ECHELON
RISK +
CYBER

PJ DICK

CMMC READINESS FOR PJ DICK, TRUMBULL, AND THE LINDY GROUP

How Echelon Supported a Leading Construction Firm in Preliminary Gap Analysis for CMMC Level 2 Compliance

BACKGROUND AND CONTEXT

A Family of Construction Leaders Strengthening Its Security & Compliance Posture

PJ Dick, Trumbull, and The Lindy Group (recognized as one of the Northeast's most respected heavy civil and building contractors) operate across complex, high-security environments.

The teams frequently perform work inside federal facilities and other sensitive locations, where strong physical and digital safeguards are essential.

The company started to see advanced compliance requirements appear more frequently in bid submissions, shortlist presentations, and pre-award evaluations. This included Department of Defense advanced CMMC certifications, DFARS, and NIST-based requirements.

"We started seeing things trickle down from certain jobs involving DFARS," shared Matt Lawson, Information Security Officer at PJ Dick–Trumbull–Lindy. **"Suddenly it wasn't just 'tell us what you do,' it was 'prove it,' complete with SPRS scores and evidence."**

- Matt Lawson, Information Security Officer at PJ Dick–Trumbull–Lindy.

For an organization committed to maintaining eligibility for government projects, beginning to adapt before the DoD required certification was the right strategic move.

"The companies wanted to continue pursuing government work. Compliance is a requirement for that. And honestly, it just makes sense for business and modernization overall," said PJ Dick–Trumbull–Lindy's CIO Todd Porterfield.

- Todd Porterfield, Chief Information Officer at PJ Dick–Trumbull–Lindy.

THE CHALLENGE

A Large, Modern IT Environment Preparing for Formal CMMC Alignment

With a mature technology environment and an established IT team, PJ Dick–Trumbull–Lindy wanted to validate its current state against NIST 800-171 and begin to build the documentation, clarity, and structure required for CMMC Level 2 certification.

Echelon's assessment provided a clear, organized picture of the organization's readiness and highlighted opportunities to further strengthen documentation, formalize boundaries for CUI, and align long-term strategic decisions.

Key focus areas identified in the assessment included:

- **Identifying the controls requiring additional documentation and formalization**
- **Standardizing and centralizing documentation**
- **Strengthening executive-level visibility into risk and prioritization**

Matt reflected on the value of having a structured, external perspective:

"We valued having an external perspective to validate our approach and ensure the prioritization aligned with CMMC expectations."

THE CHALLENGE

A Large, Modern IT Environment Preparing for Formal CMMC Alignment

ECHELON'S APPROACH

1. Comprehensive CMMC Gap Assessment

Echelon completed a full CMMC gap analysis, including interviews, documentation reviews, and comparison of the current environment against required controls. The collaborative process surfaced strengths, validated existing practices, and clarified where additional formalization or documentation would be beneficial.

"They systematically went through all the schools of security mentioned in CMMC," Matt recalled. "A lot of interviews; a lot of sit-downs."

Those early deliverables provided lasting value.

A Large, Modern IT Environment Preparing for Formal CMMC Alignment

ECHELON'S APPROACH

2. Plan of Action & Milestones

The assessment informed a formal Plan of Action & Milestones (POA&M), which proved crucial for aligning leadership and building long-term strategy.

"The POA&M helped us communicate even more effectively to the C-suite," Todd shared.

Echelon's strategy emphasized:

- *Developing core documentation and policy materials*
- *Evaluating potential enclave and SRM solutions*

"We wanted to make sure everything aligned to NIST 800-171," said Kelsey Cunningham, Echelon's Cybersecurity Manager on the Risk Advisory + Compliance Services team, who led a series of workshops to assess the organization's current and target security posture and developed policies aligned with the NIST 800-171 framework.

- Kelsey Cunningham, *Cybersecurity Manager*

3. Policy Development & Standardization

Echelon and the internal team worked through collaborative workshops to begin to formalize a CMMC-required policy for each control family. This process included initial development of related supporting documentation.

"The latest incident response plan still stands today," Matt said.

Impact & Outcomes

Improved Alignment and Organizational Visibility

One of the earliest benefits was stronger communication and shared understanding across teams and business units.

“It led to deeper conversations between the business units,” said Matt.

A Durable Foundation That Helped Guide the Program

Even as personnel and vendor relationships naturally evolve, the structure created early in the journey continues to guide the organization’s compliance posture.

“Echelon’s early work continues to be part of our compliance foundation,” Matt said. “We still reference some of those documents today.”

High Trust in Echelon’s Team

Matt summarized his experience working with Echelon across multiple initiatives, including evaluating and selecting security services, completing penetration tests and security assessments, and Strategic Security Program planning.

“Echelon is the most refreshing security company I've ever dealt with. There's no fluff. People know what they're doing. Nobody wastes our time. I love it.”

And on consistency, Matt added:

“It’s really impressive to see the team that Echelon has come in time and time again, no matter what project it is. You can tell everybody is seasoned and mature in their security knowledge.”

A Confident Path Toward CMMC Level 2 Compliance

Today, PJ Dick–Trumbull–Lindy continues advancing toward CMMC Level 2 certification. Its early investment created a strong position for future government opportunities.

And even as internal programs evolve, the partnership's impact remains meaningful.

"As far as security expertise," Matt added, **"I still heavily depend on and trust Echelon. Every engagement has been worthwhile."**

ECHELON
RISK +
CYBER

echeloncyber.com