PUBLIC RECORDS / WORKED EXAMPLE

Johnson Controls: settlement and cybersecurity assurance

Checking contractor cybersecurity | Part 1

Prepared by Dossier Editorial | November 14, 2026

EVIDENCE SOURCES	EVIDENCE CHECKED	PUBLISHER INSTITUTIONS
5	2026-11-14	3

SECTIONS	READER QUESTIONS	REVIEW SCOPE
7	6	Public records

EVIDENCE CHECKED	2026-11-14
EDITION	1 | Public-source research
ARTICLE	dossierplus.ai/blog/johnson-controls-cybersecurity-settlement-compliance-evidence

IMPORTANT USE NOTE

Prepared by Dossier Editorial with AI assistance from public records. This educational document review does not claim a live Dossier investigation, technical security assessment, human approval or legal review. It is not a legal opinion or a certification of any contractor's present compliance.

Generated by Dossier · Doc ID DSR-VGSE-S8ZV-Z47T · Seal 5C9437A9F747 · SHA-256 EBF3A9B182AA9DFF · Issued 2026-11-14 17:15 UTC

PART 01

The decision in brief

No. The Johnson Controls agreement announced by DOJ on November 13, 2026 resolves specified historical allegations; it is not a current NIST SP 800-171 assessment or certification. The three corporate defendants agreed to a $5 million settlement plus interest without admitting liability. A present compliance conclusion requires evidence tied to the relevant contractor, contract requirements, information system and assessment period.

Publication date: November 14, 2026. Historical event dates are identified separately. This PDF and the article use the same structured source selection and findings.

PART 02

Executive summary: resolution is not assurance

A settlement answers a defined legal question. A security assessment answers whether specified safeguards are implemented and effective within a defined system. Those questions require different evidence. This case shows how to preserve that distinction when a vendor questionnaire asks whether an enforcement matter has been resolved.

- Established: a signed agreement addresses alleged cybersecurity failures during January 1, 2018-August 1, 2025, associated with 25 listed contract and subcontract entries.
- Qualified outcome: the agreement contains no admission of liability. Its government monetary release for covered conduct is conditional on receipt of the settlement amount and subject to reservations.
- Open here: current contract-specific compliance, payment receipt and later filed dismissals were not independently verified. [S1]

The parent company's latest annual report describes security monitoring and external assessments. That is relevant company context, but it does not supply the assessment results for the contract and system a reader may be evaluating. [S5]

PART 03

Identify the entity, contract and system

The agreement defines JCI as Johnson Controls, Inc., Johnson Controls Fire Protection LP and Johnson Controls Security Solutions LLC. Keep these parties distinct from the SEC reporting parent, Johnson Controls International plc. A shared brand does not make every subsidiary, contract or system interchangeable. [S1] [S5]

IDENTITY FIELD	VERIFIED EXAMPLE	REVIEW CONSEQUENCE
Civil actions	1:24-cv-2500, Northern District of Georgia; 1:26-cv-448, District of Columbia	Use court plus docket number; avoid a company-name-only match. [S1]
Exhibit scope	Exhibit A contains 25 numbered entries.	Entries can contain multiple instruments; this is not a count of 25 distinct systems. [S1]
Worked contract identifier	Entry 16: subcontract KSCFL24008 under prime 80KSC024FA049.	Record both identifiers. The exhibit alone does not define the system boundary or prove present performance. [S1]

Generated by Dossier · Doc ID DSR-VGSE-S8ZV-Z47T · Seal 5C9437A9F747 · SHA-256 EBF3A9B182AA9DFF · Issued 2026-11-14 17:15 UTC

IDENTITY FIELD	VERIFIED EXAMPLE	REVIEW CONSEQUENCE
Applicable requirements	The actual contract, incorporated clauses and amendments.	Verify the required standard and revision for the period being assessed; these instruments were not reviewed here.
Current system and evidence period	Named system boundary, assessment date and scope.	A parent-level program statement cannot supply these missing details.

For the worked example, the defensible starting record is “listed subcontract; current system assurance unresolved.” Do not expand it to “all Johnson Controls systems failed” or “all systems are now compliant.” Neither conclusion follows from this agreement.

PART 04

Chronology: conduct, signatures, filing and announcement

DATE	DOCUMENTED DEVELOPMENT	WHAT THE DATE MEANS
January 1, 2018-August 1, 2025	The government alleges failures within this period.	Alleged historical conduct, not a finding about today’s systems. [S1]
June 7, 2024; February 11, 2026	The agreement recites the filing dates of the Georgia and D.C. actions, respectively.	Case history described in the agreement; underlying complaints were not reviewed. [S1]
October 19, 2026	Latest signature date visible in the signed counterparts.	Paragraph 23 defines effectiveness by the last signatory’s date. This is separate from the later announcement. [S1]
November 12, 2026	Johnson Controls International plc files its FY2026 Form 10-K.	Current company disclosure, including Item 1C on cybersecurity. [S5]
November 13, 2026	DOJ announces the $5 million settlement.	Announcement of the agreement; not a payment receipt. [S2]
November 14, 2026	This review checks the agreement, announcement, NIST guidance and annual report.	Evidence-check and article publication day; no technical testing performed.

Some signature pages are scans with little extractable text. We visually checked the counterparts and Exhibit A rather than assigning the press-release date to every event. Keeping these dates separate prevents an announcement from becoming an invented execution or payment date.

PART 05

Findings: the supported outcome and the material gaps

The government’s allegations include inadequate knowledge and control of relevant systems, access restrictions, system security plans and plans of action. These are allegations in Recital I, not technical findings made by this article. Recital J provides both that JCI does not admit liability and that the United States does not concede its claims lacked foundation. [S1]

Generated by Dossier · Doc ID DSR-VGSE-S8ZV-Z47T · Seal 5C9437A9F747 · SHA-256 EBF3A9B182AA9DFF · Issued 2026-11-14 17:15 UTC

The $5 million obligation includes interest under paragraph 1. Paragraph 4 conditions the government's covered-conduct monetary release on receipt; paragraph 13 connects receipt to filing dismissal stipulations. Paragraph 6 preserves specified claims and authorities. None of those provisions is a remittance record, a filed dismissal or evidence of an actual suspension or debarment. [S1]

Free docket searches did not yield the later filings for these two matters. We did not review a payment receipt or filed dismissal stipulation, and this is not a complete docket certification. The bounded result is an agreed settlement with those completion steps unverified in this review—not a claim that payment or dismissal has failed to occur.

The November 12 parent filing describes round-the-clock monitoring, vulnerability assessments, and third-party penetration testing and maturity assessments. These are the company's descriptions of its program. Item 1C does not provide the underlying results needed to assess the worked subcontract's particular system. The disclosure is useful contrary context to any assumption that the historical allegations describe every current control. [S5]

NIST's assessment guidance distinguishes the system security plan's description of the environment and safeguards from assessment of their implementation and effectiveness. A plan can identify what should be in place; it does not, by itself, demonstrate that each safeguard works. For a current review, seek the relevant assessment scope, results, exceptions and subsequent closure evidence. [S3]

There is also a version trap. NIST's catalog marks SP 800-171 Revision 2 withdrawn and superseded by Revision 3 on May 14, 2024. That catalog status does not show that a particular contract was amended. Match the obligation to the actual contract and relevant period before using either revision as the review benchmark. [S4]

These five source items serve different roles: an agreement, an agency announcement, two NIST reference pages and an issuer filing. They are not five independent audits. No current system security plan, assessment report, contract amendment or remediation closure record was obtained.

PART 06

Decision tree: can the present compliance question be answered?

1. HAVE YOU MATCHED THE EXACT CONTRACTOR, CONTRACT AND SYSTEM?

- If established: Record legal entity, prime and subcontract identifiers, system boundary and assessment period before interpreting evidence.
- If unresolved: Keep scope unresolved. A brand name, settlement headline or parent filing cannot fill those identity fields.

2. DO YOU HAVE THE APPLICABLE CLAUSES AND STANDARD REVISION?

- If established: Map each requirement to the instrument that imposes it, including amendments and relevant dates.
- If unresolved: Obtain the contract requirements through an authorized channel. Do not substitute the newest standard for an unverified contractual obligation.

Generated by Dossier · Doc ID DSR-VGSE-S8ZV-Z47T · Seal 5C9437A9F747 · SHA-256 EBF3A9B182AA9DFF · Issued 2026-11-14 17:15 UTC

3. IS THERE A SCOPED ASSESSMENT WITH RESULTS AND TREATMENT OF OPEN FINDINGS?

- If established: Check who performed it, when, which systems and requirements it covers, its limitations, and evidence supporting any claimed closure.
- If unresolved: Record current compliance as unverified. A policy, security plan or statement that testing occurs is insufficient for the missing result.

4. ARE YOU ALSO BEING ASKED WHETHER THE LITIGATION AND PAYMENT STEPS ARE COMPLETE?

- If established: Review the agreement's conditions, actual payment evidence and filed dispositions separately from the technical assessment.
- If unresolved: Keep the legal settlement as context. Do not treat it as a technical pass or a current failure finding.

5. DOES NEW EVIDENCE ALTER THE SCOPE OR OUTCOME?

- If established: Add a dated finding, retain the earlier version and explain exactly which conclusion changed.
- If unresolved: State the review date and coverage. Missing evidence supports an open question, not an assumed answer.

The tree is an evidence-review method. Contract interpretation and technical assurance may require qualified review; this public walkthrough performs neither on the reader's behalf.

PART 07

Reproduce the review in Dossier

- Frame one testable question: "What evidence supports current compliance for subcontract KSCFL24008's relevant system and period?" Track settlement completion as a separate question.
- Preserve the five public originals with their URLs, retrieval dates and file hashes. Note that scanned signatures need visual review and that the SEC filing is a parent-company statement.
- Record the three agreement parties, two court/docket identifiers and the exhibit's prime/subcontract pair in case notes or an attached inventory. Leave unknown system and contract-version fields explicitly unresolved.
- Build the dated chronology above. Distinguish alleged conduct, signature dates, issuer disclosure, public announcement and this review's evidence date.
- Link each finding to a precise source location: Recital I for allegations, paragraphs 4 and 13 for conditional completion steps, Exhibit A for the contract entry, and Item 1C for the company's account.
- Create separate open evidence tasks for contract scope, current assessment results, remediation closure, payment receipt and filed disposition. Do not mark one task complete merely because another is supported.
- Before exporting, reconcile the executive summary with the evidence table and unanswered questions. Keep any later nonpublic security material in its authorized workspace; a public article needs no sensitive configuration details.

This describes a reproducible authoring workflow. No live Dossier matter was created or investigated, no assessment was commissioned and no provider was contacted. The downloadable report uses the same public-source content as this article.

Generated by Dossier · Doc ID DSR-VGSE-S8ZV-Z47T · Seal 5C9437A9F747 · SHA-256 EBF3A9B182AA9DFF · Issued 2026-11-14 17:15 UTC

PART 08

What evidence would change the conclusion?

- A matched contract and amendments would establish which requirements apply to the specific legal entity, system and period.
- A scoped assessment, its limitations and evidence supporting closure of relevant findings would support a more precise present assurance conclusion. A list of planned actions alone would not establish completion.
- A receipt or other authoritative payment record, plus the actual filed dispositions, would resolve the settlement-completion questions within their documented scope.
- A later original government action or company filing could justify a follow-up. Retain the previous record and explain the change instead of silently replacing the historical finding.

The related CISA KEV walkthrough asks a complementary question: whether a public vulnerability entry establishes exposure in a particular vendor deployment. Both reviews require a precise match between a public record and the system about which a decision is being made.

PART 09

Questions readers ask

DOES THE JOHNSON CONTROLS SETTLEMENT CERTIFY CURRENT NIST SP 800-171 COMPLIANCE?

No. It addresses defined historical allegations. Current assurance requires evidence matched to the contractor, contract, system, applicable requirements and assessment period; the settlement does not supply that assessment. [S1] [S3]

DID JOHNSON CONTROLS ADMIT LIABILITY?

No. Recital J contains no admission of liability by JCI and no concession by the United States that its claims lacked foundation. DOJ says the resolved claims are allegations and there has been no determination of liability. Neither qualification is a current technical compliance finding. [S1] [S2]

HAS THE $5 MILLION BEEN PAID?

This review did not obtain payment evidence. The agreement requires $5 million plus interest, and the announcement says the companies agreed to pay. Those documents alone do not verify receipt or the later filing of dismissal stipulations. [S1] [S2]

IS A SYSTEM SECURITY PLAN THE SAME AS AN ASSESSMENT?

No. NIST describes a plan as documenting the system environment, requirements and their implementation. Assessment examines implementation and effectiveness. A current assurance review needs results and scope, not merely evidence that a plan exists. [S3]

Generated by Dossier · Doc ID DSR-VGSE-S8ZV-Z47T · Seal 5C9437A9F747 · SHA-256 EBF3A9B182AA9DFF · Issued 2026-11-14 17:15 UTC

DOES REVISION 2'S WITHDRAWAL AUTOMATICALLY CHANGE AN EXISTING CONTRACT?

The NIST catalog records withdrawal and supersession, not the terms of a particular contract. Check incorporated clauses and amendments before selecting the applicable revision. No contract amendment was reviewed in this case walkthrough. [S4]

WHAT REMAINS UNRESOLVED AS OF NOVEMBER 14, 2026?

Contract-specific current compliance, the worked example's system boundary and assessment results, payment receipt and filed dismissals remain unverified here. The company's annual report supplies program context but not the missing contract-specific assessment. [S5]

PART 10

Linked source register

Titles with a recorded URL link to that source. Entries without a URL identify retained material but do not open an original file. For any court or business record being used in litigation, obtain a certified copy directly from the clerk or filing authority and preserve the retrieval date.

S1 **Signed Johnson Controls cybersecurity settlement agreement**
Original signed settlement agreement. Anchor: Recitals A-C and I-J; paragraphs 1, 4, 6, 13 and 23; signature counterparts; Exhibit A entry 16. 17-page original. Latest visible signature October 19, 2026. Allegations, defined release and reserved matters; not payment, dismissal or current security-assessment proof. · retrieved 2026-11-14

S2 **Johnson Controls and subsidiaries agree to pay $5 million**
Original agency announcement. Anchor: November 13, 2026 release 26-1360; settlement summary; final liability qualification. Agency announcement links the agreement. Same publisher as S1; announcement date is not an execution or receipt date. · retrieved 2026-11-14

S3 **NIST SP 800-171A assessment: purpose and scope**
Original standards guidance. Anchor: Purpose; Scope; system security plan and assessment of implementation and effectiveness. General assessment methodology. Not a Johnson Controls assessment or a determination of a specific contract's requirements. · retrieved 2026-11-14

S4 **NIST SP 800-171 Revision 2 publication record**
Original publication and version record. Anchor: Withdrawn May 14, 2024; superseded by SP 800-171 Revision 3. Catalog history, not evidence that a particular government contract was amended. · retrieved 2026-11-14

S5 **Johnson Controls International plc FY2026 Form 10-K**
Original issuer annual filing. Anchor: Filed November 12, 2026; year ended September 30, 2026; Item 1C Cybersecurity, printed pages 25-26. Parent CIK 833444; company-described security program. Underlying contract-specific assessment reports were not supplied by this disclosure. · retrieved 2026-11-14

Generated by Dossier · Doc ID DSR-VGSE-S8ZV-Z47T · Seal 5C9437A9F747 · SHA-256 EBF3A9B182AA9DFF · Issued 2026-11-14 17:15 UTC