Privacy and Data Security Update for Defense Contractors

T.J. Crane

May 19, 2017

Overview

- DoD interim rule
  - Expanded DFAR reporting obligations
  - New DFAR definitions
  - Cloud services
- Changes to local breach notification laws
- Possible federal breach notification law

Caveats

- Not intended to
  - Cover all laws or industries
  - Create an attorney-client relationship

- Seek counsel for a particular legal issue

Expanded reporting obligations

Key points on reporting

- Rule applies to all contractors with covered defense information residing in or transiting through their information systems

- Requires safeguarding and reporting, without abrogating prior requirements

Key points on reporting (cont'd)

- Subcontractors must report to the prime contractor, and directly to DoD
  - This could lead to inconsistent reports
- Pertains not just to unclassified controlled technical information
  - Think CDI, not UCTI

Key points on reporting (cont'd)

- Covered defense information is unclassified information that is
  - Provided to the contractor by or on behalf of DoD in connection with contract performance; or
  - Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of contract performance

Key points on reporting (cont'd)

- And is:
  - Controlled technical information,
  - Critical information (operations security),
  - Export control, or
  - "Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (*e.g.*, privacy, proprietary business information)"

Key points on reporting (cont'd)

- And is:
  - Controlled technical information,
  - Critical information (operations security),
  - Export control, or
  - "Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (*e.g.*, privacy, proprietary business information)"

When to report?

- Discovery of a "cyber incident that affects"
  - A covered contractor information system,
  - Covered defense information residing in a covered contractor information system, or
  - The contractor's ability to perform contract requirements that are designated as operationally critical support

"Cyber incident"

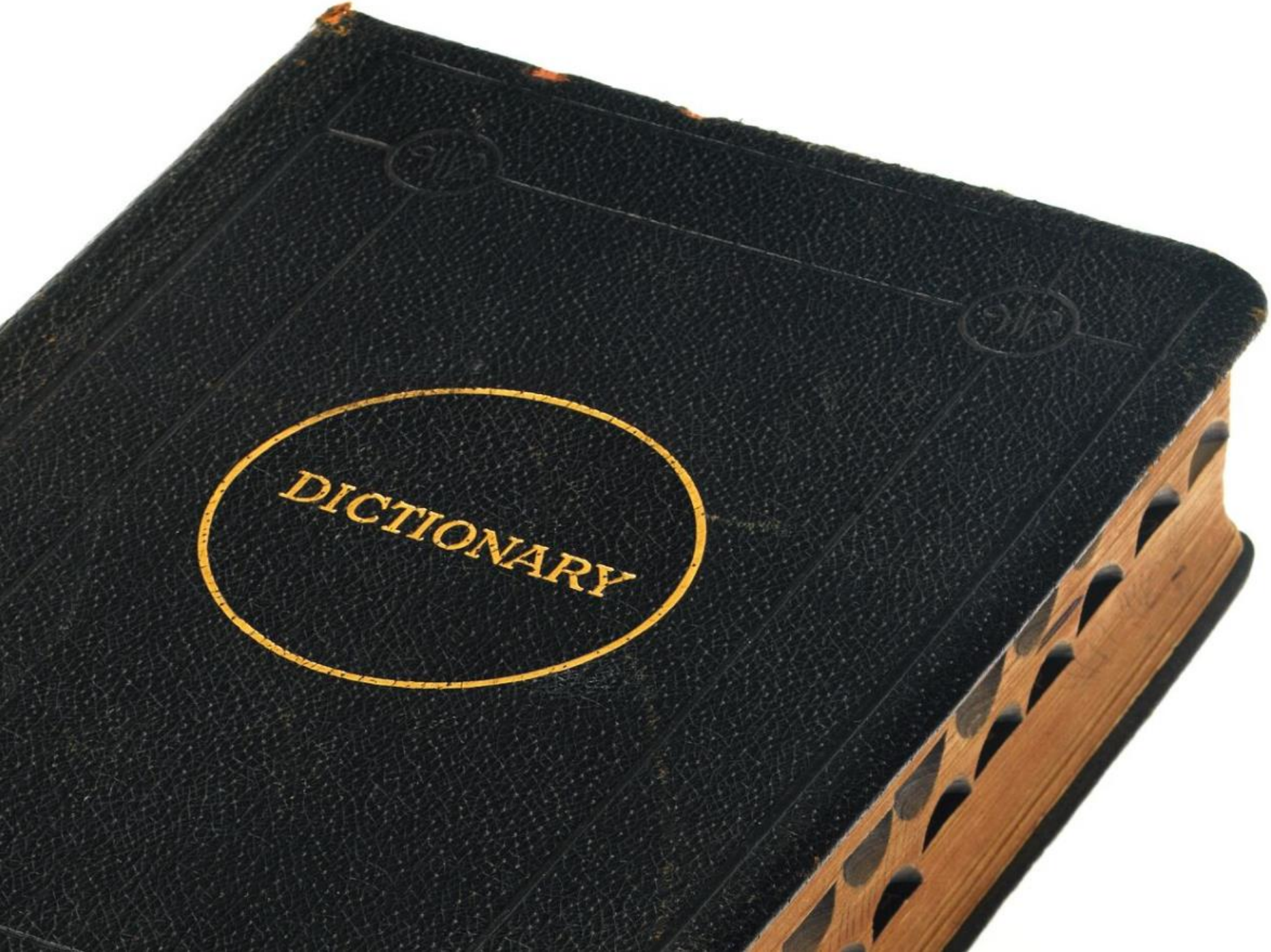
- Actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein

"Cyber incident"

- Actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein

"Cyber incident"

- Actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein


DICTIONARY

New definitions

48 C.F.R. § 202.101

"Compromise"

- 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

"Compromise"

- 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

"Media"

- Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system

Reporting obligations

- Conduct a review for evidence of compromise and analyze the systems involved

- "Rapidly report" cyber incidents to DoD
  - This still means within 72 hours

Welcome to the DoD-DIB Cyber Incident Reporting & Cyber Threat Information Sharing Portal

Text only version

Home | Contact | Resources | Login or Sign Up

Report a Cyber Incident

Access to this page requires a DoD-approved medium assurance certificate. For more information please visit the ECA website.

Apply to DIB CS/IA Program

Cleared defense contractors apply to join the DIB CS/IA Program for voluntary cyber threat information sharing. Access requires a DoD-approved medium assurance certificate. For more information please visit the ECA website.

Log into the DIB CS/IA Information Sharing Portal

Current DIB CS/IA Program participants login to the DIBNet portal. Access requires a DoD-approved medium assurance certificate. For more information please visit the ECA website.

What to provide?

- A cyber incident report;
- Malicious software, if detected and isolated; and
- Media (or access to covered contractor information systems and equipment) upon request

Is my reporting protected?

- Trade secret or otherwise proprietary information?
- Might reporting be interpreted as an admission of failing to provide adequate security?

Limitations on use

- Access and use of information received or created in the performance of the contract
  - Is limited to the purpose of furnishing advice or technical assistance directly to the Government in support of its activities and
  - Shall not be used for any other purpose
- Contractor must protect the information from unauthorized release or disclosure

Limitations on use (cont'd)

- Contractor must "ensure that its employees are subject to use and nondisclosure obligations…prior to…being provided access to or use of the information"

- Reporting party is a third-party beneficiary of the non-disclosure agreement between the Government and the contractor

Limitations on use (cont'd)

- Contractor shall include this clause in all subcontracts that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items

Limitations on use (cont'd)

- Information shared "shall not, by itself, be interpreted as evidence that the contractor … failed to provide adequate information safeguards for covered defense information…."
- A breach of the reporting obligations or restrictions can give rise to criminal, civil, administrative, and contract actions

Cloud services

Cloud computing defined

- "[A] model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources … that can be rapidly provisioned and released with minimal management effort or service provider interaction."
  – 48 C.F.R. § 239.7601

Cloud computing defined (cont'd)

- This includes other commercial terms:
  - On-demand self-service,
  - Broad network access,
  - Resource pooling,
  - Rapid elasticity, and
  - Measured service
- Also, any _____-as-a-service

On cloud services

- Before contracting, contractors must declare any intent to use cloud computing
- DoD will first require provisional authorization by Defense Information Systems Agency

On cloud services (cont'd)

- Services must be provided in accordance with the Cloud Computing Security Requirements Guide
  - http://iase.disa.mil/cloud_security/Pages/index.aspx
- Must not access, use, or disclose Government data unless specifically authorized by contract, task order, or delivery order

On cloud services (cont'd)

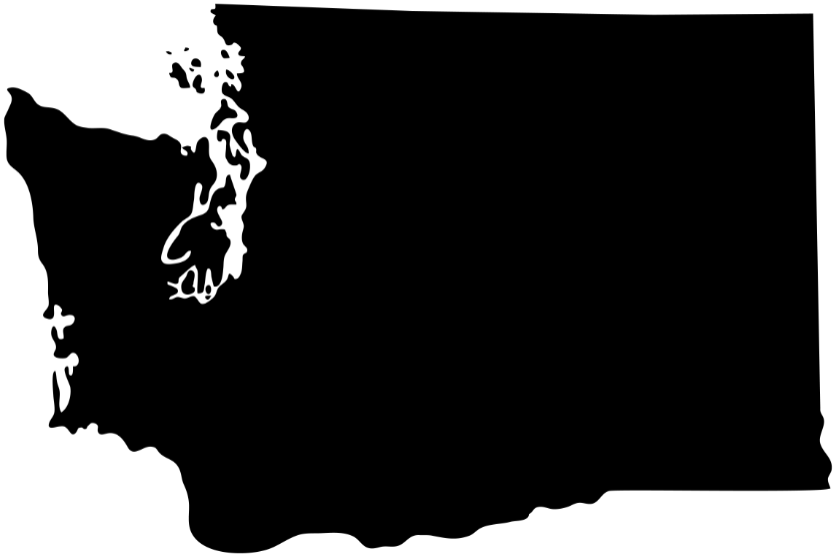
- Without written authorization, cloud computing service providers must maintain all Government data that is off of DoD premises within
  - The 50 states,
  - The District of Columbia, or
  - The outlying areas of the United States

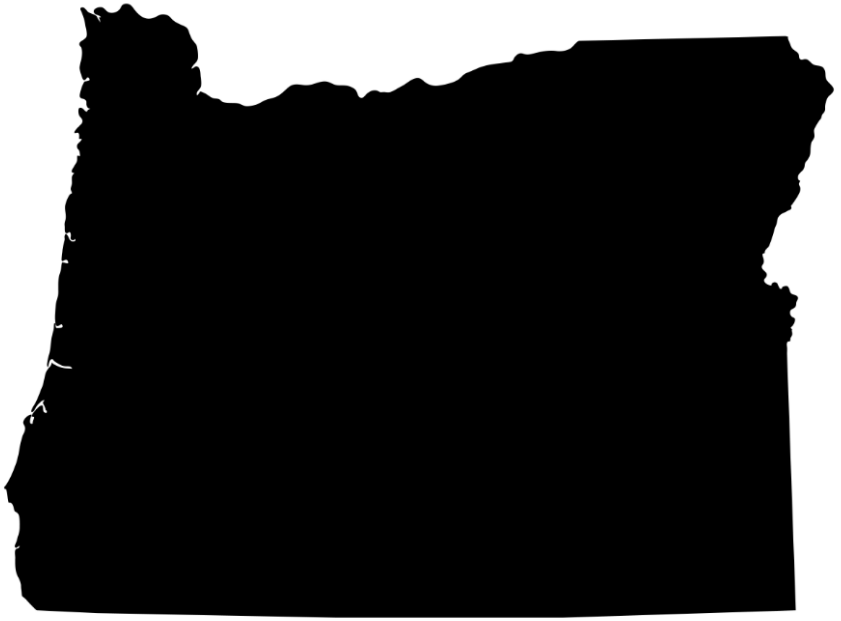
On cloud services (cont'd)

- Contractors shall ensure that employees are subject to the access, use, and disclosure prohibitions and obligations
- Prohibitions and obligations survive the contract

On cloud services (cont'd)

- Without written authorization, cannot use Government-related data for any purpose other than to manage the environment that supports the Government data
- Must notify the Government of any requests for access to Government-related data (*e.g.*, warrant, seizure, or subpoena)





Selected changes in local data security breach notification laws

Notable changes in Washington

- No longer just “computerized” data
- “Secured” means
  - Encrypted to meet or exceed NIST standard or
  - Otherwise modified to render PI “unreadable, unusable, or undecipherable by an unauthorized person”

Notable changes in Wash. (cont'd)

- Must notify Washington Attorney General if more than 500 residents are affected

- Must notify
  - In "the most expedient time possible and without unreasonable delay"
  - But within 45 days (with exceptions for law enforcement and measures to determine the breach scope or restore system integrity)

Notable changes in Oregon

- Personal information now includes biometric data used for transactions
  - *E.g.*, fingerprint, iris, retina, etc.
- Must notify the Oregon Attorney General if more than 250 residents are affected

Notable changes in Ore. (cont'd)

- No notification needed upon reasonable determination that consumers are "unlikely to suffer harm"
  - Document in writing
  - Maintain the writing for five years
    - (Perhaps retain longer depending on risk profile)
- Expansion of personal information to include, e.g., certain health policy numbers

Discussion