New FAR/DFARS Compliance Challenges for Small Businesses in 2014

Frank S. Murray

FOLEY & LARDNER LLP

NDIA Small Business Conference
September 10, 2014

Overview

- Recent Compliance Trends
- New and Proposed Rules regarding Counterfeit Parts and Nonconforming Items
- DFARS Cybersecurity Rule: Safeguarding Unclassified Controlled Technical Information
- Supply Chain Risk: Interim Rule
- Conclusion

Recent Compliance Trends

Recent Compliance Trends

- Self-reporting requirements
  - Placing the monitoring burden on the contractor
  - But the compliance systems and risks still have costs that the government will ultimately bear
  - How will the government use the information?
- Flow it down, all the way down
  - Several new clauses that require flow down to all tiers
  - Imposes government-unique requirements on suppliers who may not see themselves as in the government market
- Fewer exceptions for commercial items or small business

Counterfeit Parts & Nonconforming Items

Counterfeit Electronic Parts

- DFARS 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System
  - Final DFARS rule adopted May 6, 2014
  - Not applicable to SBC prime contractors: at prime contract level, applies only to CAS-covered contracts
  - However, SBC subcontractors are affected, because primes are required to flow down the requirement to all subs/suppliers at all tiers, including SBCs and commercial item subs/suppliers
  - Also, DOD has publicly indicated that it intends to issue a separate rule in the future that would extend counterfeit detection/avoidance requirements to

"Counterfeit Electronic Part"

- Revised definition of "counterfeit electronic part"
  - Definition in proposed rule had created risk that run-of-the-mill quality issues could be labeled as "counterfeit parts"
  - Final rule clarifies that **intent** to mislead or misrepresent is required
  - "unlawful or unauthorized reproduction, substitution or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer"
  - Includes used electronic parts represented as new, or false identification of grade, serial number, lot

"Suspect Counterfeit Part"

- "Suspect counterfeit electronic part" definition
  - "electronic part for which credible evidence (including, but not limited to, visual inspection or testing) provides reasonable doubt that the electronic part is authentic"
  - "Credible evidence" language is new in final rule and mirrors the standard for contractor disclosures of suspected fraud under the mandatory disclosure rule
  - Affords contractors leeway to conduct a reasonable investigation into a part's authenticity before labeling it "suspect counterfeit"
  - DOD: "fact-based approach"

"Risk-Based" System

- Final rule expressly endorses a "risk-based" approach by contractors to counterfeit electronic parts detection and avoidance
- Encourages contractors to focus inspection/testing efforts on electronic parts that are at most risk of being counterfeited, or that pose the greatest risk to mission performance or safety, rather than a "one-size-fits-all" approach
  - » Supplier risk – grey market, independent distributors
  - » Product risk – obsolete parts, safety-critical or mission-critical parts, parts with a history of

Required System Criteria

1) Training of personnel
2) Inspection/testing of electronic parts
   - Includes criteria for acceptance/rejection
3) Processes to abolish counterfeit parts proliferation
4) Processes for maintaining electronic part traceability
   - Requires tracking of electronic parts back to original manufacturer – pedigree record identifying "name and location of supply chain intermediaries"
   - Can use item unique identification (IUID) marking, but must comply with DFARS 252.211-7003, Item Unique Identification and Valuation

Required System Criteria (cont.)

5) Use of trustworthy suppliers
   - Buy from OEM/OCM (including authorized aftermarket manufacturers) or through OEM/OCM-authorized distribution channels
   - If not available through those channels, must use suppliers that meet applicable counterfeit detection and avoidance system criteria
6) Reporting and quarantining of counterfeit and suspect counterfeit electronic parts
   - Report to Contracting Officer and through GIDEP
   - Parts subject to reporting requirement include parts not yet delivered to DOD – if purchased for delivery to, or on behalf of, DOD
   - Quarantining: counterfeits and suspect counterfeits cannot be returned to seller and must be segregated from supply chain

Required System Criteria (cont.)

7) Methodologies to identify suspect counterfeit electronic parts and to determine if suspect parts are in fact counterfeit
8) Design, operation, and maintenance of systems to detect and avoid counterfeit and suspect counterfeit electronic parts
   - Contractor can use current Government- or Industry-recognized standards
9) Flow down of counterfeit detection and avoidance requirements
   - Flow down required to <u>all suppliers</u> who are "responsible for buying or selling electronic parts or assemblies containing electronic parts, or for performing acceptance testing"
   - Includes commercial item/COTS suppliers
   - <u>Includes small businesses</u>
   - Flow down must "include the substance of" DFARS 252.246

Required System Criteria (cont.)

10) Process for keeping continually informed of current counterfeiting information and trends
   - Detection/avoidance techniques in industry standards
11) Processes for screening GIDEP reports and other credible sources of counterfeiting information
12) Control of obsolete electronic parts
   - No guidance on what this means or how contractors are expected to "control" the risks posed by obsolete parts
   - What about DOD responsibility for updating design

New Cost Principle

- DFARS 231.205-71, Cost of Remedy For Use or Inclusion of Counterfeit Electronic Parts and Suspect Counterfeit Electronic Parts
  - » Costs of counterfeit electronic parts or suspect counterfeit electronic parts are **unallowable**
  - » Costs of **rework or corrective action** required to remedy the use or inclusion of counterfeit or suspect counterfeit electronic parts are **unallowable**
  - » Leads to onerous indemnification provisions that primes will try to flow down to SBC suppliers/subcontractors; many commercial suppliers unlikely to accept the liability

Effective Date of DFARS Counterfeit Parts Rules

- New rules effective as of May 6, 2014
- Apply to contracts awarded on or after May 6, 2014
- Do not apply to contracts awarded prior to May 6, 2014 – absent a contract modification
- New authentication and traceability requirements may limit ability to use existing inventory of electronic parts on newly awarded DOD contracts

Key Takeaways from New Rules

- "Zero-tolerance" sounds good as a talking point, but comes with costs
- Flow down requirement will present practical issues
  - » Commercial suppliers may not accept flow down – what then?
  - » Indemnification requirements – potential liability could vastly exceed subcontract value, particularly for lower-tier suppliers
  - » Are contractors responsible for auditing/reviewing each supplier's counterfeit detection/avoidance system?
- Traceability will be an immediate challenge
  - » Can you show chain of custody back to original

Key Takeaways from New Rules

- Importance of Industry Standards
  - Not expressly "adopted" as part of the rules, but referenced in several system criteria and likely to substantially influence DCMA's Checklist
  - Criteria now require contractors to stay informed about detection/avoidance techniques in industry standards
  - Consult and monitor updates to applicable industry standards – and use them as models for your own system where appropriate
  - Under proposed FAR rule for "Higher Level Quality Requirements," contracting officer can incorporate an industry standard into contracts as a higher-level quality standard, if concerned about risk of receiving nonconforming items

Counterfeit Parts Compliance Tips

- Easiest and most cost-efficient counterfeit prevention practice?
  - Whenever possible, buy directly from the OEM/OCM or its authorized distributor, and require your suppliers to do so too
- Review your inspection, testing and authentication practices against industry standards/best practices
- Establish a plan and procedures for quarantining and destroying suspect counterfeit parts
  - Do you maintain traceability of parts in inventory to particular suppliers/lots?
  - How would you respond if you receive a report that a certain part supplied by Company X was found to be counterfeit?

Counterfeit Parts Compliance Tips

- Assess "item risk" vulnerabilities
  - Obsolete or rare parts
  - High value parts
  - Safety-critical parts or parts critical to functionality
  - Parts that have been counterfeited previously (GIDEP reports)
- Assess and address "supplier risk"
  - Limit purchases of in-production parts to OCMs or authorized distributors and require suppliers to do same
  - Inspect/audit supplier quality systems and counterfeit detection/avoidance systems
  - Purchases from "independent distributors" are a danger zone – make sure the distributor is reliable or certified against applicable counterfeit standards (e.g., SAE AS6081), and additional testing of parts may be required

Counterfeit Parts Compliance Tips

- Adapt purchase order/supplier terms and conditions as required to deal with counterfeit-specific issues, such as impoundment of suspect counterfeits
- Establish internal reporting requirements and procedures for suspect counterfeit parts
- Register for and monitor GIDEP (and other industry sources) for reports of counterfeits
- Look for opportunities to remove obsolete parts from design

Expanded Reporting of Nonconforming Items

- FAR Case 2013-002, Expanded Reporting of Nonconforming Items
- Proposed FAR rule issued June 10, 2014
- Proposed rule, not yet effective; open for comment through September 11, 2014
- FAR rule, so will apply to all federal procurements, not just DOD procurements
- Proposes a new contract clause, 52.246-XX, Reporting Nonconforming Items

Reporting of N/C Items Proposed Rule

- Intended to implement the reporting requirements for counterfeit electronic parts under DOD counterfeit electronic parts rules – but goes much further
  - Applies to all items/parts, not just electronic parts
  - Applies to all federal procurements, not just DOD contracts
  - As proposed, would effectively require every company in the federal government supply chain to join GIDEP for purposes of reporting nonconforming items and screening GIDEP for reports of nonconforming items

Reporting of N/C Items Proposed Rule

- Would require reporting to contracting officer and to GIDEP of counterfeit/suspect counterfeit parts or a "major" or "critical" nonconformance in a "common item" that constitutes a "quality escape" resulting in the release of like nonconforming items to more than one customer
- Lots of key definitions
  - Major nonconformance & critical nonconformance (already defined in FAR Part 46)
  - "Common item" – item with multiple applications vs. a single or peculiar application. Includes parts, materials, components, assemblies, etc. that are commonly available items (such as nondevelopmental items, COTS items, NSN items).

Potential Issues With Proposed Rule

- Definitions are vague and potentially overbroad, leading to reporting of run-of-the-mill quality/warranty issues
  - » "Major nonconformance": a nonconformance likely to "materially reduce the usability of the supplies or services for their intended purpose"
  - » "Common item": seems to cover almost everything
  - » What is the issue the rule is intended to address?
- Flow down to <u>all suppliers at all tiers</u>, including commercial suppliers
  - » Are commercial suppliers going to agree to adopt a government-unique reporting system, joining and screening GIDEP, for what may be a very small

Potential Issues With Proposed Rule

- GIDEP not currently equipped to handle reporting as proposed in rule
  - » Eligibility limited to U.S. and Canadian companies, due to export-controlled info on GIDEP, but proposed rule would effectively require every company in federal supply chain to join GIDEP and screen it for reports
  - » Aside from eligibility concerns, is GIDEP equipped to handle the increased volume of reporting that the proposed rule would trigger?
  - » FAR Council indicated at public meeting in June 2014 that they are aware of these "GIDEP issues" and are working on them, but not clear how the rule can be finalized without the GIDEP issues being resolved first

Potential Issues with Proposed Rule

- Procedures to address (or remove) inaccurate GIDEP reports?
  - Not discussed in the proposed rule
  - What is the recourse if someone reports your part as nonconforming, and you think the report is wrong?
  - Important due to concerns that reports could lead to "de facto debarment" based on duty to screen GIDEP reports
- Civil liability issues for mandatory GIDEP reporting
  - Congress provided civil immunity for reports relating to counterfeit electronic parts in DOD procurements, but proposed rule goes much

Potential Issues with Proposed Rule

- Will excess reporting of garden-variety quality issues drown out the really important reports (counterfeit parts)?
  - Reporting system less useful if it becomes a big "data dump" of every warranty issue that arises in federal supply chain
- What if commercial suppliers won't accept the flow down and decline to join or screen GIDEP?
  - Does that mean you can't use them at all?

DFARS Cybersecurity Rule

DFARS Rule: Safeguarding UCTI

- DFARS 252.204-7012, Safeguarding of Unclassified Technical Information (UCTI)
  - Final rule adopted November 18, 2013 and effective for contracts awarded after that date
  - Applies to all DOD solicitations and contracts, including commercial item solicitations/contracts
  - BUT, requirements of the clause are implicated only for contractors who have UCTI on their information systems
  - Flow down requirement to subcontractors at all tiers

New DFARS Rule: Safeguarding UCTI

- 3 Key Elements of the Rule
  - Contractors must adopt and implement certain NIST IT security standards to protect UCTI
  - Mandatory reporting to DOD of "cyber incidents" within 72 hours
  - Flow down of requirement to all tiers of subcontractors, including commercial item subcontractors
    - Preamble to final rule suggests that DOD considers Internet Service Providers (ISPs) or cloud service providers to be "subcontractors" in context of this rule

"Controlled Technical Information"

- What is "Controlled Technical Information" (CTI)?
  - Technical information with a military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.
  - Technical information, not personal information (governed by other rules, HIPAA, etc.)
  - CTI "is to be marked with one of the distribution statements B-through-F, in accordance with DoD Instruction 5230.24, Distribution Statements on Technical Documents."
    - Important limitation on scope of definition; if not marked,

"Controlled Technical Information"

- Distribution Statements for CTI (from DODI 5230.24)
  - Distribution Statements B through F all contain restrictions on dissemination of information beyond DOD
  - Reasons for applying one of these limiting Distribution Statements include:
    - Administrative or Operational Use
    - Contractor Performance Evaluation
    - Critical Technology
    - Export Controlled Information
    - Foreign Government Information
    - OPSEC
    - Proprietary/Patentable Information
    - Test and Evaluation Information
    - Software Documentation/Manuals
    - Vulnerability Information

Contractor Systems Covered

- Depending on how contractor's unclassified IT system is structured, rule's impact can be very broad
- Safeguarding requirements apply to any of contractor's "project, enterprise, or company-wide unclassified information technology system(s) that may have UCTI resident on or transiting through them."
- Rule can have enterprise-wide impact
- "Transiting through": One e-mail forwarding UCTI?

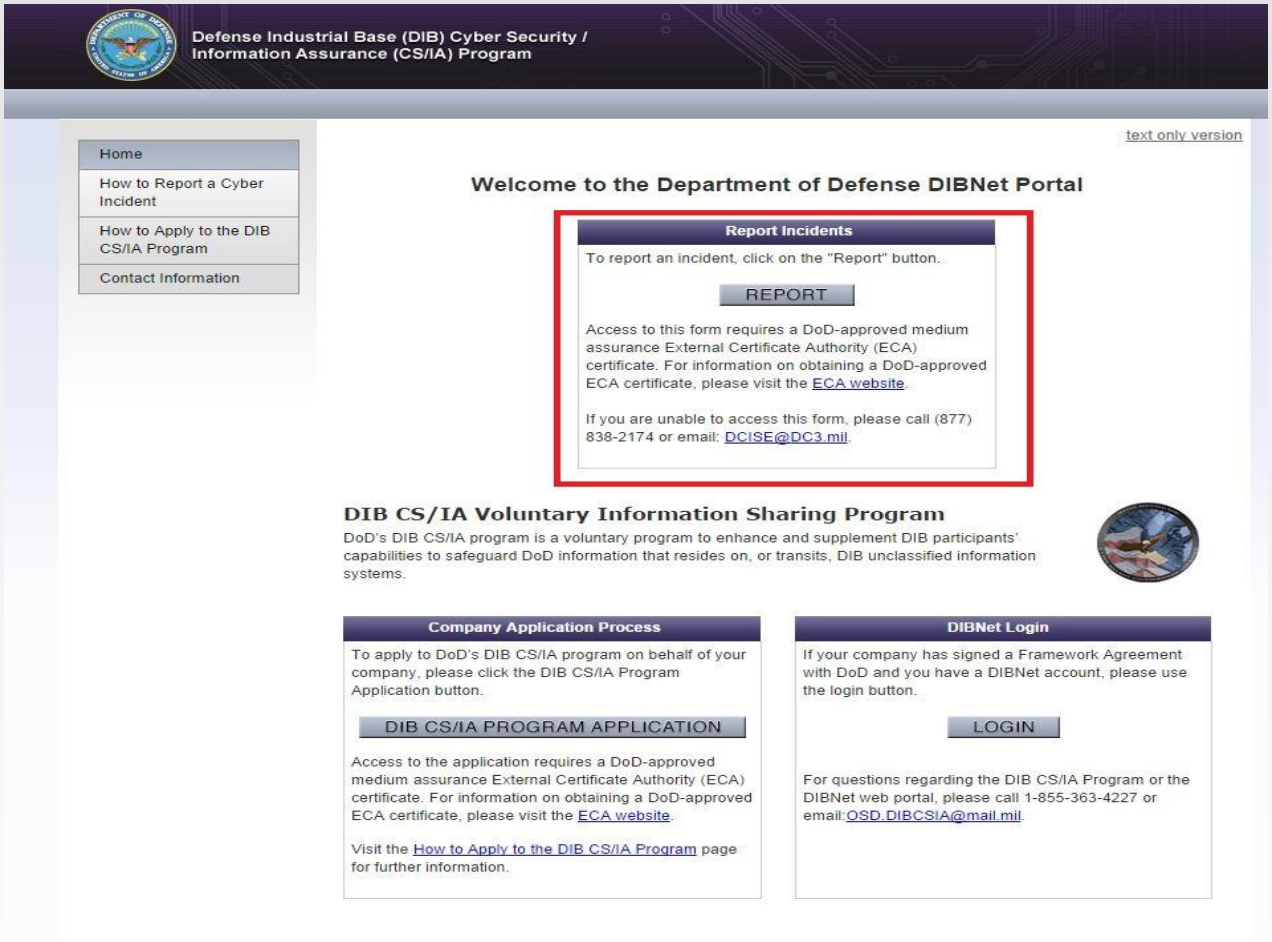
Minimum Security Controls for UCTI

- Rule requires contractors with CTI "resident on or transiting" through their unclassified information systems to apply specified "minimum security controls" listed in NIST Special Publication 800-53
  - 51 security controls, under 14 categories
  - Access Control; Awareness & Training; Audit & Accountability; Configuration Management; Contingency Planning; Identification & Authentication; Incident Response; Maintenance; Media Protection; Physical and Environmental Protection; Program Management; Risk Assessment; System & Communications Protection; and System & Information Integrity
- Some flexibility to depart from the specified controls, but only if contractor provides written

"Cyber Incident" Reporting

- Contractors required to report certain "cyber incidents" to DOD via web portal within 72 hours of discovery
  - "Cyber incident" = actions taken through use of computer networks that result in actual or potentially adverse effect on an information system and/or the information residing on it
- Reportable "cyber incidents"
  - Possible exfiltration, manipulation, or other loss or compromise of UCTI
  - Other activities allowing unauthorized access to contractor's system on which UCTI is resident/transiting

Reporting Cyber Incidents



DOD Cyber Incident Reporting Portal
http://dibnet.dod.mil

Cyber Incident Reporting & Investigation

- DFARS 252.204-7012(d)(1) identifies details to be included in cyber incident reports to DOD
- Contractors required to take actions to support DOD "damage assessment"
  - » Review of unclassified network for evidence of compromise
  - » Review data accessed during incident to identify specific UCTI implicated by incident
  - » Preserve and protect images of known affected IT systems and all relevant monitoring/packet capture data for at least 90 days

Issues with Safeguarding Rule

- How will DOD handle cyber incident reports?
  - Will it share information with other private sector companies as part of cyber threat information sharing?
  - What if information contractors are required to include in incident report is subject to non-disclosure agreement or other restrictions?
  - Will cyber incident reports factor into past performance evaluations?
- Will DOD conduct inspections/audits of contractor IT systems for compliance, or address compliance only in context of cyber

Issues with Safeguarding Rule

- Will report of a cyber incident be deemed to establish that contractor had inadequate security controls?
  - DOD says a properly reported cyber incident, "by itself," will not be interpreted as an automatic breach of the rule, but that doesn't mean DOD can't treat a cyber incident report as a breach
- What are consequences of contractor "breach" of this clause?

Issues with Safeguarding Rule

- How to apply the reporting requirement in flowdowns
  - Compromise of subcontractor network: standard flow down may not require subcontractor to report to prime, only to DOD directly
  - Primes should include a requirement by subcontractor to report to prime as well
  - Prime would then arguably have to file its own report within 72 hours of notification by sub, as clause includes reporting of "incident on a subcontractor network"
- Are small business or commercial item subcontractors familiar with the new requirements and capable of meeting them?

Cybersecurity Tips

- Review security of your information systems and ensure your unclassified systems include the security controls required by the new DFARS rule on safeguarding UCTI
- Review solicitations and contracts for information security requirements
  - Other agencies likely to use DFARS UCTI rule as model
  - Director of National Intelligence in process of adopting cybersecurity rules for responses to cyber attacks on classified networks
- Be prepared to describe your cybersecurity procedures & controls in response to a solicitation, and have a good response plan in the event of a breach

Cybersecurity Tips

- Ensure subcontractors have adequate cybersecurity for information you share with them
  - » Incorporate appropriate requirements in subcontracts
- Monitor cybersecurity legislation and rulemakings to assess any new standards/requirements – and engage in the process as appropriate
  - » Government is looking for input from industry
  - » Cybersecurity standards and requirements still being developed; if you see an issue, raise it

DFARS Supply Chain Risk Rule

DFARS Rule on Supply Chain Risk

- Interim DFARS Rule on Supply Chain Risk issued on November 18, 2013
  - As interim rule, effective immediately, but open for comment and may be revised later when final rule is issued
  - Comment period ended January 17, 2014
- Rule implements Section 806 of FY 2013 NDAA
- Allows DoD to consider the impact of supply chain risk in procurements related to National Security Systems (NSS)
- Intersection of cybersecurity and supply chain

DFARS Rule on Supply Chain Risk

- Purpose is to mitigate risk of sabotage or introduction of malicious function or other subversion of sensitive DOD IT systems through compromised hardware/software
- Contract clause to be incorporated into all procurements of IT, whether acquired as service or supply
  - But only "active" for NSS procurements – DoD does not want to signal which procurements are for NSS
- Applies to commercial item procurements

DFARS Rule on Supply Chain Risk

- Rule gives DoD the authority to:
  - Exclude a source that fails to meet qualification standards established to reduce supply chain risk
  - Exclude a source that fails to achieve an acceptable rating on a supply chain risk evaluation factor
  - Withhold consent for a contractor to subcontract with a particular source, or direct a contractor to exclude a particular source from consideration for a subcontract
- DoD doesn't have to disclose its reasons for exclusion or even that it did exclude a source
- Exercise of this authority cannot be challenged in a bid protest or in any Federal court

Conclusion

- DOD is "beating the drum" on quality issues (counterfeits, nonconforming items) and trying to accomplish policy goals through all-tier flow downs
- Many recent rules require self-reporting
  - Possible new frontier in False Claims Act cases?
  - What will government do with reports? (Past performance or non-responsibility issues? Supply chain risk?)
- Rulemakings frequently underestimate the impact of new requirements on small businesses and commercial suppliers – make your voice heard during comment period

QUESTIONS?

Frank S. Murray
Foley & Lardner, LLP
fmurray@foley.com
(202) 295-4163