crowell moring

# CRISIS MANAGEMENT AND FIRST AID: WHEN GOVERNMENT CONTRACTORS ARE THE HEADLINERS

## WELCOME

OOPS 2014

crowell moring

# SUPPLY CHAIN CHALLENGES: THE NEW DOD RULE ON COUNTERFEIT ELECTRONIC PARTS

Chris Haile

Grant Book

OOPS 2014

# Origins of the New Rule

Primarily Implements §818 of the FY 2012 National Defense Authorization Act

- Directed that DoD issue regulations for detection and avoidance of counterfeit electronic parts in the supply chain
- Directed that the new regulations include contractor- and subcontractor-reporting requirements, but established protection from civil liability on the basis of such reporting
- Established a new criminal offense (18 U.S.C. § 2320) for trafficking in counterfeit goods or services

# Key Elements

- Covered contractors must implement systems to detect, avoid, and report counterfeit electronic parts
- Government audits of those systems
- Costs relating to counterfeit and suspect counterfeit electronic parts are generally unallowable

# Detection and Avoidance Systems

**New DFARS clause at 252.246-7007**

- Applicable where:
  - The Contract procures
    - Electronic parts
    - End items, components, parts or assemblies containing electronic parts, or
    - Services where any of the above are provided as part of the service;

    AND
  - The prime contractor is CAS-covered

# Detection and Avoidance Systems

**Flowdown Requirements**

- If applicable at the prime level, then the requirements flow down to subcontractors at all tiers
  - Subcontractors need not be CAS-covered
  - Includes subcontracts for commercial or commercial-off-the-shelf (COTS) items
  - Includes small business subcontractors
- Broad flowdown creates an usual burden on commercial / small suppliers
- Will suppliers opt out of DoD work?

# Detection and Avoidance Systems

**Electronic Part**

- "an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly"
- "includes any embedded software or firmware"

DFARS 252.246-7007(a)

# Detection and Avoidance Systems

## Counterfeit Electronic Part

"An 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, or a source with the express written authority of the original manufacturer or current design activity, including authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics." DFARS 252.246-7007(a)

# Detection and Avoidance Systems

**System criteria**

- Must include risk-based policies and procedures that address at least 12 criteria:
  1. Training of personnel
  2. Inspection and testing of electronic parts, including criteria for acceptance and rejection
  3. Processes to abolish counterfeit part proliferation
  4. Processes for maintaining electronic part traceability
  5. Use of sources that are OEMs or authorized to manufacture the parts
  6. Reporting and quarantining of counterfeit and suspect counterfeit electronic parts

# Detection and Avoidance Systems

**System Criteria (Cont'd)**

7) Methodologies to identify suspect counterfeit electronic parts and determine authenticity
8) Design, operation, and maintenance of systems to detect and avoid counterfeit and suspect counterfeit electronic parts
9) Flow down of counterfeit detection and avoidance requirements
10) Process for keeping continually informed about counterfeiting information and trends
11) Process for screening GIDEP
12) Control of obsolete electronic parts

# Detection and Avoidance Systems

## Inspection and Testing of Electronic Parts

- While part of the system overall, this is not required for every part
- Whether/how to test or inspect may depend upon the source of the part and a risk-based assessment

# Detection and Avoidance Systems

## Hierarchy of Sources

- Favor use of suppliers who are original or authorized sources , or who obtain their supplies exclusively from  such sources
- If not available from one of the above, then use suppliers who themselves “meet applicable detection and avoidance system criteria”
- DoD Preamble to the rule identifies this as an explanation of “what types of suppliers may be deemed ‘trusted’ and therefore treated differently from other suppliers”
- Electronic parts from suppliers who cannot meet these criteria may require substantially more stringent inspection and testing to authenticate the parts

# Detection and Avoidance Systems

## A Note on "Trusted Suppliers"

- FY 2012 NDAA established the term in this context
- DoD was directed to establish criteria so that contractors could use trusted suppliers when parts were no longer in production or available in stock from OEMs or authorized manufacturers/dealers
- DoD decided to implement the concept without the term (*e.g.*, referring to use of "suppliers that meet applicable counterfeit detection and avoidance criteria")
- But a further DFARS case (2014-D005) is open to address identification of trusted suppliers and may eventually provide more guidance

# Detection and Avoidance Systems

**Traceability**

- Systems must address traceability
- May use industry standards and best practices
- But must include:
  - Certification and traceability documentation
  - Clear identification of the name and location of supply-chain intermediaries from the manufacturer to the direct source of the product for the seller
  - manufacturer's batch identification where available

# Reporting Requirements

## Systems must also address reporting of "Counterfeit Electronic Parts" and "Suspect Counterfeit Electronic Parts"

- Report to:
  - Contracting Officer, and
  - Government-Industry Data Exchange Program (GIDEP)
- When to report: "when the Contractor becomes aware of or has reason to suspect that, any electronic part or end item, component, part, or assembly containing electronic parts [being acquired by DoD] contains counterfeit electronic parts or suspect counterfeit electronic parts."
- These requirements to be further addressed in FAR Case 2013-002 ("Expanded Reporting of Nonconforming Supplies")

# Reporting Requirements

## Suspect Counterfeit Electronic Part

"an electronic part for which credible evidence (including, but not limited to, visual inspection or testing) provides reasonable doubt that the electronic part is authentic."

DFARS 2252.246-7007(a)

# Audit of Systems

- Audit to be conducted as part of purchasing system evaluation (*See* DFARS 252.244-7001)
- Failure to show an acceptable system for detection and avoidance of counterfeit electronic parts may lead to purchasing system disapproval and withholding of payments
- DCMA is expected to develop a "Counterfeit Detection and Avoidance System Checklist"

# New DFARS Cost Principle

- New DFARS 231.205-71 makes unallowable the costs of counterfeit and suspect counterfeit electronic parts, as well as the costs of re-work or corrective action

- Very Limited Exception:
  - Contractor has an operational, government-approved system to detect and avoid counterfeit parts;
  - The counterfeit or suspect counterfeit electronic part was government-furnished property; AND
  - The contractor reports to the government within 60 days of becoming aware

# Challenges for Implementation

- Flowdown challenges and impacts on commercial supply chains
- Undefined standards and risk-based concepts
- Government audits
- Monitoring compliance

# Questions

Chris Haile
202-624-2898
chaile@crowell.com

Grant Book
202-624-2512
gbook@crowell.com