EXIGENT

CYBERSECURITY

Policy on Responding to Audit Inquiries Without a Compliance Program

EXIGENT

Policy – Audit Inquiries

CYBERSECURITY

Purpose

This document clarifies Exigent Technologies' policy on responding to client audit inquiries related to Cybersecurity Framework Compliance (such as NIST SP 800-171, HIPAA, PCI-DSS, CMMC, etc.) in scenarios where the client does not have an active or functional compliance program in place.

Statement of Position

Exigent Technologies cannot provide comprehensive or authoritative responses to audit questions on behalf of clients who lack a formalized compliance program, such as our *Vigilant Compliance* offering, or equivalent internal governance. In the absence of documented compliance activities, controls, and evidence, any attempt to answer such inquiries would be speculative, incomplete, and potentially misleading to auditors, insurers, regulators, or downstream partners.

We will only answer the most basic factual or infrastructure-related questions within our operational scope (e.g., confirming firewall models or MFA enablement). We will not:

- Certify compliance or make representations about your adherence to any framework.
- Construct compliance evidence or documentation retroactively.
- Complete audit questionnaires requiring attestation to policy, governance, or operational controls beyond our managed services.
- Accept liability for any compliance-related findings or failures resulting from incomplete or inaccurate responses.

Rationale

NIST, CMMC, PCI, HIPAA, and similar compliance frameworks require a comprehensive and programmatic approach, including:

- Formal policy creation and maintenance,
- Documented evidence collection for each control,
- Control implementation and validation,
- Ongoing risk assessment and monitoring,
- Staff training and acceptance tracking,
- Continuous governance and review.

Absent this, any audit participation would lack defensible grounding and expose both the client and Exigent to undue risk.

CYBERSECURITY

Cost Considerations

Compliance is not a "check-the-box" exercise. Even policy development alone can represent a significant investment:

For a single client's policy suite, Exigent has observed:

- Investigation, authoring, review, editing, finalization, dissemination, and acceptance tracking:
    - At an estimated 80 hours over 2 weeks, billed at $250/hour (reflecting senior-level, specialized compliance expertise), this totals $20,000.

This does not include:

- Control implementation or technical remediation,
- Evidence collection and audit mapping,
- Staff training and attestations,
- Ongoing compliance monitoring and reporting.

As an example, a full SP 800-171 program (policies, controls, evidence, and governance) often represents a multi-phase, multi-month engagement, with costs scaling according to environment complexity and the number of controls requiring remediation. For even moderately complex environments, total initial compliance investment often exceeds $50,000–$75,000, not including internal staff time and process changes.

Our Recommended Approach

To support compliance objectives efficiently and reduce risk, Exigent offers Vigilant Compliance, which includes:

- Framework alignment to SP 800-171 and related standards (e.g., CIS, CMMC, etc.).
- Policy authoring and approval workflows.
- Control mapping, evidence collection, and remediation plans.
- Staff training, attestation tracking, and ongoing monitoring.
- Structured reporting for audits and external assessments.

Engaging in such a program is the only viable path to confidently respond to audits and regulatory demands.

Conclusion

In summary, without a formal compliance program in place, Exigent Technologies' participation in compliance audits is necessarily limited to operational facts within our managed scope. Clients must engage in a structured compliance initiative - such as Vigilant Compliance - to enable defensible audit responses and achieve compliance readiness. Attempting to answer audit questions without a compliance program is not only impractical - it is risky and exposes your organization to potential audit failure, penalties, and reputational harm. Establishing such a program is a non-negotiable prerequisite for meaningful audit support.