ISI

Scoping: Drawing Your Boundary

The single decision that drives the size, cost, and difficulty of everything else.

John Nolan | Aug 17 | 1:45pm

1

STEP 1 OF 6

Review & Confirm

You can't scope what you haven't counted.

PEOPLE

- Employees with CUI access
- Contractors & subcontractors
- Temporary or contingent staff

Ask: *Role, access level, vetting status?*

HARDWARE

- Workstations, laptops, servers
- Mobile devices & removable media
- Network gear, printers, IoT/OT

Ask: *On-prem, cloud, or remote — who owns it?*

SOFTWARE

- Business & engineering apps
- Cloud / SaaS platforms
- Email, file-share, collaboration tools

Ask: *Does it touch CUI — even briefly?*

Categorize as you go — tag every asset to its CUI category and the NIST SP 800-171 requirement families it triggers, not just a yes/no flag.

ISI INSIGHT Most inventories miss shadow IT/BYOD, personal cloud storage, forgotten legacy systems, and orphaned service or API accounts.

2

STEP 2 OF 6

Know Your Vendors

Your compliance boundary extends to every vendor touching CUI.

SCOPE RED FLAGS

- Stores, processes, or generates CUI
- Can access systems that touch CUI
- Ownership responsibilities undocumented — no Shared Responsibility Matrix

WHAT TO REQUEST

- Certification status — FedRAMP, CMMC, ISO
- A Shared Responsibility Matrix, mapped to NIST SP 800-171 Rev 2 objectives

Get it in writing — a signed Shared Responsibility Matrix beats a verbal assurance every time.

ISI INSIGHT Fourth-party risk counts too — your vendor's own subcontractors and sub-processors can extend your CUI boundary.

3

STEP 3 OF 6

Visualize in Detail

If you can’t see the data flow, you can’t defend the boundary.

NETWORK DESIGN DIAGRAM

- A visual layout of your IT infrastructure
- Every system, connection & boundary

CUI DATA FLOW DIAGRAM

- Traces how CUI moves through your environment
- System to system, step by step

Draw both — the network diagram shows where CUI could go; the data flow diagram shows where it actually goes.

ISI INSIGHT Interview your staff to map how CUI actually flows today — not the ideal state on paper.

STEP 4 OF 6

4 Reduce Exposure

Smaller scope, lower cost, less risk.

With your inventory and diagrams complete, use them to pinpoint:

1	**WHERE CUI LIVES**	Exactly which systems store, process, or transmit it.
2	**WHO HAS ACCESS**	Every user who can currently can access CUI – whether they need to or not.
3	**WHERE TO CUT**	Assets and access you can segment or scope out entirely.

Bottom line — fewer systems in scope means fewer systems to secure, assess, and maintain.

5

STEP 5 OF 6

Minimize Disruption

Enclaves cut risk — but only if the trade-offs pencil out.

COST QUESTIONS

- Build vs. migrate: what's the true cost of an enclave vs. going enterprise-wide?
- Payback: do build savings outweigh added management overhead?

OPERATIONS QUESTIONS

- Split duty: do users split time between defense and non-defense contracts?
- Commercial carve-outs: what functionality must stay outside the enclave?
- Day-to-day friction: how would two tenants affect daily operations?

No universal answer — weigh cost and operational trade-offs against your specific contract mix.

ISI INSIGHT Enclaves work best when defense and commercial duties are cleanly separable — heavy overlap often favors going enterprise-wide instead.

STEP 6 OF 6

6

Build for the Long Term

Compliance is a journey, not a point-in-time check.

- **Map today's scope to tomorrow's contracts** — Factor in current and pipeline CDRLs / DD254s.
- **Set scope triggers** — New contracts, M&A, org changes, new CUI categories.
- **Keep the SSP & POA&M living** — Not one-time deliverables — revisit them on a cadence.
- **Build in headroom** — A foundation that scales, not one you rebuild.

Get the foundation right, and every future contract builds on it.