UTILITIES PRIVATIZATION AND CYBERSECURITY PANEL

DLA ENERGY WORLDWIDE CONFERENCE 2026

Steve Brain – Dominion Energy

CYBERSECURITY CHALLENGES – SECURING CRITICAL INFRASTRUCTURE

Cyber and Physical Security Excellence: In addition to improving system reliability and resilience, DE delivers industry-leading cyber and physical security protections that are increasingly essential to mission assurance. As the utility service provider to some of the nation's most critical government facilities and installations in Virginia, we operate with the understanding that secure, dependable energy underpins national defense and continuity of operations.

CYBERSECURITY CHALLENGES – SECURING CRITICAL INFRASTRUCTURE

DE employs a comprehensive security framework that integrates:

- Rigorous cybersecurity protocols aligned to the evolving threat landscape
- Robust physical security controls across all facilities and assets
- Continuous real-time monitoring of cyber and physical threats
- Rapid incident-response capabilities to contain and mitigate issues quickly

At the center of this protection model is the Dominion Energy Physical and Cyber Security Control Center, which provides 24/7 oversight of the physical security of our generation, transmission, and distribution assets, while continuously detecting, analyzing, and mitigating potential cyber threats across the enterprise.

BLUF (WHY THIS MATTERS)

Bottom Line Up Front

- Utility service providers are subject to federal contractor cybersecurity requirements due to energy supply contracts with federal government customers.
- These requirements apply to systems that stores or processes designated government information (FCI/CUI).
- Because utility systems may not segregate federal and non-federal customer data, compliance obligations could extend across systems supporting public utility service operations.
- Increased regulatory scrutiny and upcoming CMMC requirements create near-term contract risk if not addressed.

PRACTICAL IMPLEMENTATION CONCERNS & HURDLES

What CMMC isn't:

- A cybersecurity program designed to safeguard operational utility infrastructure.

What CMMC is:

- An assessment of a contractor's compliance with information safeguarding standards. Generally applicable to assets that process, store, transmit FCI/CUI.
- The goal of the CMMC program is to verify that the DIB is safeguarding sensitive information (FCI/CUI).
- This is fundamentally an information protection program.

PRACTICAL IMPLEMENTATION CONCERNS & HURDLES

So many questions!

- "the Department" will specify the required CMMC level in the solicitation and the resulting contract."
  - Level 1 – Basic safeguarding of FCI
  - Level 2 – Broad protection of CUI - Decided by the type of information processed, transmitted, or stored on the contractor or subcontractor information systems.
- The required CMMC level is based on the type of data – FCI or CUI, that will be processed, stored, or transmitted on a contractor's IS during performance.
  - What utility data is CUI, can the government provide examples?
  - If the CUI information used by the contractor is *defense* related – Level 2 C3PAO assessment. How is private utility data *defense* related?
  - Can the government provide an example linked to an applicable NARA category?
- What is the DLA process for accurately categorizing utility data as CUI?
- What is the DLA process for determining the CMMC level for UP contracts?
- What government data, FCI or CUI, conveyed or otherwise is identified in the contract?
- What contract deliverable, transmitted to the government would be CUI when stored on a government system?

PRACTICAL IMPLEMENTATION CONCERNS & HURDLES

Category Concerns

- CUI designations in the CUI Registry's "Critical Infrastructure" category generally only apply to information submitted to or generated by the federal government or to information about government-owned facilities and cannot be the basis for requiring contractor CUI controls.
  - Talk to me about the CEII example!
  - In most cases ONLY CUI when stored government systems.
- Inconsistent standards to categorize and mark – I think it's important, mark it CUI!
  - E.g., US Army applying "default" CUI marking to outgoing email

Key Impediments

- DLA has not yet determined CMMC levels for Utility Privatization (UP) contracts.
- Results in unresolved scoping of assets and information repositories that safeguard CUI.

FINANCIAL AND OPERATIONAL CONCERNS

- CMMC program costs and requirements may affect the extent to which existing DIB companies decide to continue doing business with DoW.
  - Flow-down to subcontractors – SMB's may struggle to be compliant.
- Broader Federal Expansion: FAR 52.204-21
  - E.g., GSA, NASA, DHS, and other all have dissimilar CUI programs.
  - No CMMC (third-party certification) currently included in proposed FAR rule.
- Utility contracts are cost-of-service based. Additional requirements that increase service costs might ultimately be passed on the DoW.
- Applicable CUI not yet identified in UP contracts as a matter of conveyance or deliverable.
- Uncertainty of scope – what assets may be storing, processing, or transmitting CUI.
- Lack of clear guidance could introduce unnecessary complexity in the exchange of out-of-scope data.
- Incorrect CMMC level assignments.

RECOMMENDATIONS

- Encourage DoW to engage with energy sector stakeholders and industry SMEs.
- Continuing with positive engagements such as this forum and industry surveys, increases the likelihood of the Department achieving its goals.
- Working together will ensure applicable data is safeguarded from threats.

THANK YOU!