



Holding Vendors Accountable with SLAs

Tommy Thompson, ENP, PMP
Senior Consultant
Federal Engineering, Inc.



#IWCE26

Agenda



Why This Matters

In public safety, expectations that are not enforceable are optional.

What's Broken Today

WHAT'S BROKEN TODAY

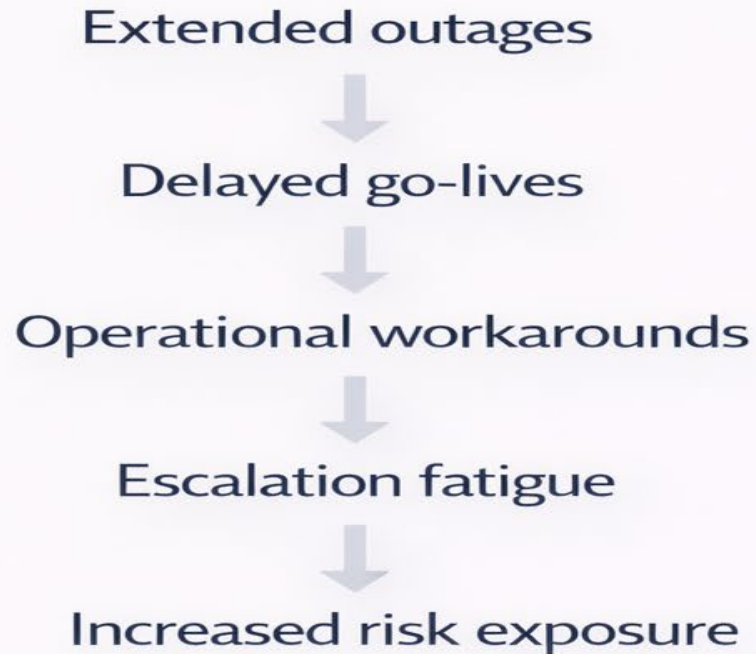
- **Vague language** replaces measurable commitments
- **Metrics undefined or unenforceable**
- **Verification** manual or absent
- **Penalties discretionary, or waived**
- **Vendor templates** drive the contract – **not operations**

THE RESULT

- Extended outages
- Missed milestones
- Vendor finger-pointing
- Operational and reputational risk

Weak SLAs protect vendors, not operations.

The Cost of a Weak SLA



Who Pays the Price?

- Call takers and dispatchers
- IT and technical staff
- Agency leadership
- The public and responders

Weak SLAs shift cost and risk from vendors to public safety agencies.

Anatomy of a Strong SLA

WHAT'S BROKEN TODAY

DEFINED METRICS

- Uptime
- MTTR
- Availability

VERIFICATION

- Logs
- Dashboards
- Independent monitoring

PENALTIES & CREDITS

- Automatic
- Financial or service-based
- No discretion

REVIEW CYCLE

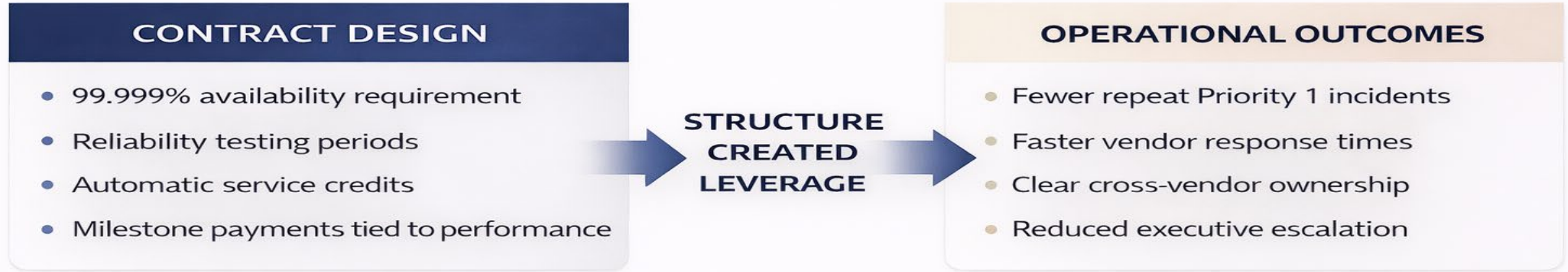
- Quarterly reviews
- Corrective action plans
- Executive visibility

TERMINATION TRIGGERS

- Repeated failures
- Rolling periods
- Material breach

If any element is missing, the SLA is informational, not enforceable.

Real-World Example: CAD Deployment



When payment and acceptance depend on performance, behavior changes.

Writing Enforceable SLAs

Precision creates enforceability.

DEFINE THE METRIC

- Measurable
- Calculated

DEFINE THE CLOCK

- Start / stop rules

TIE MONEY TO PERFORMANCE

- Payment follows verification

AUTOMATE REMEDIES

- No discretion

AUTOMATE REMEDIES

- No discretion

Checklist Test:

- Measurable?
- Verifiable?
- Automatic?
- Chronic failure defined?

If performance cannot be measured and verified, it cannot be enforced.

CONTRACT FAILURES

- Accepting vendor boilerplate
- “Reasonable efforts” language
- Confusing warranties with SLAs
- Cybersecurity excluded from scope
- Undefined shared responsibility

WARNING SIGNS

- Manual enforcement required
- No objective reporting
- Credits negotiated or waived
- Chronic issues normalized

If enforcement requires negotiation, the SLA is already broken.



Warranty

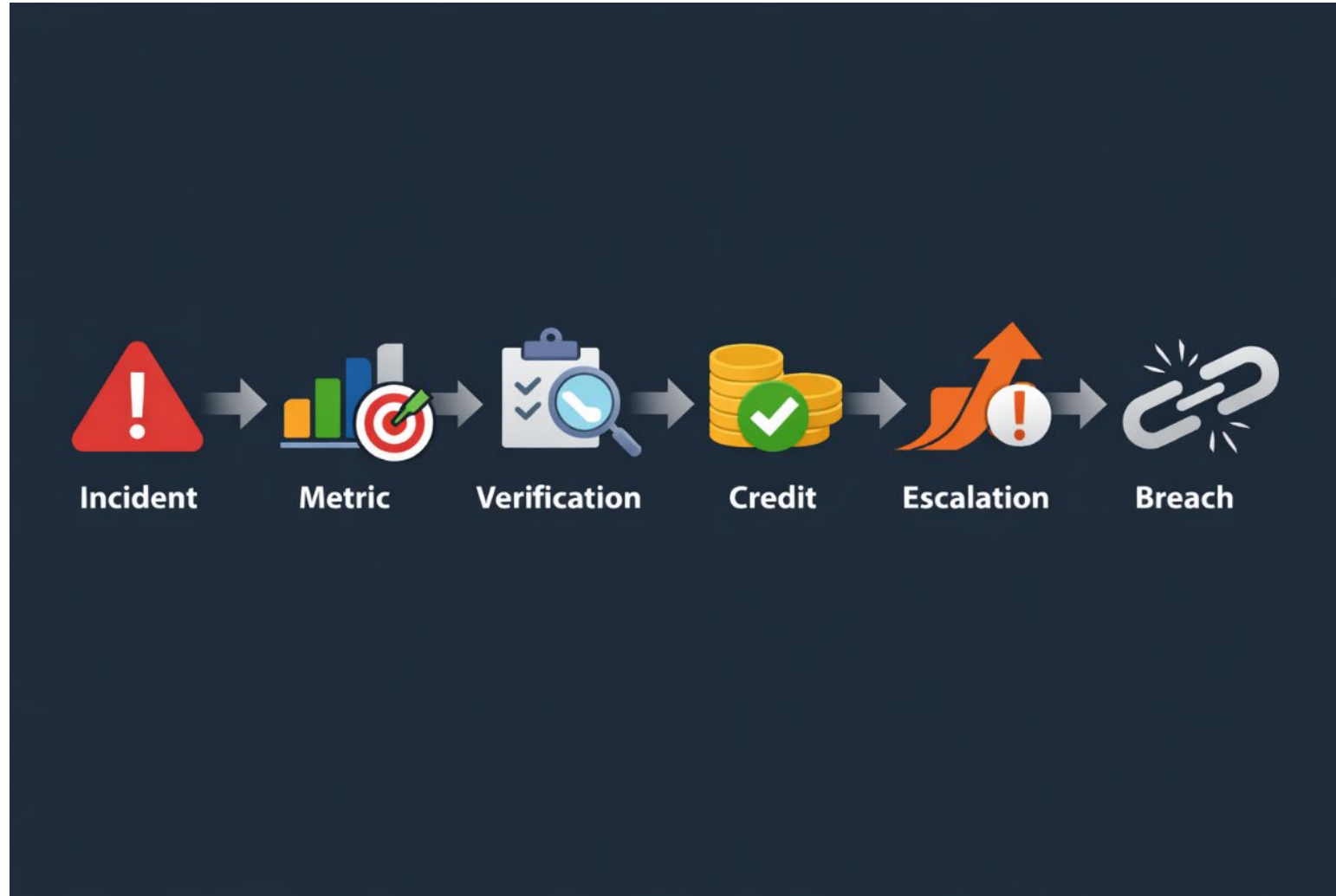
- Defects
- Fixes bugs
- One-time
- Vendor-defined
- No penalties



SLA

- Availability
- Protects operations
- Continuous
- Agency-defined
- Enforceable remedies

The SLA Enforcement Chain



Aligning SLAs with NG9-1-1 and CJIS



CJIS REQUIREMENTS

- Uptime & Availability
- Audit Support



CYBER INCIDENT CLOCKS

- Defined Response
- Defined Restoration



CLOUD & DATA CONTROLS

- Hosting
- Residency
- Access Control



NENA i3 ALIGNMENT

- Functional Elements



SHARED ESinet MODELS

- Multi-Agency Accountability



Compliance Lens

- Availability is Mandatory
- Security Requires SLA Clocks
- **Compliance ≠ Enforceability**
- Must Survive **Audits** and **Incidents**

Compliance requirements strengthen SLAs only when they are measurable and enforceable.

Enforcement Strategies



PAYMENT LEVERAGE

- Milestones tied to **verification**



PROOF REQUIREMENTS

- Response validated | Reliability demonstrated



STRUCTURED REVIEWS

- Quarterly validation | Documented corrections



TIME-BASED ESCALATION

- Defined triggers



ALIGN TIME & MONEY

- Payment follows integrity

Governance Focus:

- ✓ Audit-proof
- ✓ Documented **performance**
- ✓ Automatic remedies
- ✓ Transparent enforcement

Enforcement works best when it is automatic, consistent, and transparent.

Negotiation Tactics

- Start from your own SLA proposals
- Benchmark against peer public safety contracts
- Define SLA expectations explicitly in the RFP
- Negotiate service escalation above compliance
- Tie renewal and extensions to performance history

Leverage Focus:

- ✓ Audit-strength requirements
- ✓ Defined **service exemptions**
- ✓ Enforceable **penalties**
- ✓ Escalating service procurement metrics

Strong negotiation sets the conditions for long-term accountability.

Operational Enforcement

- Defined priorities for incidents (1-4)
- MTTR clocks & explicit escalation rules
- 30/60/90-day post-upgrade reliability periods
- 30/60/90-day post-upgrade reliability periods

Credits, Breach, and Governance

- ✓ Automatic **service credits** tied to charges
- ✓ Chronic **failure** defined by rolling performance
- ✓ Formal **RCA** with corrective actions required
- ✓ Scorecards & executive reviews each quarter

Clear, well-written SLAs create **enforceable operational accountability.**

Tools You Can Use

Practical Tools

- SLA metric and enforcement checklist
- Model SLA clauses for uptime, MTTR, and escalation
- Vendor performance scorecard templates
- Quarterly SLA review & corrective action worksheet

Execution Focus:

- ✓ Enforce accountability
- ✓ Automate validation
- ✓ Track improvement
- ✓ Require follow-through

Tools only matter when they are **embedded, used, and enforced.**

Key Takeaways

Strong SLAs protect operations, not vendors

Accountability must be defined, measured, and enforced

Performance verification is as important as performance targets

Payments and acceptance should depend on outcomes

Transparency and governance drive long-term reliability

Remember:

If expectations are not enforceable,
they are optional.

Accountability protects public safety operations and public trust.



Technology fails – Accountability shouldn't

Tommy Thompson, ENP, PMP
Senior Consultant | Federal Engineering, Inc.
tthompson@fedeng.com



Thank You !