New DoD Regulations:

Safeguarding Unclassified Controlled Technical Information

April 10, 2014

National Defense Industrial Association
Small Business Division – Executive Committee

Robert S. Metzger & Lucas T. Hanback
750 Ninth Street, N.W., Ste. 710
Washington, D.C. 20001
rmetzger@rjo.com www.rjo.com

New DFARS 252.204-7012: Safeguarding UCTI

- Proposed Rule – June 29, 2011
- Final Rule Issued Nov. 18, 2013
- Requires DoD contractors and subcontractors to
  - **Safeguard** unclassified controlled technical information (UCTI)
  - **Report** cyber incidents
- Applies to contracts and subcontracts
- Contract clause is to be included in *all* solicitations and contracts – including FAR Part 12 (commercial items)
- Obligation to "provide adequate security" means small businesses will need to meet certain cyber standards
- Rule applies only to handling of designated information but necessarily affects company information systems and practices

What is "Unclassified Controlled Technical Information"?

"Unclassified"

Information that has not been given one of the classifications (Confidential, Secret, or Top Secret) under Executive Order 13526 .

E.O. 13526 (12/29/2009)

✚

"Controlled Technical Information"

"means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination."

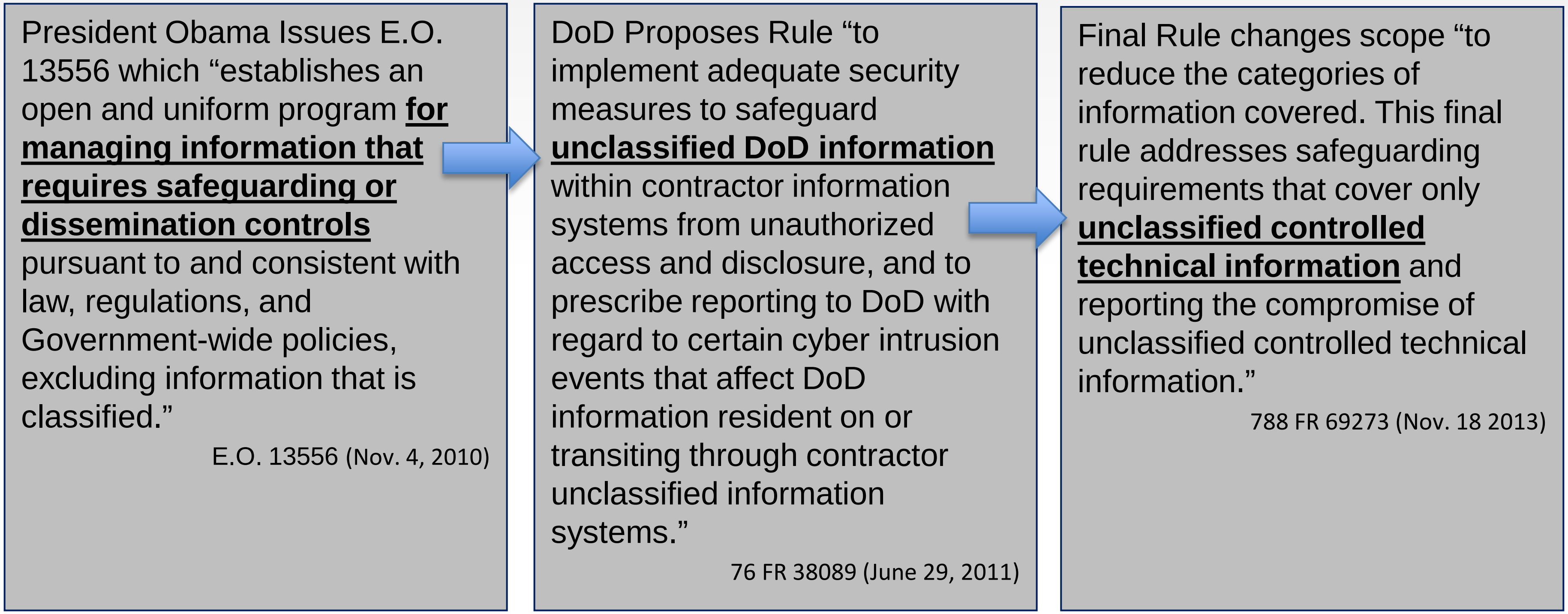
78 Fed. Reg. 69273, at 69280 (11/18/2013)

Unclassified Controlled Technical Information Includes:

- Technical data
- Computer software including executable code and source code
- Engineering data
- Drawings
- Associated specifications
- Data sets
- Studies and analyses

Under the New Rule, UCTI will be marked with a "distribution statement"

The new rule should come as no surprise



President Obama Issues E.O. 13556 which "establishes an open and uniform program **for managing information that requires safeguarding or dissemination controls** pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified."

E.O. 13556 (Nov. 4, 2010)

DoD Proposes Rule "to implement adequate security measures to safeguard **unclassified DoD information** within contractor information systems from unauthorized access and disclosure, and to prescribe reporting to DoD with regard to certain cyber intrusion events that affect DoD information resident on or transiting through contractor unclassified information systems."

76 FR 38089 (June 29, 2011)

Final Rule changes scope "to reduce the categories of information covered. This final rule addresses safeguarding requirements that cover only **unclassified controlled technical information** and reporting the compromise of unclassified controlled technical information."

788 FR 69273 (Nov. 18 2013)

- Final scope narrowed in response to comments – dropped types "basic" and "enhanced" from proposed rule – eliminates contractor discretion about what to protect
- The final rule applies only to contractors with "controlled technical information" resident on or transitioning through their information systems – **DoD has the obligation to identify UCTI**.
- The final rule reinforces the reporting requirements.
- Rule does not cover broader information in initially proposed rule (e.g. information exempt from FOIA, "critical program information," etc.)

The cyber threat explains the new rule

- "Stolen data provides potential adversaries extraordinary insight into the United States' defense and industrial capabilities and allows them to save time and expense in developing similar capabilities. Protection of this data is a high priority for the Department and is critical to preserving the intellectual property and competitive capabilities of our national industrial base and the technological superiority of our fielded military systems."
  - Secretary of Defense Chuck Hagel – October 10, 2013 Memorandum

- DoD is using its regulatory authority and control over acquisition practices to improve cyber security.
- The new rule implements E.O. 13556 - Controlled Unclassified Information.
  - NARA was designated by E.O. 13556 to take lead in implementation.
  - In issuing the final rule, DoD decided it would not wait for NARA to finish.
- DoD believes its contractors share with it a common interest in protecting information and responding to cyber incidents. Measures taken to comply with the new regulation also protect commercial data, e.g., IP and PII.

Small Business impacts – likely understated

- DoD forecasts modest cost impacts.
  - DoD estimates 6,555 contractors (½ small) handle UCTI and will be affected and 5 reports per company per year (3.5 hrs/response) will be required.
  - Rule requires maintaining an image of compromised data for 90 days – DoD estimates minimal costs as result of this.
- These estimates almost certainly are low.
  - Compliance is required of companies that want to do business with DoD. Few small companies will implement separate systems "just" for UCTI.
  - Companies without active cyber programs will incur non-recurring and recurring costs. Advice from specialists and counsel may be required.
  - Reporting experience on DIB Voluntary Cyber Security and Information Assurance (CS/IA) Program suggests DoD's impact estimates are low.
  - Changes may affect policies and business practices, e.g. remote work
  - Costs of response to a cyber incident can be substantial.
- Compliance costs are allowable as overhead (not direct).

New DFARS

- The new rule creates new DFARS subpart 204.73.
  - DFARS sets forth:
    - Scope – "applies to contracts and subcontracts requiring safeguarding of unclassified controlled technical information resident on or transiting through contractor unclassified information systems."
    - Definitions – "controlled technical information," "technical information," "cyber incident."
    - Policy – 1) "provide adequate security to safeguard unclassified controlled technical information;" 2) "report to DoD certain cyber incidents" that affect UCTI
    - Mandatory contract clause – DFARS 252.204-7012

DFARS Clause 252.204-7012

- **Included in all solicitations and contracts**
  - **Mandatory flow down to subcontracts**
- **Included in commercial item contracts**
- **Specifies minimum* security controls for safeguarding**
- **Clarifies reporting requirements and mechanisms**

* *but the contractor shall apply "other information systems security requirements" if "required to provide adequate security in a dynamic environment based on an assessed risk of vulnerability."*
DFARS 252.204-7012(b)(2)

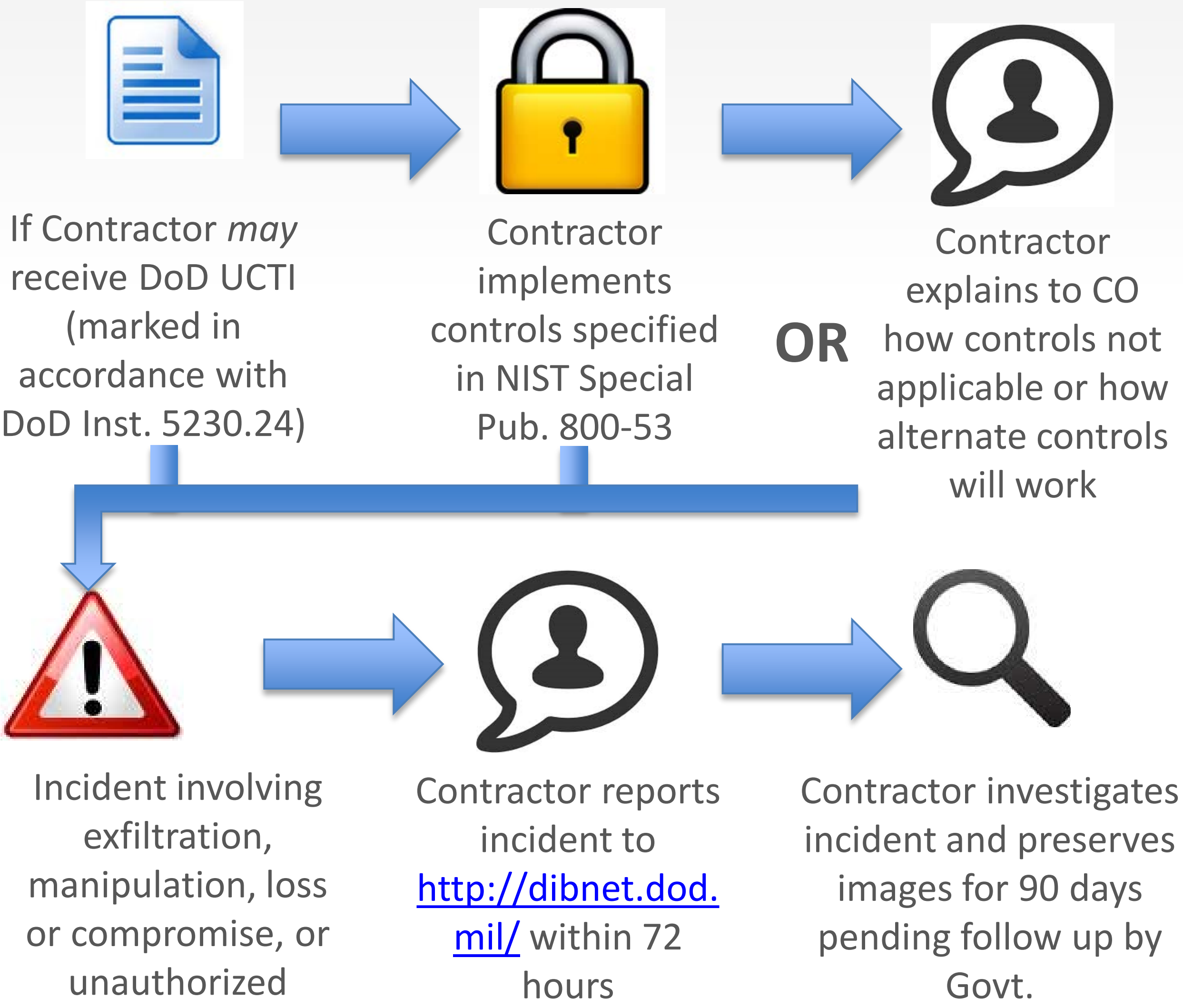
What are the basic requirements?

Safeguard

Applies for any UCTI residing on or transiting through system

Report

Must be done within 72 hours of “discovery of any cyber incident” that affects UCTI



If Contractor *may* receive DoD UCTI (marked in accordance with DoD Inst. 5230.24)

Contractor implements controls specified in NIST Special Pub. 800-53

OR

Contractor explains to CO how controls not applicable or how alternate controls will work

Incident involving exfiltration, manipulation, loss or compromise, or unauthorized access of UTCI

Contractor reports incident to http://dibnet.dod.mil/ within 72 hours

Contractor investigates incident and preserves images for 90 days pending follow up by Govt.

Safeguarding – Detailed Requirements

The Contractor shall provide "**adequate security**" to safeguard **unclassified controlled technical information** from compromise.

DFARS 252.204-7012(b)

Controlled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information 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.

DFARS 252.204-7012(a)

Technical Information includes:

Research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

In theory, DoD components will mark UCTI with the "**Distribution Statement.**"

B – "Distribution authorized to **U.S. Government agencies only** (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office)."

C – "Distribution authorized to **U.S. Government agencies and their contractors** (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office)."

D – "Distribution authorized to the **Department of Defense and U.S. DoD contractors only** (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office)."

E – "Distribution authorized to **DoD Components only** (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office)."

F – "Further dissemination **only as directed by** (inserting controlling DoD office) (date of determination) or higher DoD authority."

DoD Inst. 5230.24

Safeguarding – 14 Control Areas per NIST SP 800-53

To provide adequate security, the Contractor shall:

(1) Implement information systems security in its project, enterprise, or company-wide unclassified information technology system(s) that may have unclassified controlled technical information resident on or transiting through them. The information systems security program shall implement, at a minimum—

(i) The specified **National Institute of Standards and Technology (NIST) Special Publication (SP) 800–53 security controls** identified **in the following table**; or

(ii) If a NIST control is not implemented, the Contractor shall submit to the Contracting Officer a written explanation of how—

(A) The required security control identified in the following table is not applicable; or

(B) An alternative control or protective measure is used to achieve equivalent protection.

DFARS 252.204-7012(b)

NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems in accordance with the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347.

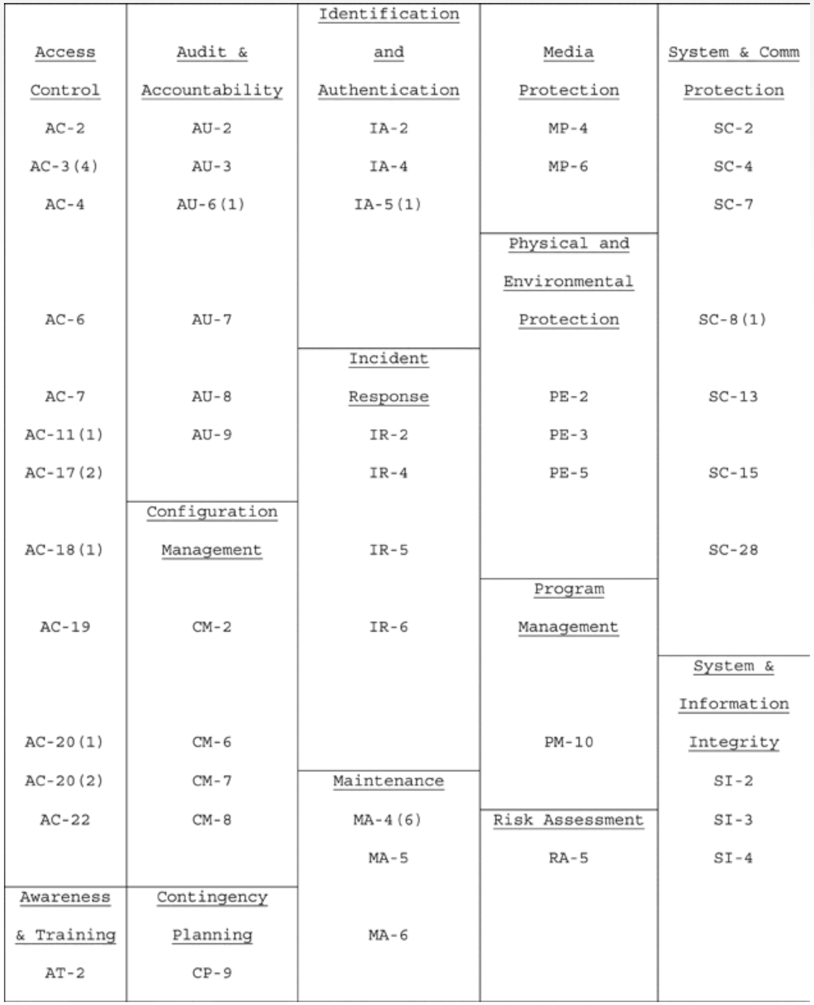
NIST Special Pub. 800-53 – Specifies controls for:
(1) Access control,
(2) Awareness and training,
(3) Audit and accountability,
(4) Configuration management,
(5) Contingency planning,
(6) Identification and authentication,
(7) Incident response,
(8) Maintenance,
(9) Media protection,
(10)Physical and environmental protection,
(11)Program management,
(12)Risk assessment,
(13) Systems and communication protection, and
(14) System and information integrity.

The DFARS lists 51 controls among the ~ 300 included in NIST SP 800-53

1. **Review 252.204-7012** required controls and **NIST** controls
2. **Implement** listed control **OR**
3. If control is inapplicable, **explain** why to CO **OR**
4. **Explain** how **alternative** protective measure will be used

The DFARS establishes no mechanism for CO (or other DoD) oversight, review or approval. It may be sufficient to "decide and document" decisions rather than seek approval. The test may be *after* an *incident.*

DFARS 252.204-7012 (51 NIST Controls)



		Identification		
Access	Audit &	and	Media	System & Comm
Control	Accountability	Authentication	Protection	Protection
AC-2	AU-2	IA-2	MP-4	SC-2
AC-3(4)	AU-3	IA-4	MP-6	SC-4
AC-4	AU-6(1)	IA-5(1)		SC-7
			Physical and	
			Environmental	
AC-6	AU-7		Protection	SC-8(1)
		Incident		
AC-7	AU-8	Response	PE-2	SC-13
AC-11(1)	AU-9	IR-2	PE-3	
AC-17(2)		IR-4	PE-5	SC-15
	Configuration			
AC-18(1)	Management	IR-5		SC-28
			Program	
AC-19	CM-2	IR-6	Management	
				System &
				Information
AC-20(1)	CM-6		PM-10	Integrity
AC-20(2)	CM-7	Maintenance		SI-2
AC-22	CM-8	MA-4(6)	Risk Assessment	SI-3
		MA-5	RA-5	SI-4
Awareness	Contingency			
& Training	Planning	MA-6		
AT-2	CP-9			

Table 1—Minimum Security Controls for Safeguarding

Minimum required security controls for unclassified controlled technical information requiring safeguarding in accordance with paragraph (d) of this clause. (A description of the security controls is in the NIST SP 800–53, ''Security and Privacy Controls for Federal Information Systems and Organizations'' (*http://csrc.nist.gov/publications/PubsSPs.html*).)

Legend:

AC: Access Control
AT: Awareness and Training MP:
AU: Auditing and Accountability
CM: Configuration Management
CP: Contingency Planning
IA: Identification and Authentication
IR: Incident Response
MA: Maintenance
MP: Media Protection
PE: Physical & Environmental Protection
PM: Program Management
RA: Risk Assessment
SC: System & Communications Protection
SI: System & Information Integrity

The specific controls are just a small subset of those stated in NIST SP 800-53. The functional areas covered correspond to areas where a prudent business would seek to protect its information systems and IP. NIST also has prepared the new *Framework for Improving Critical Infrastructure Cybersecurity* - a guide to strategy that is useful for all sizes of business.

Safeguarding – Detailed Requirements

Examples of NIST Controls:

AC-2 – Account Management requires the organization to "Assign account managers for information system accounts; Establish conditions for group and role membership; Specifies authorized users of the information system, group and role membership."

NIST SP 800-53 contains 3 and a half pages of details on this requirement including related controls and 13 optional enhancements for the requirement.

AU-2 – Audit Events requires the organization to "Determine that the information system is capable of auditing [certain] events."

NIST SP 800-53 contains approximately 1 page of details on this requirement including 4 optional enhancements.

Other Sources and Standards Can Be Considered, e.g.,

- NIST Risk Management Framework (multi-industry)
- ISO 27001
- COBIT 5
- CCS Critical Security Controls

Commercial companies should inform Contracting Officers where they have adopted these or other standards in lieu of NIST 800-53 Rev. 4.

Many DoD contractors already will have many (or all) of the required controls. Review will be necessary to assess systems and compliance risks. Companies can decide some controls are inapplicable or choose other measures than NIST.

Cyber Incident Reporting – Detailed Requirements

What do you have to report?

"Cyber Incidents"

Reportable **cyber incidents** include the following: (i) A cyber incident involving possible **exfiltration**, manipulation, or other loss or **compromise** of any unclassified controlled technical information resident on or transiting through Contractor's, or its subcontractors', unclassified information systems. (ii) **Any other activities** not included in paragraph (d)(2)(i) of this clause that **allow unauthorized access** to the Contractor's unclassified information system on which unclassified controlled technical information is resident on or transiting.

DFARS 252.204-7012(d)(2)

Compromise means **disclosure of information to unauthorized persons**, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

Cyber incident means **actions taken through the use of computer networks** that result in an actual or potentially **adverse effect on an information system and/or the information** residing therein.

Exfiltration means any **unauthorized release of data** from within an information system. This includes copying the data through covert network channels or the copying of data to unauthorized media.

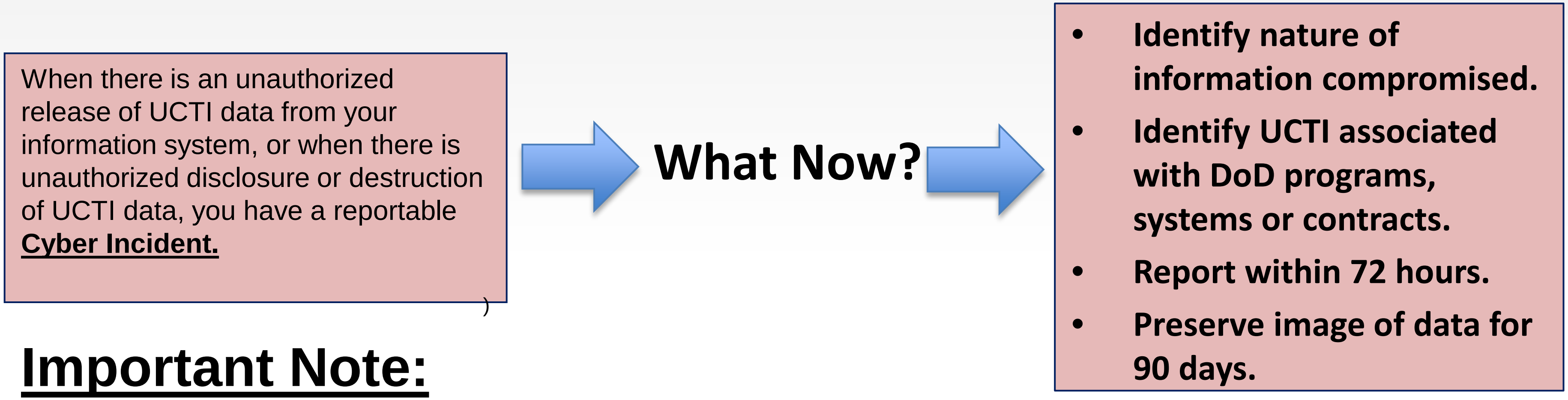
DFARS 252.204-7012(a)

Companies should have no trouble knowing when "acute" incidents occur, e.g., hacking, data theft. Where UCTI is lost or compromised, reporting is a must. Unauthorized access to a system on which UCTI resides also is a reportable incident.

Reporting requirements have twin purposes. One is to inform the DoD customer of potential injury from loss of its controlled data. The other is to inform DoD of how the attack occurred so that it can improve cyber defenses and better address threats.

A "cyber incident" is an unauthorized disclosure or release of UCTI.

Incident Reporting – Detailed Requirements



When there is an unauthorized release of UCTI data from your information system, or when there is unauthorized disclosure or destruction of UCTI data, you have a reportable **Cyber Incident.**

)

What Now?

- **Identify nature of information compromised.**
- **Identify UCTI associated with DoD programs, systems or contracts.**
- **Report within 72 hours.**
- **Preserve image of data for 90 days.**

Important Note:

This reporting does not abrogate the Contractor's responsibility for additional safeguarding and cyber incident reporting requirements pertaining to its unclassified information systems under other clauses that may apply to its contract, or as a result of other U.S. Government legislative and regulatory requirements that may apply (e.g., as cited in paragraph (c) of this clause).

In other words – compliance with DFARS 252.204-7012 reporing requirements **does not** relieve the contractor of the burden from compliance with other laws and statutes governing restricted or classified information. Recognize also other potentially applicable federal or state laws or contract requirements.

(For example, Contractors must still comply with E.O. 13556 – which governs classified information.)

What must be reported? (see next slide)

DFARS 252.204-7012(a)

Incident Reporting – 13 Detailed Requirements

What does the Report Contain?

(i) Data Universal Numbering System (**DUNS**).

(ii) **Contract numbers affected** unless all contracts by the company are affected.

(iii) Facility **CAGE code** if the location of the event is different than the prime Contractor location.

(iv) **Point of contact** if different than the POC recorded in the System for Award Management (address, position, telephone, email).

(v) **Contracting Officer** point of contact (address, position, telephone, email).

(vi) Contract **clearance level**.

(vii) **Name of subcontractor and CAGE code** if this was an incident on a subcontractor network.

(viii) **DoD programs, platforms or systems involved**.

(ix) **Location(s) of compromise**.

(x) **Date** incident discovered.

(xi) **Type of compromise** (e.g., unauthorized access, inadvertent release, other).

(xii) **Description** of technical information compromised.

(xiii) Any **additional information** relevant to the information compromise.

DFARS 252.204-7012(d)(1)

What else must the contractor do?

Conduct a more detailed review to determine the specific data and technical information accessed and the scope of the compromise to the information system.

Preserve relevant images and monitoring data captured for at least 90 days to allow DOD time to request additional information for purposes of a DOD damage assessment.

No "Safe Harbor"

Reporting **does not** create a safe harbor for cyber incidents, although the rule provides that a "cyber incident that is properly reported by the contractor shall not, by itself, be interpreted under this clause as evidence that the contractor has failed to provide adequate information safeguards."

However, if the Gov't investigates an incident and finds a less than "adequate security," that could be breach and expose the company to damages or other liability.

Takeaways – for small, medium-sized business

- The new DFARS will impact small and medium-sized businesses more than large DoD contractors (who already have cyber-compliant systems).
- DoD has decided the cost and operational impact is necessary to protect its UCTI – but costs are recoverable only via overhead.
- Companies must assess if they provide "adequate security" to safeguard UCTI.
- Non-recurring impacts include, e.g, self-assessment, system and process enhancements and 1-time equipment buys.
- Recurring impacts will include additional staffing, training and operational costs.
- Providing "adequate security" is a dynamic, not static obligation.
- The rule could impact organizational structure and operations.
  - Some companies may segregate compliant (UCTI) from non-compliant (comm'l) systems.
  - Cyber assurance may limit access via mobile and personal devices and affect telework.
- The rule will affect dealings with subcontractors.
  - Care must be taken to flow down requirements and assure compliance.
  - Subcontractors must confirm and adhere to reporting requirements.

Questions

Speaker Biography – Bob Metzger

Robert S. Metzger received his B.A. from Middlebury College and is a graduate of Georgetown University Law Center, where he was an Editor of the *Georgetown Law Journal*. He was a Research Fellow, Center for Science & International Affairs, Harvard Kennedy School of Government.

Mr. Metzger is the Managing Partner of the Washington, D.C. office of Rogers Joseph O'Donnell, P.C. He is a member of the International Institute for Strategic Studies (IISS), London. Academic publications on international security topics include articles in *International Security*, the *Journal of Strategic Studies* and *Indian Defence Review*. He is a Vice-Chair of the Supply Chain Assurance Committee of TechAmerica. He is recognized as a leading national expert on supply chain assurance and cyber risk management.

Mr. Metzger advises leading US and international companies on key public contract compliance challenges and in strategic business pursuits.

SELECTED EXTERNAL PUBLICATIONS

available at http://www.rjo.com/metzger.html

- "Convergence of Counterfeit and Cyber Threats: Understanding New Rules on Supply Chain Risk," *Federal Contracts Report*, Feb. 18, 2014
- "DoD Counterfeit Parts Rule – So Little After So Long," *Law360* , Jun. 5, 2013
- "New DOD Counterfeit Prevention Policy: Resolves Responsibilities Within DOD But Leaves Many Contractor Questions Unresolved," (PDF) *Federal Contracts Report*, May 15, 2013
- "Counterfeit Electronic Parts: What to Do Before The Regulations (and Regulators) Come? (Part 2)," *Federal Contracts Report*, Aug. 21, 2012
- "Counterfeit Electronic Parts: What to Do Before the Regulations (And Regulators) Come? (Part 1)," *Federal Contracts Report*, Jun. 21, 2012 (with Jeff Chiow)
- "Legislating Supply Chain Assurance: Examination of Section 818 of the FY 2012 NDAA," *The Procurement Lawyer*, Vol. 47, No. 4 (with Jeff Chiow)

Speaker Biography – Lucas Hanback

Lucas T. Hanback received his B.S. from Virginia Tech and he graduated with honors from The George Washington University Law School where he was a member of the *Public Contract Law Journal*, and his note was published in the Fall 2010 edition.

Mr. Hanback is a member of the American Bar Association Section of Public Contract Law where he serves as the Young Lawyer Liaison to the Employment Safety & Labor Committee and the Contract Claims and Disputes Resolution Committee. Prior to entering practice, Mr. Hanback worked as a government contractor with Booz Allen Hamilton. He served on the Task Force for Business and Stability Operations in Iraq and Afghanistan, and was commended in writing by the Deputy Under Secretary of Defense for outstanding performance. Mr. Hanback formerly served as an artillery officer in the United States Marine Corps and is a combat veteran of the war in Iraq. He was awarded two Navy Commendation Medals, one with the Combat "V".

Mr. Hanback advises clients on a diverse array of government contracts topics including small business issues, employment issues in government contracting, government contracting ethics and compliance, defense and cyber security issues, the false claims act, and GSA schedule contracting.

SELECTED EXTERNAL PUBLICATIONS

available at http://www.rjo.com/hanback.html

- "SBA Case Highlights Ambiguity in the Small Business Jobs Act," *Law360*, Feb. 21, 2014.
- "Seventh Circuit: Reassignment of Disabled Workers is not Required," *The Corporate Counselor*, May 2012.
- "The Contingency Contracting Corps in Counterinsurgency Operations: Using Money to Effectively Fight Insurgents," *Public Contract Law Journal*, Fall 2010.

About RJO -- GOVERNMENT CONTRACTS

- San Francisco (1981)
- Washington, DC (2011)
- Ranked in Chambers USA
  - GovCon Tier 2
- 15+ GovCon Attorneys
- Experience across the spectrum
- Impressive clients of all sizes
- Enterprise-critical assignments
- Committed to public contracts
- Demonstrated thought leadership
- Cleared attorneys, SCI capable