ANWAR ABU-SHAYED

Proposal and Comment Information

Title: Agency Information Collection (FFIEC 101), ICP-202612

Comment ID: FR-2026-0038-01-C04

Submitter Information

Name: Anwar Abu-shayed

Submitted Date: 11/14/2026

Re: ICP-202612 — FFIEC 101 | OMB Control No. 7100-0319

I formally oppose the unconditional three-year extension of FFIEC 101 without a corresponding commitment to modernize federal financial risk reporting.

My attached Federal Financial Risk Measurement and Reporting Modernization Initiative identifies material regulatory gaps and proposes comprehensive reforms addressing capital adequacy, cybersecurity exposure, institutional governance solvency, independent assurance, consumer financial injury, workforce protections, evidentiary integrity, and federal supervisory accountability.

This proposal was also submitted directly to OMB/OIRA on November 14, 2026, under ICR Reference No. 202610-1557-001.

I respectfully request that the Board incorporate the attached proposal in its entirety into the administrative record and consider its recommendations for separate rulemaking and legislative referral, where appropriate.

Financial capitalization alone does not establish institutional soundness.

Respectfully submitted,

Anwar Abu-Shayed, M.S.
Cybersecurity | Enterprise Risk Management | Institutional Governance

FEDERAL FINANCIAL RISK MEASUREMENT AND REPORTING MODERNIZATION INITIATIVE

Formal public comment • OMB information-collection review • petition for rulemaking

RE: FFIEC 101 — Regulatory Capital Reporting for Institutions Subject to the Advanced Capital Adequacy Framework

Federal Register: 91 FR 65843–65845 (October 16, 2026) | FR Doc. 2026-21185

Federal Reserve: ICP-202612 | OCC: 1557-0239 | Board: 7100-0319 | FDIC: 3064-0159

OCC ICR reference: 202610-1557-001

Submitted to: Office of the Comptroller of the Currency; Board of Governors of the Federal Reserve System; Federal Deposit Insurance Corporation; Office of Management and Budget, Office of Information and Regulatory Affairs

Submitted by: Anwar Abu-Shayed, M.S. — Cybersecurity | Enterprise Risk Management | Institutional Governance

Connecticut, United States

Requested disposition

Preserve uninterrupted FFIEC 101 reporting, but do not grant an unqualified three-year extension without addressing the practical utility, reliability, burden methodology and modernization needs of this collection. I request a 12-month approval, if practicable, with a documented review and modernization plan; an opportunity to be heard before OMB; and separate, properly authorized proceedings to develop the supplemental reporting and prudential reforms set out below.

This submission complements my comprehensive opposition to the proposed interagency Third-Party Risk Management Guidance (OCC-2026-0793 and Federal Reserve OP-1881). Its specific purpose is to strengthen the information architecture through which regulators evaluate capital adequacy, operational exposures, institutional soundness and the consequences of financial innovation. It does not request suspension of essential reporting or contend that approval of an information collection alone creates substantive prudential obligations.

Core policy principle

Prohibition Against Institutional Risk Externalization. Institutions should not improve apparent financial performance by transferring unrecognized operational, legal, cybersecurity, consumer or employment-related costs to the public. Financial capitalization must be evaluated alongside the integrity of the infrastructure and governance systems on which financial operations depend.

No institution should be considered sound merely because it can afford the consequences of misconduct. Innovation must not precede independently verified remediation.

I. Objection to unchanged renewal and scope of review

The joint notice states that the first comment period closed August 4, 2026, with no comments received, and that the agencies intend to seek a three-year extension without revision. It acknowledges ongoing work to revise advanced-approaches capital requirements and explains that the existing collection expires December 31, 2026. These circumstances support continued reporting, not an assumption that the collection is optimally designed. [1]

The absence of prior comments is not evidence of public approval or proof of information quality. This timely comment addresses all five areas expressly solicited: necessity and practical utility; accuracy of burden estimates; quality, utility and clarity; use of technology to minimize burden; and capital, start-up, operating, maintenance and purchased-service costs.

FFIEC 101 already collects regulatory capital components, risk-weighted assets and operational-loss data. FR Y-15 addresses systemic financial importance, and FR Y-14Q includes operational-risk information used in supervisory capital analysis. [3–5] I seek a gap analysis and complementary collection, not duplication or elimination of existing data.

Under the Paperwork Reduction Act (PRA), 44 U.S.C. §§ 3506–3508, the agencies and OMB must evaluate the actual use and practical utility of information. PRA approval is distinct from a substantive capital rule, supervisory order or legislative amendment. All new mandatory fields, restrictions and remedies proposed here require the proper statutory authority, notice-and-comment procedures where applicable, and information-collection clearance. Existing mandatory reporting must continue under valid approval.

II. Request for OMB certification review and shortened renewal

Section 3506(c)(1) requires a sufficiently independent agency review process, including an objectively supported burden estimate, assessment of need, and plans for efficient management and use of collected information. Section 3506(c)(3) requires certification and supporting documentation; § 3507(h)(1)(B) requires the renewal submission to explain actual use of prior collection results. Under 5 C.F.R. § 1320.3(l), the relevant inquiry includes reliability, adequacy, accuracy and actual timely usefulness. [6–8]

The OCC's ICR record (202610-1557-001) lists 40 annual responses, 26,960 annual hours, $0 separately reported dollar-cost burden and an unchanged request for 36 months; the record was listed as received in OIRA when reviewed. [2] These figures require explanation, not an inference that the certification is false or that labor and technology cost nothing.

I request that OMB and each agency provide the following verification record, with lawful redactions and nonconfidential summaries where necessary:

- How FFIEC 101 information has been used for supervisory decisions, capital model validation, examination planning, risk monitoring and corrections; examples should be anonymized when needed.
- Evidence of data validation, error rates, reconciliation performance, and how anomalies, missing values and inaccurate reporting are investigated and resolved.
- The rationale for unchanged burden estimates, the split between labor and non-labor costs, and the assumptions concerning automated reporting, external vendors, technology changes and

recordkeeping.

- A crosswalk of existing collections and supervisory sources, showing which prospective cybersecurity, provider-concentration, consumer-harm and governance exposures are already measured and which remain unmeasured or insufficiently comparable.
- A review of the certification record and any public comment received in this second comment period; if a material deficiency is found, identify corrective procedures and the appropriate timeline.

Under § 3507(g), three years is a ceiling, not a required approval duration. I request a 12-month approval maintaining continuity, subject to OMB's determination and applicable law, followed by a documented modernization review. If OMB determines that substantive changes to an existing rule's collection are appropriate, apply § 3507(h)(2)–(3) as relevant. Section 3507(f) permits qualifying independent multi-member regulators to override specified OMB actions by majority vote and certification; any such action should be accompanied by the statutorily required explanation. I do not assert that OMB has an absolute veto.

Under 44 U.S.C. § 3508, I request an opportunity to be heard or to submit further written statements before a final necessity and practical-utility determination. I recognize that such an opportunity is discretionary. [7]

III. Unreconciled marketplace lending and new technological risks

The Treasury Department's May 10, 2016 marketplace lending white paper identified benefits as well as risks associated with emerging credit models, data access, underwriting and financial technology. [9] A decade later, institutions continue to expand marketplace lending, automated underwriting, artificial intelligence, cloud infrastructure, digital assets and external financial service relationships. The agencies should document which previously identified vulnerabilities have been resolved, the evidence of closure and what new risks have emerged. Historical loss measurements alone cannot establish the absence of prospective exposure.

The September 15, 2026 third-party risk management proposal expressly seeks greater tailoring of supervision and replacement of existing guidance. Its consumer-compliance treatment is limited, and its residual-risk approach allows institution-specific judgment even where information or negotiating leverage is constrained. [10] My earlier submission objects to reducing supervisory expectations without reciprocal protections, binding safeguards where authorized, independent verification and enforceable accountability.

The 2024 Synapse bankruptcy provides an example of the dangers of fragmented records and loss of access to funds across financial intermediaries. Cross River Bank's 2016 public comments on third-party lending and subsequent 2018 and 2023 FDIC enforcement actions likewise warrant review of the adequacy of assurance and corrective action before new expansion. These examples were addressed in my prior interagency submission; the present request is to develop verifiable data, not to adjudicate individual claims or presume that previous deficiencies remain uncorrected.

Black October 2026 and correlated technology failure

Wiz Research's October 30, 2026 initial report described at least nine AI development-platform incidents. The Cloud Security Alliance's November 5 analysis examined twelve disclosed incidents involving AI development, hosting and inference infrastructure. It identified credential concentration and the possibility of correlated exposure even where the root causes of incidents differ. [11–12] This evidence postdates the third-party proposal and is directly relevant to risk-measurement modernization. It does not establish that a specific bank was compromised, or that all incidents constitute a single campaign.

The Financial Stability Board's December 2023 third-party risk toolkit similarly recognizes that common critical-service dependencies may transmit risk across institutions. [13] Regulators must measure provider concentration, credential exposure and recovery capacity alongside financial interdependence. Loss-bearing capital cannot substitute for the ability to preserve the integrity, availability and authenticity of critical financial records.

IV. Institutional Governance Solvency (IGS)

I propose an Institutional Governance Solvency standard as an overarching analytical framework, not a replacement for statutory capital classifications. It would evaluate five distinct dimensions: financial solvency; technological resilience; evidentiary integrity; legal and regulatory compliance; and workforce and institutional governance.

Each dimension should be assessed independently, with transparent methodology, materiality criteria and an evidentiary record. The proposed framework must prevent a high capital score from masking a critical control failure. Conversely, a reported allegation, union absence, foreign relationship, or isolated nonmaterial incident must not automatically trigger an adverse determination. Agencies should use verified facts, appropriate supervisory judgment, opportunity to correct disputed data, and statutory process before imposing consequences.

V. Systemic Operational, Cybersecurity and Institutional Governance Risk Report (SOCGR)

I propose a supplemental collection with standardized data definitions. Use existing FFIEC 101, FR Y-15, FR Y-14Q, Call Reports, incident reports and other supervisory collections whenever reasonably available. Apply reporting requirements through the appropriate collection for each institution; the current FFIEC 101 respondent population should not be treated as covering all fintech or marketplace lenders.

Reporting category	Proposed data elements
Financial servicing	Delegated functions, transaction counts and values, historical contractual relationships, ownership and record-control boundaries
Technology concentration	Critical providers, downstream dependencies, substitutability, recovery targets, linked institutions
Cybersecurity and AI	Material vulnerabilities, near misses, incidents, credential exposure, model/vendor dependency, validation and remediation status

Reporting category	Proposed data elements
Digital assets	Custody, liquidity, counterparty, settlement and technological exposure, if applicable
Foreign dependencies	Jurisdiction of processing, provider control, privileged access, beneficial ownership where material
Evidence and data governance	Source-system lineage, unauthorized access, adverse profiling, correction, evidence preservation and access controls
Financial and custodial integrity	Unreconciled amounts, unsupported balances, title/custody/transfer exceptions, recovery and reconciliation
Independent assurance	Scope, assessor independence, testing date, severity, original findings and verified closure
Consumer and workforce injury	Substantiated losses, restitution, staffing and turnover, protected reporting and labor-law findings
Enforcement and legal exposure	Outstanding orders, recurrence, material pending claims, recognized liabilities, estimated contingent exposures
Resilience and remediation	Recovery exercises, service continuity, remediation funding, independently verified completion

Metrics must distinguish event counts, loss amounts, exposure estimates and unresolved control failures; record the reporting period, institution, legal entity, units and relevant scope. Use consistent event IDs to prevent counting one loss multiple times across institutions, vendors or reports. Where suitable, use a secure quarterly core schedule and separate event-based reporting aligned with existing notification rules. Proportionality should reflect material activity, dependencies and consumer exposure, not asset size alone.

VI. Operational Risk Capital Adjustment (ORCA) and capital recalculation

I propose evaluation of an Operational Risk Capital Adjustment through separate prudential rulemaking. The objective is to measure material residual exposure not captured by existing operational-risk models, reserves or capital requirements. Relevant events include verified cybersecurity and reporting failures, recurring servicing errors, concentrations of critical providers, underfunded restitution, insufficient recovery capability and unresolved material enforcement findings.

A capital adjustment must not double-count risks already recognized in risk-weighted assets, existing requirements, provisions, reserves or qualifying mitigants. The agencies should model incremental stress losses, credit and market spillovers and existing coverage, independently validate scenarios, and make the methodology available for comment. No fixed surcharge is proposed without calibration. Document uncertainty and sensitivity; reassess only after independently verified remediation.

Existing authority provides a complementary route. Under 12 C.F.R. §§ 3.123(b)(3), 217.123(b)(3) and 324.123(b)(3), the appropriate regulator may require modified advanced-approaches risk-weighted asset calculations when the regulatory determination is made that calculated amounts are not commensurate with actual risks. [14] I request standard review triggers for verified material

deficiencies, significant model changes, unsupported risk classifications and persistent unreconciled records. These triggers should initiate review, not automatically impose a capital change. Agencies should require corrective plans where the qualification rules require them and exercise the existing recalculation authority on its statutory and regulatory terms.

VII. Federal Regulatory Risk Concentration Index

I propose a supplemental concentration measure covering cloud infrastructure; payment processors; mortgage and loan servicing platforms; AI development, inference and hosting; identity and authentication systems; data aggregators; software supply chains; fourth-party providers; cross-border dependencies; and genuinely independent alternatives.

For each critical financial function, collect provider identifiers, the proportion of function volume dependent on each provider, whether alternatives share underlying infrastructure, the recovery time and recovery-point objectives, actual recovery performance and the feasibility of switching providers. Evaluate an exposure-weighted Herfindahl-type concentration measure alongside largest-provider share, dependence on common upstream components, and modeled loss or service disruption under simultaneous-provider failure. Publish proposed definitions, weighting and validation results before any use for supervision. A concentration score is a signal for examination, not proof of unsafe conduct.

Require scenario testing of a common cloud or payment provider outage, credential compromise across multiple AI vendors, failure of a primary and backup service with a shared dependency, and inability to recreate an authoritative financial ledger. Retain only necessary confidential technical details; publish aggregate sector-level measures rather than exploitable architecture maps.

VIII. Mandatory predeployment reconciliation and preventive reporting

New products and technology arrangements should undergo independent risk review before launch. Document existing deficiencies relevant to the proposed product; inventory critical downstream dependencies; verify data access, financial reconciliation and operational recovery; validate AI underwriting and adverse decisions; test authorized adversarial and resilience scenarios; and obtain independently supported closure of material findings. For existing applicable notification rules, reconcile incident triggers rather than duplicate them. [15]

Establish a Preventive Operational Risk Register for material near misses, failed controls and detected attempted compromise, separately from booked losses. Collect dates of detection, containment and remediation, affected functions, estimated exposure ranges, and evidence of recovery. Map high-value credentials held in external platforms, test revocation of compromised tokens and confirm that alternative providers are genuinely independent. Do not collect secrets themselves.

No expansion of implicated operations should occur when independently established material unresolved deficiencies make that expansion unsafe or unsound, subject to lawful authority and process. Apply existing growth restrictions where appropriate and seek binding future standards through separate proceedings. A new business model is not evidence that an older vulnerability has been corrected.

IX. Independent assurance and non-recurrence

Require independent, nonaffiliated assessment of material cybersecurity, financial-reporting and compliance controls where authorized. Assessors must have documented independence, conflict disclosures, access to evidence, authority to report adverse findings through protected channels and freedom from outcome-contingent compensation. Preserve original findings and subsequent revisions. Authorized penetration testing, model validation, forensic review, and recovery testing must challenge—not operate—essential financial functions.

Create an Independent Remediation Certification standard. For each material finding, document responsible management, corrective action, expected cost, milestones, retest method, evidence, verifier and closure date. Record re-opened or recurring findings and independently evaluate effectiveness after closure. Termination of a regulatory order is not, by itself, evidence that every underlying risk has been eliminated; evaluate recurrence without presuming current noncompliance.

Create an Institutional Remediation Debt measure: quantified remaining cost to implement validated corrective actions, separately identifying funded, unfunded and uncertain amounts. Do not characterize estimates as booked liabilities unless accounting requirements support recognition. Require periodic confirmation that remediation funding is available, and report missed milestones with causes and supervisory disposition.

X. Regulatory Evidence Provenance and Authentication Standard (REPAS)

The Basel Committee's 2026 BCBS 239 implementation publication describes continuing challenges with end-to-end lineage and timely risk aggregation. [16] I propose a data-integrity and evidentiary standard for material regulatory representations. It should complement existing risk-data requirements, not automatically convert every record into publicly disclosed evidence.

Control	Proposed minimum requirement
Provenance	Source-system and record identifiers; accountable institution and custodian; reporting scope
Authentication	Authorized submitter and authorized record changes; segregation of duties
Lineage and transformation	Reproducible source-to-report mapping; transformation rules and version information
Record integrity	Tamper-evident audit trail, cryptographic integrity checks, original and corrected versions retained
Reconciliation	Trace aggregates to underlying records; identify unexplained exceptions and materiality
Independent verification	Sample-based source testing; independent review of material discrepancies and model overrides
Accountability	Executive certification with defined scope, evidence access and correction procedures

Missing values must be distinguishable from true zeroes, nonapplicability, confidentiality, pending verification and errors. Require parent/subsidiary and foreign banking group reporting boundaries to avoid double counting. Preserve time-series revisions, restatements, correction reasons and authorization. Where relevant, use period averages and peak exposures instead of relying only on quarter-end snapshots.

A Regulatory Data Discrepancy Register should identify cross-report inconsistencies across relevant FFIEC 101, FR Y-15, FR Y-14Q and Call Report fields, with mapping differences and documented resolution. A Regulatory Exception Register should record waivers, alternative methods, material model changes and exemptions, their authorization, expiration and controls. Unsupported model assumption changes should trigger an independent challenge. Do not treat valid differences in reporting scope as errors or treat unexplained discrepancies as proven fraud.

Require Data Recoverability Certification: demonstrate that the institution can reconstruct authoritative balances, transaction histories and custody or servicing records independently of an unavailable provider. Preserve sufficient audit evidence for legally authorized review. Cryptographic hashes demonstrate integrity relative to the hashed version; they do not, alone, establish truth, completeness or lawful authority.

XI. Externalized Financial Harm Register and micro-loss aggregation

Operational-risk accounting generally centers on institutional losses. It may not capture the economic consequences borne by consumers, employees or the public outside the institution's own accounts. To identify this risk transfer, establish an Externalized Financial Harm Register separate from recognized accounting loss and prudential capital metrics.

Record the origin and category of the event, institution-recognized gross loss, recoveries, independently substantiated consumer loss, employee loss, restitution ordered and unpaid, contingent exposure, and identifiable public administrative or litigation costs where reliably measurable. Maintain clear statuses: allegation, investigation, substantiated finding, settlement without admission, adjudicated violation, recognized liability and resolved claim. Do not assume allegations are proven. Avoid duplicate accounting of restitution and underlying injury; quantify uncertainty rather than invent values.

Consumer indicators should cover misapplied payments, incorrect fees, unresolved escrow or custody balances, credit-reporting inaccuracies, improper servicing, established wrongful foreclosure practices, delayed access to funds and unauthorized financial-data use. Include accessible dispute resolution and correction outcomes, restitution completion and recurrence. Calculate micro-loss counts and aggregate amounts by common root cause even when individual events fall below existing collection thresholds, with proportionate controls and no duplicative reporting.

Establish a Consumer Restitution Reconciliation schedule: opening outstanding obligation, newly ordered or established amounts, payments, verified delivery, adjustments and closing balance. Distinguish returned principal from compensation and penalties. Independently test that relief actually reaches affected people, particularly consumers whose accounts were closed or transferred.

XII. Misconduct-Adjusted Profitability and risk transfers

I propose a supplementary analytical reconciliation of earnings attributable to established unlawful conduct, without redefining GAAP or regulatory capital. Identify improperly collected fees or charges, other substantiated unlawful gains, recognized restitution and related costs; map each amount to the applicable accounting entry. Distinguish amounts embedded in earnings, amounts reversed, amounts still retained and associated contingent exposure. Avoid subtracting the same cost twice or treating settlements as admissions.

Create a Residual Operational Exposure Register for sold, securitized, transferred, outsourced or discontinued activities. Record continuing servicing, indemnification, data retention, consumer claims, guarantees, custody and provider dependencies, as applicable. Derecognition of an asset does not independently establish that all related operational or legal risks have ended. Existing FR Y-14Q instructions already address historical losses associated with discontinued or sold operations; build upon such rules rather than duplicate them. [5]

Reconcile gross operational losses with realized insurance recoveries, other reimbursements, disputes, coverage exclusions and outstanding recoveries. Existing advanced-approaches rules address qualifying mitigants, including insurance; this proposal seeks transparent reconciliation and detection of correlated risks, not elimination of legitimate mitigation. [17]

XIII. Workforce governance, protected reporting and collective bargaining

The BLS 2025 annual release reports union membership of 0.8 percent in finance and 5.9 percent in the private sector overall. [18] These are industry-level estimates, not evidence that any specific institution has committed misconduct or that union status alone determines safety and soundness.

Personnel responsible for cybersecurity, enterprise risk, internal audit and compliance must be empowered to report material deficiencies without economic coercion. Collect aggregate staffing levels and vacancies, turnover, outsourcing, material staffing changes after adverse findings, substantiated retaliation, protected reporting outcomes, established labor-law violations and lawful collective bargaining coverage. Require independent investigation of credible interference indicators; preserve original findings when employees or contractors depart.

Establish a Protected Workforce Governance Register and an Independent Auditor Interference Register with anonymized event IDs, finding status, independent review, corrective action and recurrence. Protect identities, labor organizing and confidential whistleblower channels; no indiscriminate reporting of union membership or protected disclosures. Employees must retain lawful organizing and collective bargaining rights under 29 U.S.C. §§ 157–158. I propose employer neutrality and recognition of duly selected bargaining representatives through appropriate legal mechanisms, not compulsory individual union membership.

My broader legislative proposal seeks harmonization of whistleblower laws, protection of former employees from retaliation, and abolition of compulsory predispute arbitration for employees and consumers, allowing voluntary informed post-dispute arbitration. Congress must enact new rights beyond existing authority. Reporting should measure established retaliation and remediation, not obstruct access to regulators or courts.

XIV. Governance-adjusted compensation and distributions

Collect aggregate executive incentive compensation, dividends, repurchases, material reductions in risk staff and remediation budgets, outstanding restitution and verified unfunded corrective-action requirements. Evaluate whether incentive designs reward short-term earnings at the expense of operational integrity, and whether discretionary distributions impair funding of corrective action or financial soundness.

I propose a Governance-Adjusted Compensation Review, and legally authorized restrictions on discretionary distributions or incentive compensation when applicable statutory conditions are established. Existing safety-and-soundness provisions include compensation standards; no new compensation cap or automatic clawback is imposed by this comment. Where broader recoupment or distribution restrictions require rulemaking or Congress, initiate the proper proceeding. Protect innocent employees' ordinary wages and avoid penalizing legally protected reporting.

XV. Conditional federal protection and historical outsourcing

Consistent with my prior proposal, I request legislation categorically disqualifying from federal deposit insurance institutions that utilize or have previously utilized third parties for essential financial servicing, including through affiliates, subcontractors, successors and predecessors. This is a proposed bright-line statutory eligibility condition, not current law. It would apply irrespective of asset size, business model, or prior approval. An independent evaluator who tests controls without assuming operational decision-making is distinct from an outsourced financial servicer.

As an initial reporting measure, collect present and historical delegated servicing arrangements, operational responsibilities, ownership, record control, consumer exposures, outstanding findings, associated claims and transition capability. Bank-controlled software and independent testing should be distinguished from actual delegation of essential financial functions. Establish legally defined historical scope, reliable record requirements, anti-circumvention and orderly resolution procedures. Preserve protections for existing insured depositors and continuity of critical services. Subject the proposal to competition, financial-stability and feasibility evaluation; categorical disqualification requires congressional authorization and due process. Deposit insurance is protection of eligible deposits, principally assessment-funded, rather than an unrestricted grant to institutions.

Pending legislation, evaluate actuarially justified risk factors in the FDIC's existing risk-based assessment system under 12 U.S.C. § 1817(b)(1). [19] Where evidence demonstrates a link to probability or magnitude of Deposit Insurance Fund loss, consider common-provider concentration, unreliable custodial records, recurring cyber incidents and unresolved material findings. Calibrate and validate changes through notice and comment under § 1817(b)(1)(F). Assessments should reflect fund risk, not function as unauthorized punitive sanctions.

XVI. BSA, FOIA, data rights and foreign dependencies

In coordination with Treasury, FinCEN and the CFPB, develop lawful metrics covering financial-risk profiling, sources of adverse data, third-party access, automated decisions, correction outcomes, improper processing, and independently validated AML/CFT and whistleblower controls. My prior proposal seeks reform of the BSA and FOIA and enforceable consumer rights to obtain and correct nonprotected data, challenge adverse decisions, preserve material evidence and obtain remedies. Do not require disclosure of suspicious activity reports or protected investigative information; preserve legitimate confidentiality and permit controlled access to independently existing records where lawful. New private rights and broader statutory disclosure changes require congressional action.

Foreign operational exposure should be measured by relevant infrastructure jurisdiction, privileged access, control and dependencies, not unsupported assumptions based on nationality. Propose reportable foreign-interest lobbying expenditure, qualifying principals, conflicts and established violations of applicable foreign-influence, sanctions or federal-funds restrictions. Coordinate with the agencies possessing legal jurisdiction. Lawful foreign commerce and protected political activity do not constitute misconduct. Any targeted operational hold for ongoing material unlawful activity must be supported by statutory authority, evidence and due process; preserve innocent depositors' rights.

XVII. Existing supervisory and enforcement powers

I request an evidence-based escalation matrix linking verified findings to existing lawful powers. The following authorities are distinct from proposed new capital formulas or automatic sanctions. [14, 19–22]

Existing authority	Proposed review or action
12 C.F.R. §§ 3.123, 217.123, 324.123	Evaluate model qualification, corrective plans and modified advanced-approaches calculations where the applicable criteria are met.
12 U.S.C. § 1831o(g)	Evaluate more stringent treatment of insured depository institutions determined unsafe or unsound after required notice and opportunity for hearing; not automatic reclassification.
12 U.S.C. § 1831p-1(a), (b), (e)	Evaluate binding safety-and-soundness standards and deficiency plans; require orders upon statutory plan failure, including applicable growth or tangible equity measures.
12 U.S.C. § 1818(b)(6)	Evaluate restitution and other affirmative relief within existing enforcement authority; restitution predicates include unjust enrichment or reckless disregard as specified.
12 U.S.C. § 1817(b)(1)	Consider validated Deposit Insurance Fund risk factors through lawful assessment rulemaking.

Section 1831p-1(e)(1)(A) distinguishes standards prescribed by regulation, for which an agency must require an acceptable corrective plan upon the covered finding, from guideline standards, for which such a plan is discretionary. The statute also provides for corrective orders upon failure to submit or materially implement a required plan, with additional restrictions under specified conditions. This distinction supports my petition for binding operational, internal-control, information-system,

loan-documentation, underwriting and compensation standards within existing statutory authority. It does not make all supervisory guidance enforceable or direct regulators to find a violation without evidence.

Establish an interagency review protocol for independently established material failures, repeat violations and inadequate remediation; document supervisory disposition and reasons. Consider restitution, removal of unlawful financial gains, growth restrictions, rescission or qualified staffing under § 1818(b)(6) when legal predicates are met. New mandatory penalties, expanded private rights of action, treble damages, categorical insurance disqualification and automatic operational holds require any necessary legislative or regulatory changes. Distinguish enforcement findings from allegations; preserve procedural rights.

XVIII. Burden estimates and actual reporting costs

The October 16 notice provides the following annual estimates. [1] The respondent counts are reporting categories, not necessarily unique organizations because different legal entities within a group may report.

Respondent category	Count	Hours per quarter	Annual hours
OCC national banks / federal savings associations	10	674	26,960
Board state member banks	4	674	10,784
Board BHCs/SLHCs — SLR tables only	5	3	60
Board other BHCs/SLHCs	9	677	24,372
Board intermediate holding companies	7	3	84
FDIC insured state nonmember bank / savings association	1	674	2,696
Total reporting-category count and annual hours	36	—	64,956

The totals are derived from published category counts and hours; the full-year estimates are counts multiplied by quarterly burden and four. They are not audited actual workloads. The OCC ICR separately records $0 dollar-cost burden, which must not be confused with zero economic cost. Request the objective basis for all burden estimates, actual respondent experience, methodology and treatment of in-house labor, independent verification, start-up systems, vendor services, ongoing maintenance, corrections and exceptional workloads. [1–2, 6]

Burden reduction should target manual re-entry, conflicting definitions, duplicate submissions and avoidable reconciliation costs, not the elimination of essential financial accountability. Evaluate incremental costs and benefits of proposed collections separately, including costs shifted to consumers, employees, agencies and the public. Quantify reporting hours and non-labor costs through a representative pilot before requiring new fields. Acknowledge that capital and prudential costs belong in separate substantive assessments where applicable.

XIX. Secure interoperable regulatory reporting infrastructure

Develop a common data dictionary, legal-entity and provider identifiers, standardized units, field-level mappings, machine-readable submission specifications and secure transmission. Preserve raw submissions, corrections, version histories, audit records, authenticated receipt identifiers and incident recovery. Establish secure role-based access, validation at source, clear error messages and monitored exception queues. Provide accessible alternative submission channels, receipt confirmation and continuity for public comments as well as institutional reports.

Regulators should apply to their own infrastructure appropriate cybersecurity, availability, integrity and evidence-preservation standards. Automation must increase accuracy, transparency and timely use, not obscure source records or exclude persons from the administrative process. Require external testing of reporting-system resilience, privacy controls and correction workflows. Do not publish exploitable vulnerability details or personally identifying consumer or whistleblower information.

XX. Federal Regulatory Accountability Index

The proposed accountability measures should assess agency performance as well as private-sector risk. Develop aggregate metrics for complaint acknowledgment and disposition; time from material finding to supervisory response; referrals accepted or returned; repeated violations after intervention; independently verified corrective-action closure; restitution ordered versus delivered; substantiated retaliation outcomes; reporting discrepancies and correction timeliness; and reporting-portal outages and recovery.

Create an Interagency Accountability and Referral Register that identifies a responsible authority, referral date, status, next procedural step, outcome category and reason for closure. Publish aggregate nonconfidential statistics. Protect confidential supervisory information, legitimate investigative confidentiality, whistleblower identities and sensitive security details. The existence of a complaint or referral is not a finding. The objective is transparent responsibility, prevention of jurisdictional gaps and a verifiable record of whether collected information actually supports agency functions.

XXI. Implementation, data standards and allocation of responsibility

I propose the following schedule, measured from the effective date of applicable authority or approval. All deadlines below are proposed policy milestones, not existing legal requirements. Existing reporting continues during modernization. Do not impose an unapproved mandatory collection.

Proposed milestone	Deliverable and responsibility
90 days	OCC, Board, FDIC and OIRA review: establish task force, assign a lead agency for each workstream, inventory actual uses and review certification record.
180 days	Publish nonconfidential reporting-gap analysis, scope crosswalk and objective burden assumptions; identify existing data that can be reused.
270 days	Develop SOCGR and REPAS data definitions, privacy safeguards, QA criteria, pilot design and reviewer roles.

Proposed milestone	Deliverable and responsibility
12 months	Seek renewed approval and launch appropriately cleared pilot; test accuracy, completeness, usability, respondent time and cost.
18 months	Evaluate ORCA and concentration-index methodologies, scenario testing, DIF risk relevance and possible binding standards; seek separate public comment.
24 months	Implement approved supplemental collection and associated controls, with proportionate phased coverage; refer necessary legislation to Congress.
Annually	Publish nonconfidential aggregate results, recurrence, remediation, reporting burden and agency accountability; revise based on evidence.

The Federal Reserve should lead systemic concentration and prudential methodology; OCC and FDIC should coordinate examination, institution-level reporting and independent closure criteria; FDIC should evaluate DIF risk; OMB/OIRA should review practical utility, burden and duplication. Coordinate with CFPB for consumer protection, Treasury/FinCEN for BSA matters, DOL/NLRB for their respective labor and whistleblower jurisdictions, and Congress for newly proposed statutory rights and eligibility restrictions. NCUA may consider corresponding measures in separate credit-union proceedings; it is not a signatory to this FFIEC 101 notice.

For any pilot, define data owner, validation rules, reporting frequency, error handling, legal collection authority, confidentiality classification, retention, publication policy and thresholds for any follow-up. Collaborate with institutions of varying complexity and independent experts. Use secure structured fields rather than unbounded narrative where suitable. Evaluate accuracy and respondent burden before expanding coverage; revise definitions that do not demonstrate incremental practical utility.

XXII. Formal requests and petition

I respectfully request that the OCC, Board, FDIC and OMB take the following actions within their respective authority:

- Preserve ongoing FFIEC 101 reporting while reconsidering an unconditional three-year extension; approve a shorter 12-month period if appropriate and establish a documented modernization review.
- Include this comment in the agency and OMB review records; provide a reasoned nonconfidential response to practical-utility, actual-use, certification and burden questions; grant an opportunity to be heard under § 3508 where appropriate.
- Map existing collections and assess gaps before establishing SOCGR, REPAS, the concentration index, IGS and the supplemental registers, with a properly cleared pilot and independently tested data controls.
- Evaluate ORCA, risk-based assessment refinements, capital recalculation reviews, growth restrictions and other lawful remedies using validated evidence and without double counting or automatic adverse determinations.
- Develop independent assurance, non-recurrence and predeployment review criteria, consumer restitution reconciliation, financial injury and misconduct-adjusted profitability measures, and

protected workforce governance safeguards.

- Establish interoperable and secure regulatory data submission, publish nonconfidential aggregate accountability measures, and document agency referral and remediation effectiveness.
- Initiate separate proceedings for binding standards and substantive prudential amendments; coordinate with the proper authorities and refer proposed statutory reforms, including the historical servicing prohibition, enhanced consumer/worker rights and abolition of compulsory arbitration, to Congress.

This comment also constitutes a petition, pursuant to 5 U.S.C. § 553(e), for the issuance or amendment of rules within the recipient agencies' lawful jurisdiction, including safety-and-soundness standards under 12 U.S.C. § 1831p-1. Please process that petition separately as appropriate and provide a reasoned disposition consistent with 5 U.S.C. § 555(e) where applicable. I request consideration of the entire submission in the information-collection review and related proceedings; I do not contend that all substantive reforms may be adopted by extension of an OMB control number.

XXIII. Conclusion

Capital adequacy cannot be assessed comprehensively without evaluating the reliability of the financial records, technological infrastructure, personnel and institutional controls responsible for financial activity. Regulatory information must do more than describe historical financial loss: it must support prevention, accountability and independently verifiable remediation.

The American public must not bear the costs of institutional misconduct or technological expansion while private institutions retain the profits and federal protections. Federal protection is not an entitlement to institutional impunity.

Respectfully submitted,

Anwar Abu-Shayed, M.S.

Cybersecurity | Enterprise Risk Management | Institutional Governance

Connecticut, United States

Authorities and source record

References are provided as static, searchable text for the administrative record. The proposed mechanisms, names, metrics and timelines in this submission are original policy recommendations, not existing requirements. The official collection notice is the basis for the burden calculations and deadline. Numerical FR Y-15 aggregates from a separately discussed dataset are not relied upon here because the source data have not been independently reproduced.

[1] Joint FFIEC 101 notice, 91 FR 65843–65845 (Oct. 16, 2026), FR Doc. 2026-21185; initial notice 91 FR 34347 (June 5, 2026). https://www.federalregister.gov/d/2026-21185

[2] OMB/OIRA, OCC ICR 202610-1557-001, OMB 1557-0239. https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202610-1557-001 — Public ICR summary consulted; this comment does not represent a review of every underlying certification attachment or a finding that the certification is inaccurate.

[3] FFIEC, FFIEC 101 current reporting forms and description. https://www.ffiec.gov/resources/reporting-forms/ffiec101

[4] Federal Reserve, FR Y-15, Systemic Risk Report. https://www.federalreserve.gov/apps/reportingforms/Report/Index/FR_Y-15

[5] Federal Reserve, FR Y-14Q Capital Assessments and Stress Testing, including Schedule E operational risk and associated Q&A. https://www.federalreserve.gov/apps/reportingforms/Report/Index/FR_Y-14Q ; https://www.federalreserve.gov/publications/fr-y-14-qas/fr-y-14q.htm

[6] 44 U.S.C. § 3506(c), agency responsibilities, review and certification. https://uscode.house.gov/us/usc/t44/s3506/

[7] 44 U.S.C. §§ 3507(f)–(h), 3508, approval, renewal and hearing; 5 U.S.C. §§ 553(e), 555(e). https://uscode.house.gov/us/usc/t44/s3507/ ; https://uscode.house.gov/us/usc/t44/s3508/

[8] 5 C.F.R. § 1320.3(b), (l), burden and practical utility. https://www.ecfr.gov/current/title-5/section-1320.3

[9] U.S. Treasury, Opportunities and Challenges in Online Marketplace Lending (May 10, 2016). https://home.treasury.gov/news/press-releases/jl0452

[10] Proposed Third-Party Risk Management Guidance, 91 FR 58536–58544 (Sept. 15, 2026), FR Doc. 2026-18859; existing guidance, 88 FR 37920 (June 9, 2023). https://www.regulations.gov/docket/OCC-2026-0793 — Prior submission by the undersigned addresses individual enforcement history and broader legislative reforms.

[11] Benjamin Read and Rami McCarthy, Wiz Research, “Black October” for AI Developer Platforms (Oct. 30, 2026, subsequently updated). https://www.wiz.io/blog/black-october-for-ai-developer-platforms

[12] Cloud Security Alliance, Black October: Concentration Risk in the AI Build-and-Host Layer (Nov. 5, 2026). https://labs.cloudsecurityalliance.org/research/csa-research-note-ai-developer-platform-concentration-risk-2/

[13] Financial Stability Board, Enhancing Third-Party Risk Management and Oversight: A Toolkit for Financial Institutions and Financial Authorities (Dec. 4, 2023). https://www.fsb.org/uploads/P041223-1.pdf

[14] 12 C.F.R. §§ 3.123, 217.123, 324.123, ongoing qualification. https://www.ecfr.gov/current/title-12/section-3.123 ; https://www.ecfr.gov/current/title-12/section-217.123 ; https://www.ecfr.gov/current/title-12/section-324.123

[15] Interagency computer-security incident notification rules, 12 C.F.R. part 53, part 225 subpart N and part 304 subpart C, as applicable.

[16] Basel Committee on Banking Supervision, Implementation of the Principles for effective risk data aggregation and risk reporting (BCBS 239 Principles) (2026). https://www.bis.org/publications/implementation-principles-effecti

ve-risk-data-aggregation-and-risk-reporting-bcbs-239-principles

[17] 12 C.F.R. § 217.161, qualification requirements for operational risk mitigants. https://www.ecfr.gov/current/title-12/section-217.161

[18] Bureau of Labor Statistics, Union Members — 2025, USDL-26-0229 (Feb. 18, 2026); 29 U.S.C. §§ 157–158. https://www.bls.gov/news.release/union2.htm

[19] 12 U.S.C. § 1817(b), risk-based deposit insurance assessments. https://uscode.house.gov/us/usc/t12/s1817/

[20] 12 U.S.C. § 1831o(g), more stringent treatment based on other supervisory criteria. https://uscode.house.gov/us/usc/t12/s1831o/

[21] 12 U.S.C. § 1831p-1, safety and soundness standards and corrective plans. https://uscode.house.gov/us/usc/t12/s1831p-1/

[22] 12 U.S.C. § 1818(b)(6), affirmative action to remedy violations or practices. https://www.law.cornell.edu/uscode/text/12/1818