOS-SB within **72 hours** of Level 2 classification, using the CMOS-SB Level 2 Notification Template, including all documentation required by that template.
- Continuation of enhanced monitoring throughout the Level 2 event period, with metric readings reported to leadership on a frequency no less than every 24 hours until de-escalation or escalation to Level 3.

7.3 Level 3 Alert — Critical

A **Level 3 Alert (Critical)** is issued when a monitored metric breach is sustained beyond two consecutive detection windows without resolution, when a breach is of severe magnitude (exceeding 3 standard deviations from baseline), when a cascade propagation event is confirmed in progress, or when two or more independent threshold breaches occur concurrently. Level 3 represents the most severe population-level emotional risk condition under PERMS and triggers the full range of mandatory response, disclosure, and remediation obligations.

Level 3 Alert obligations include:

- Notification to CMOS-SB within **4 hours** of Level 3 classification, via the CMOS-SB Emergency Notification Protocol, including full event documentation and immediate remediation actions initiated or planned.
- Mandatory public disclosure within **24 hours** of Level 3 classification, in a form and format consistent with CMOS-SB public disclosure guidance, describing the nature of the event, the affected population, and the remediation actions underway. Disclosure content must be reviewed by the system's designated monitoring lead or Population Monitoring Officer prior to publication.
- Immediate initiation of remediation measures — not merely remediation assessment — within 24 hours of Level 3 classification. At minimum, interim protective measures must be in place within 24 hours even if full remediation requires additional time.
- Direct user notification where affected users can be specifically identified, consistent with Section 9.2 remediation measure options and in accordance with EDCPS data handling requirements.

- Continued real-time reporting to CMOS-SB until the Level 3 event is de-escalated, at intervals specified by CMOS-SB upon receipt of the initial Level 3 notification.

Critical Compliance Obligation

Failure to make the required CMOS-SB notification within the Level 3 four-hour window, or failure to issue the required public disclosure within 24 hours, constitutes an independent compliance violation under PERMS in addition to the underlying alert event. Timely notification and disclosure obligations are non-waivable absent extraordinary documented circumstances approved by CMOS-SB in advance.

Section 8 — Reporting Requirements

8.1 Internal Reporting

All PERMS-subject systems must maintain a defined internal population monitoring reporting cadence, independent of any alert events, to ensure system leadership has continuous visibility into population-level emotional risk conditions. Internal reporting obligations are as follows:

Standard-Scale Systems (1,000–999,999 users):

- Quarterly Population Monitoring Summary Reports must be prepared and delivered to system leadership, covering: current metric readings against baselines, any Level 1 watch periods opened or closed during the quarter, any Level 2 or Level 3 events and their status, and a forward-looking risk assessment for the next quarter.
- Immediate reports must be generated and delivered to senior leadership upon classification of any Level 2 or Level 3 alert.

Large-Scale Enhanced Systems (1,000,000+ users):

- Monthly Population Monitoring Summary Reports must be prepared and delivered to senior leadership, covering all elements required in the Standard-Scale quarterly report, updated to reflect the preceding month's monitoring data.
- Immediate reports must be generated and delivered to senior leadership upon classification of any Level 2 or Level 3 alert, in advance of and separately from the CMOS-SB notification required under Section 8.2.

8.2 CMOS-SB Reporting

All PERMS-subject systems must maintain the following reporting obligations to CMOS-SB:

- **Annual Compliance Report** — An annual PERMS compliance report must be submitted to CMOS-SB no later than 90 days following the end of each compliance year. The annual compliance report must include: confirmation of monitoring infrastructure operational status; baseline summary and any recalibrations performed during the year; summary of all Level 1, 2, and 3 alert events; summary of all remediation actions taken; and a certification of compliance signed by the designated monitoring lead or Population Monitoring Officer.
- **Level 2 Notification** — Written notification of Level 2 alert events must be submitted to CMOS-SB within 72 hours of classification, using the CMOS-SB Level 2 Notification Template.
- **Level 3 Emergency Notification** — Emergency notification of Level 3 alert events must be submitted to CMOS-SB within 4 hours of classification, using the CMOS-SB Emergency Notification Protocol.
- **Information Request Response** — All CMOS-SB information requests related to PERMS compliance must be responded to in full within **10 business days** of receipt. Requests for extension must be submitted in writing to CMOS-SB prior to the deadline.
- **Remediation Verification Reports** — Following any Level 2 or Level 3 event, a remediation verification report must be submitted to CMOS-SB within 60 days of remediation implementation, in accordance with Section 9.3.

8.3 Public Reporting

Large-Scale Enhanced PERMS Systems (1,000,000+ users) must prepare, publish, and make freely accessible to the public an annual **Population-Level Emotional Impact Report (PLEIR)**. The PLEIR must be published no later than 120 days following the end of each compliance year and must remain publicly accessible for a minimum of 3 years from its publication date.

The PLEIR must include, at minimum, the following content components:

13. **Baseline Summary** — A description of the system's established population-level baselines as of the end of the reporting year, expressed in accessible language appropriate for a general audience, without disclosure of proprietary methodology details.
14. **Anomaly Events Summary** — A plain-language summary of all Level 2 and Level 3 alert events occurring during the reporting year, including approximate onset, nature of the condition, and resolution status. Individual user information must not be included.
15. **Remediation Actions** — A description of all material remediation actions taken during the reporting year in response to Level 2 or Level 3 events, including a summary of effectiveness outcomes where available.
16. **Year-Over-Year Trend Analysis** — A comparison of current-year population monitoring metrics against the prior year (or prior baseline period where year-over-year comparison is not yet available), identifying material positive or negative trends in each of the four baseline components.

8.4 Report Format Standards

All reports required under this section — internal, CMOS-SB, and public — must adhere to the following format requirements:

- CMOS-SB-designated reporting templates must be used for all CMOS-SB submissions where templates have been issued. Templates in force at the time of the applicable report are available on the CMOS-SB website at cmos-sb.org.
- Standardized metric definitions as specified in this standard and in CMOS-SB metric guidance must be used consistently. Systems may not substitute non-standard metric labels or definitions without CMOS-SB approval.

- Reports must be dated, versioned, and signed or certified by the designated monitoring lead or Population Monitoring Officer.
- Electronic submission of CMOS-SB reports must be made via the CMOS-SB secure submission portal or such alternative submission method as CMOS-SB designates.

Section 9 — Remediation Obligations

9.1 Remediation Duty

Upon confirmation of a Level 2 or Level 3 alert event, all PERMS-subject systems bear an affirmative duty to investigate, plan, and implement remediation measures sufficient to address the confirmed population-level risk condition. The remediation duty is non-discretionary: systems may not elect to monitor without remediating once a Level 2 or Level 3 alert has been confirmed.

The remediation duty is structured around three mandatory phases with defined timelines:

Phase	Obligation	Timeline from Alert Confirmation
Phase 1: Root Cause Analysis	Initiate a documented root cause analysis to identify the system and/or external factors contributing to the confirmed alert condition	Within 48 hours
Phase 2: Remediation Plan	Develop and document a written remediation plan specifying the measures to be taken, the responsible parties, and the expected implementation timeline	Within 7 days
Phase 3: Implementation	Implement all remediation measures specified in the approved remediation plan	Within 30 days (or as extended by CMOS-SB)

The 30-day implementation deadline may be extended upon written application to CMOS-SB, provided that: (a) the application is made before the deadline expires; (b) the application demonstrates good cause for the extension; and (c) the application includes a revised implementation timeline and a description of any interim protective measures in place during the extension period. CMOS-SB reserves the right to approve, conditionally approve, or deny extension requests at its discretion.

For Level 3 events, interim remediation measures — not merely planning — must be initiated within **24 hours** of alert confirmation, in advance of the development of the full remediation plan. Interim measures must be documented and reported to CMOS-SB as part of the Level 3 emergency notification.

9.2 Remediation Measures

Remediation measures available to PERMS-subject systems include, but are not limited to, the following categories. The selection of appropriate measures must be guided by the root cause analysis and the nature of the confirmed risk condition:

- **Content Throttling** — Reduction in the distribution volume or frequency of content categories identified as contributing to the anomaly or contagion event.
- **Pacing Adjustments** — Modification of the rate at which users are exposed to emotionally activating content or interaction sequences, including the introduction of mandatory pacing intervals where warranted.
- **Notification Architecture Changes** — Reduction in notification frequency, urgency, or emotional valence for affected user populations or segments, including temporary suspension of high-activation notification types.
- **Algorithmic Tuning** — Adjustment of content selection, ranking, or recommendation algorithms to reduce transmission-accelerating design patterns identified by the root cause analysis.
- **Feature Suspension** — Temporary suspension of specific system features that are identified as material contributors to the confirmed risk condition, where less disruptive measures are insufficient.
- **User Support Escalation** — Enhanced access to user support resources, mental health information, or supportive content for affected population segments.
- **Direct User Communication** — Direct communication to affected users regarding the nature of the risk condition and the protective measures being taken, in accordance with the transparency principles of CMOS-SB Standard 1001 (EISS).

Remediation measures must be proportionate to the severity of the confirmed risk condition. Level 2 events may be addressed through targeted, lower-intervention measures where the root cause analysis supports such an approach. Level 3 events require material, system-level remediation measures and

must not be addressed solely through user-facing communications without corresponding system-level changes, unless CMOS-SB approves an exception in writing.

9.3 Remediation Verification

The remediation duty does not conclude upon implementation of remediation measures. All PERMS-subject systems must conduct post-implementation monitoring to verify the effectiveness of remediation and report verification outcomes to CMOS-SB within **60 days** of remediation implementation.

Remediation verification requirements include:

- **Follow-Up Monitoring Protocol** — A defined post-remediation monitoring protocol must be initiated within 24 hours of remediation implementation, tracking the confirmed alert metric(s) against the relevant thresholds on an enhanced monitoring schedule throughout the 60-day verification period.
- **Effectiveness Assessment** — At the conclusion of the 60-day monitoring period, a formal effectiveness assessment must be prepared, documenting: the metric trajectory following remediation, whether alert thresholds were de-escalated, and whether any residual risk conditions remain.
- **Remediation Verification Report** — A Remediation Verification Report must be submitted to CMOS-SB within 60 days of remediation implementation, including the effectiveness assessment and the post-remediation monitoring data. This report is submitted using the CMOS-SB Remediation Verification Template.
- **Continued Monitoring** — Where the effectiveness assessment identifies residual risk conditions, enhanced monitoring must continue and a supplemental remediation plan must be submitted to CMOS-SB within 10 days of the effectiveness assessment.

Important

Successful de-escalation of an alert event does not automatically satisfy the remediation verification obligation. Verification requires a complete 60-day post-implementation monitoring

period and formal submission to CMOS-SB, regardless of how quickly the acute alert metrics return to baseline levels. Early de-escalation may, however, support a shorter post-remediation monitoring protocol if CMOS-SB approves a modified schedule upon written request.

Section 10 — Data Governance for Population Monitoring

Data

Population monitoring data generated under PERMS — including all metric measurements, anomaly records, contagion event records, drift event records, alert documentation, remediation records, and associated analytical outputs — is subject to the data governance requirements of CMOS-SB Standard 1004 (EDCPS), with the following PERMS-specific modifications and supplements. In all cases where this section conflicts with the general EDCPS requirements, this section governs for PERMS compliance data.

10.1 Data Classification and Retention

Population monitoring data under PERMS is classified and governed as follows:

Data Type	EDCPS Tier	PERMS Retention Rule	Anonymization Requirement
Aggregate population metrics (MDB, ASI, ATR, CRS readings)	Tier C (Aggregate)	Up to 5 years for trend analysis	Not applicable (aggregate only; no individual identifiers)
Individual-level data used to generate population metrics	Tier A / Tier B (Individual)	Anonymized before retention beyond 30 days	Full anonymization required at 30-day mark; no re-identification
Anomaly and alert event records	Tier C (Aggregate)	Minimum 5 years	Not applicable; records must not contain individual identifiers
Remediation records and verification reports	Tier C (Aggregate)	Minimum 5 years	Not applicable; records must not contain individual identifiers
Contagion and drift event records	Tier C (Aggregate)	Minimum 3 years	Cluster-level tracking data must be aggregated before retention beyond 30 days

Tier C (aggregate) population monitoring data generated solely for PERMS compliance purposes benefits from an extended retention period of up to 5 years, which represents a PERMS-specific extension beyond the default EDCPS retention parameters applicable to Tier C data. This extension is authorized by this section to enable the long-term trend analysis that is central to the operational purpose of PERMS.

Individual-level data used to generate population metrics — including raw data inputs to mode distribution calculations, susceptibility measurements, and resilience scoring — must be fully anonymized before any retention beyond 30 days from the date of collection. Anonymization procedures must satisfy the EDCPS anonymization standards defined in CMOS-SB Standard 1004, and must be applied on a documented, scheduled basis. Any individual-level data retained beyond 30 days without anonymization constitutes a PERMS data governance violation as well as an EDCPS violation.

10.2 Security and Access Controls

All population monitoring data generated under PERMS must be stored and managed in accordance with the following security requirements:

- **Secure, Access-Controlled Storage** — All PERMS data must be stored in systems with defined access controls limiting access to personnel with a documented operational need for the specific data category. Access control lists must be reviewed at least semi-annually and updated within 5 business days of any personnel change affecting access eligibility.
- **Full Audit Logging** — All access to, modification of, export of, or deletion of PERMS population monitoring data must be logged in a tamper-evident audit log. Audit logs must be retained for a minimum of 3 years and must be made available to CMOS-SB within 5 business days of any information request.
- **Data Segregation** — Population monitoring data must be logically or physically segregated from general operational data systems to prevent inadvertent commingling or unauthorized access.
- **Breach Response** — Any unauthorized access to or breach of PERMS population monitoring data must be reported to CMOS-SB within 48 hours of discovery, in addition to any other breach reporting obligations applicable under EDCPS and applicable law.

10.3 Cross-Standard Data Governance Coordination

Systems subject to both EDCPS (Standard 1004) and PERMS (Standard 1005) must maintain a unified data governance framework that satisfies the requirements of both standards without conflict. Where EDCPS and PERMS requirements address the same data and differ in specifics, the more protective requirement governs, except where this section expressly provides otherwise. Systems must document their unified data governance framework in a PERMS Data Governance Policy, maintained and updated at least annually and available to CMOS-SB upon request.

Section 11 — Compliance Checklist

The following compliance checklist is provided as a self-assessment tool for PERMS-subject systems. Completion of this checklist does not substitute for formal CMOS-SB compliance review and certification. Systems must complete, sign, and retain this checklist on an annual basis and submit it as part of their Annual Compliance Report to CMOS-SB.

For each item, indicate current compliance status. Where the answer is **No** or **In Progress**, the system must provide a written explanation and projected compliance date in the Remarks column or in an attached compliance gap statement.

#	Compliance Item	Applies To	Yes	No	N/A	Remarks
1	Monitoring infrastructure has been established and is fully operational, including all four required functional capabilities (population-state monitoring, anomaly detection, contagion surveillance, escalation and alert system)	All	☐	☐	☐	
2	Population-level baseline has been formally documented, including all four required components (MDB, ASI, ATR, CRS), within 90 days of PERMS implementation	All	☐	☐	☐	
3	Baseline has been refreshed within the past 12 months (or following any qualifying major system change or post-anomaly recalibration trigger)	All	☐	☐	☐	
4	Automated anomaly detection system is operational, sensitive to both acute spikes and gradual drift, and capable of causal	All	☐	☐	☐	

#	Compliance Item	Applies To	Yes	No	N/A	Remarks
	attribution distinction; methodology is fully documented					
5	Detection windows conform to tier requirements: 72-hour maximum for Standard-Scale systems; 24-hour maximum for Large-Scale Enhanced systems	All	☐	☐	☐	
6	Contagion surveillance function is active and operational, including cluster-level tracking, propagation rate measurement, source identification support, and event documentation capability	All	☐	☐	☐	
7	Drift surveillance function is active and operational, including multi-window trend analysis and documented drift detection thresholds	All	☐	☐	☐	
8	Cascade risk modeling has been implemented, including network topology analysis, quarterly scenario stress testing, and pre-emptive risk flagging capability	Large-Scale Enhanced only	☐	☐	☐	
9	Alert thresholds for Level 1, Level 2, and Level 3 have been formally defined, documented, and tested within the past 12 months	All	☐	☐	☐	
10	Escalation protocols have been tested through tabletop exercise or live drill within the past 12 months; test records are maintained and available for audit	All	☐	☐	☐	
11	Internal reporting schedule has been maintained throughout the compliance year: quarterly reports (Standard-Scale) or monthly reports (Large-Scale Enhanced) have been prepared and delivered to system leadership	All	☐	☐	☐	
12	All Level 2 and Level 3 alert events during the compliance year have been notified to CMOS-SB within the required timelines; documentation is available for audit	All (if applicable)	☐	☐	☐	
13	Annual Population-Level Emotional Impact Report (PLEIR) has been prepared and published publicly, covering baseline summary, anomaly events, remediation actions, and year-over-year trend analysis	Large-Scale Enhanced only	☐	☐	☐	

#	Compliance Item	Applies To	Yes	No	N/A	Remarks
14	All Level 2 and Level 3 remediation obligations have been fulfilled: root cause analyses initiated within 48 hours; remediation plans completed within 7 days; implementation completed within 30 days (or CMOS-SB-approved extended timeline)	All (if applicable)	☐	☐	☐	
15	Remediation Verification Reports have been submitted to CMOS-SB within 60 days of remediation implementation for all applicable events during the compliance year	All (if applicable)	☐	☐	☐	
16	PERMS Data Governance Policy is in place, current, and consistent with EDCPS requirements; individual-level data is anonymized before retention beyond 30 days	All	☐	☐	☐	
17	All population monitoring data is stored in secure, access-controlled systems with full audit logging; audit logs are retained and available for CMOS-SB review	All	☐	☐	☐	
18	A named monitoring lead (Standard-Scale) or Population Monitoring Officer (Large-Scale Enhanced) has been designated, with documented accountability for PERMS compliance, reporting, and escalation	All	☐	☐	☐	
19	Predecessor standard compliance (EISS 1001, CMSS 1002, ETDS 1003, EDCPS 1004) has been confirmed and is current for the compliance year	All	☐	☐	☐	
20	This checklist has been reviewed, completed, and signed by the designated monitoring lead or Population Monitoring Officer and is being submitted as part of the Annual Compliance Report to CMOS-SB	All	☐	☐	☐	

Certification Statement

I certify that the information provided in this compliance checklist is accurate and complete to the best of my knowledge, and that the system identified below has maintained PERMS-compliant operations throughout the compliance year covered by this report, except as noted in the Remarks column or attached gap statement.

System Name: Population Monitoring Officer /
Monitoring Lead: Signature: Date:

Compliance Year Covered: PERMS
Tier: Report Submission Date:

CMOS-SB Standard 1005 — Population-Level Emotional Risk Monitoring Standard (PERMS)

Version 1.0 | Effective June 9, 2026 | Next Review: June 9, 2027

Standard ID: CMOS-SB-1005 | Governance Spine: Pillar 5 of 5 | CMOS-SB Publication Set Item 10

Author / Architect: Isabelle Anne Thompson

Cognitive Mode OS™ is a trademark of Isabelle Anne Thompson / Sugar Sands Publishing LLC. All rights reserved.

cmos-sb.org