IR.L2-3.6.2

Incident Response

Incident Reporting

"Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization."

Objectives

[a]
Incidents are tracked.

[b]
Incidents are documented.

[c]
Authorities to whom incidents are to be reported are identified.

[d]
Organizational officials to whom incidents are to be reported are identified.

[e]
Identified authorities are notified of incidents.

[f]
Identified organizational officials are notified of incidents.

Key Discussion Points

Internal & External:
Internal officials (management) AND external authorities must both be named — DFARS 252.204-7012 requires DoD notification within 72 hours.

Track AND Document:
Tracking is real-time status. Documentation is the record. Both are required — a mental note or Slack message does not constitute either.

Suspected Incidents Too:
You don't need confirmation to report — the guide explicitly states that suspected incidents including suspicious emails should be tracked.

DFARS 72-Hour Clock:
Under DFARS 252.204-7012, cyber incidents affecting CUI must be reported to DoD via the DIBNet portal within 72 hours of discovery.

Assessment Methods

EXAMINE

Incident response policy; procedures addressing incident monitoring and reporting; incident response records and documentation; incident reporting records; incident response plan; system security plan.

INTERVIEW

Personnel with incident monitoring responsibilities; personnel with incident reporting responsibilities; personnel who have or should have reported incidents; personnel (authorities) to whom incident information is to be reported; personnel with information security responsibilities.

TEST

Incident monitoring capability; mechanisms supporting tracking and documenting of incidents; organizational processes for incident reporting; mechanisms supporting incident reporting.

IR.L2-3.6.2

INCIDENT RESPONSE — Incident Reporting

Plain English

What this control is really saying:

When an incident occurs, it has to be tracked, documented, and reported — not just handled quietly. This control requires that you know who to notify (internally and externally), that every incident gets a record, and that the right people are actually told. For DIB contractors, this includes a mandatory 72-hour report to DoD under DFARS 252.204-7012.

How it is used:

- Every incident opens a tracking ticket — assigned to a handler, timestamped, and updated until closure with a documented resolution.
- The IRP names the CEO and IT admin as internal reporting officials — any confirmed incident triggers immediate notification to both.
- The IRP identifies the DIBNet portal and the contracting officer as external reporting contacts — the 72-hour DFARS clock is explicitly documented.
- Incident records are retained for three years and include the initial report, actions taken, timeline, and final disposition.

Real World Example

The Scenario

Acme Defense had a suspected ransomware event six months ago. The IT admin isolated the affected machine and restored from backup. No ticket was opened, no documentation was created, and nobody outside IT knew it happened — not management, not the prime contractor.

What the assessor finds

The incident was never tracked or documented. No internal officials were notified. The DoD was never notified via DIBNet — the 72-hour DFARS reporting window was missed entirely. No external authorities are identified in any policy or plan. The incident effectively did not exist on paper.

SPRS Score Impact

3.6.2 carries a point value of 5. Failure to report a cyber incident to DoD within 72 hours is a direct DFARS violation — organizations that handle incidents quietly without documenting or reporting face both compliance and contract performance risk.

What Good Looks Like

All incidents tracked in a ticketing system from open to close, incidents documented with timeline and actions, internal and external reporting officials named in IRP, 72-hour DFARS reporting procedure documented, suspected incidents tracked, records retained.

Common Gaps

What assessors actually find in the field:

✗ **No incident tracking system**

Incidents are handled verbally or via Slack — no ticket, no record, no timeline exists for any past incident.

✗ **External authorities undefined**

The IRP lists internal contacts but never identifies the DIBNet portal or contracting officer as required external reporting authorities.

✗ **DFARS deadline unknown**

The IT admin is unaware of the 72-hour reporting requirement under DFARS 252.204-7012 — no procedure exists to meet it.

✗ **Incidents not reported internally**

The IT admin handles incidents alone without notifying management or legal — internal reporting officials are not defined.

✗ **Suspected incidents not tracked**

Only confirmed incidents are tracked — phishing attempts and suspicious activity are handled informally with no record.