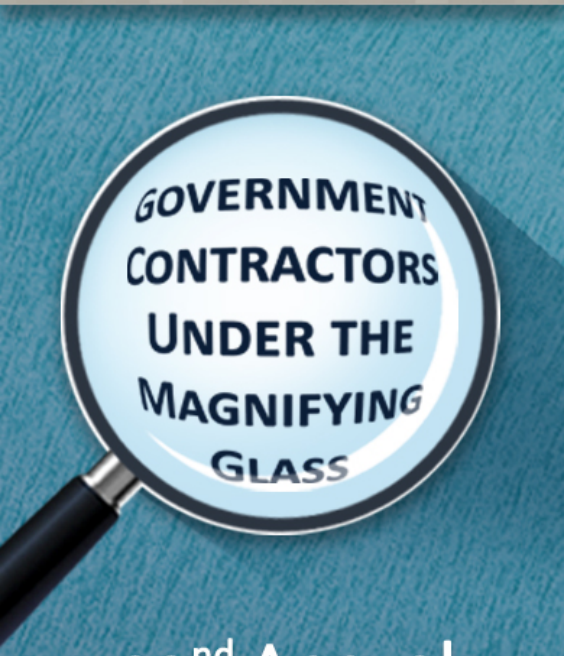
crowell moring



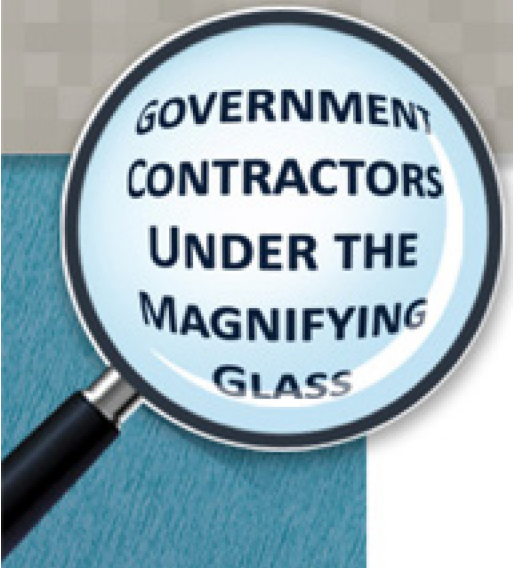
32nd Annual

WEST COAST OUNCE OF PREVENTION SEMINAR

May 18, 2016

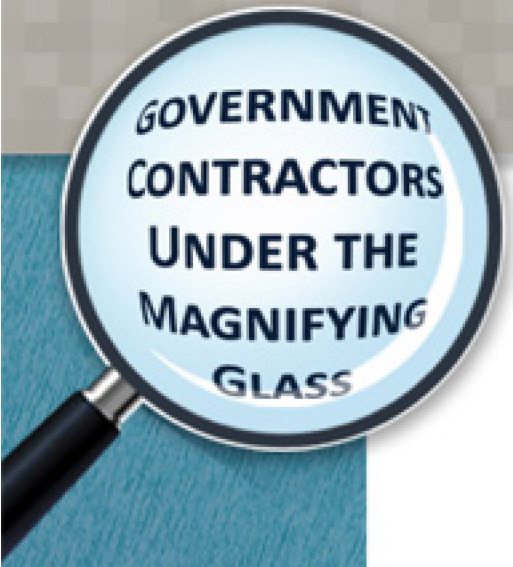
Protecting Information: Cybersecurity and Risk Management

Peter Miller
Jennifer Romano
Nathanial Wood

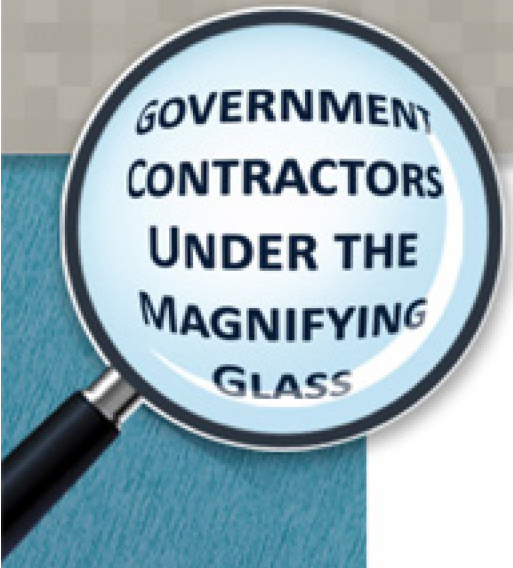


Overview

- Cybersecurity and Risk, Generally
  - Internet of Things
- New FAR Safeguarding Clause and "Old" DFARS Safeguarding Clause
- Data Incidents and Litigation

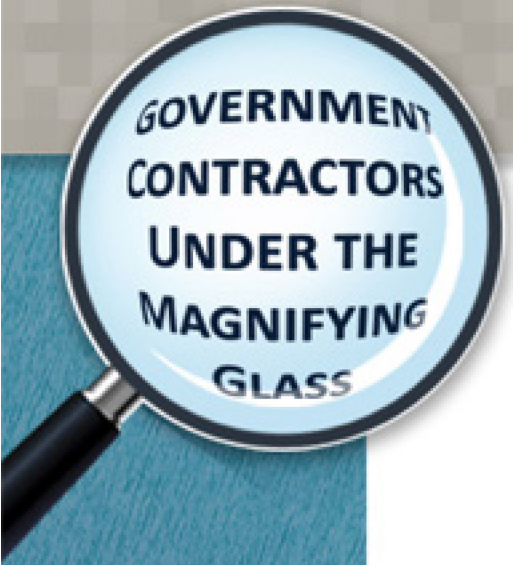


Cybersecurity and Risk, Generally



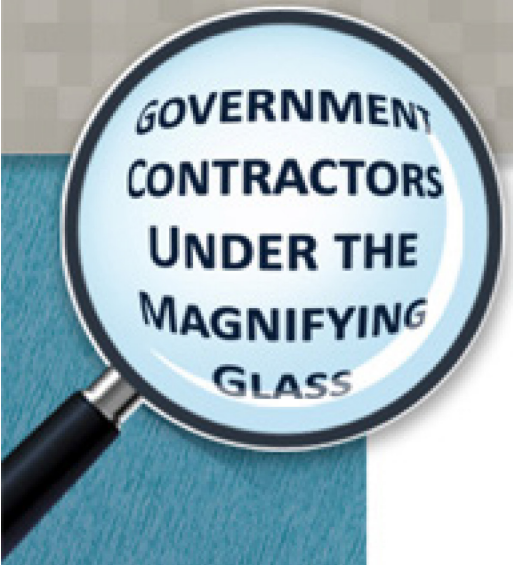
Managing Cybersecurity Risk

- No "one size fits all" approach
- Not a one-and-done activity: ongoing
- Variety of risk management frameworks and policy initiatives
- Federal government – carrot and stick
  - Statutes, guidance, and high-profile enforcement actions across industry sectors and activities (HHS, FTC, FCC, CFPB, SEC, DHS, DOJ, DOD…)
  - NIST Guidance (voluntary), e.g., Framework for Improving Critical Infrastructure Cybersecurity, Guide to Cyber Threat Information Sharing
- State government – privacy/cybersecurity teams, incident response, and risk reduction practices



Federal Cybersecurity Policy Initiatives

- NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (www.nist.gov/cyberframework/)
  - Voluntary, customizable, and provides a common vocabulary: "Identify, Protect, Detect, Respond, Recover"
  - "Supply chain risk is an essential part of the risk landscape that should be included in organizational risk management"
- NIST SP 800-150, *Guide to Cyber Threat Information Sharing* (http://csrc.nist.gov/publications/)
  - Information Sharing & Analysis Centers/Organizations (ISACs/ISAOs)
  - Cybersecurity Information Sharing Act of 2015 (12/15/15)
    - Any "non-federal entity" can share information with federal government "notwithstanding any other provision of law."
    - Information-sharing portals

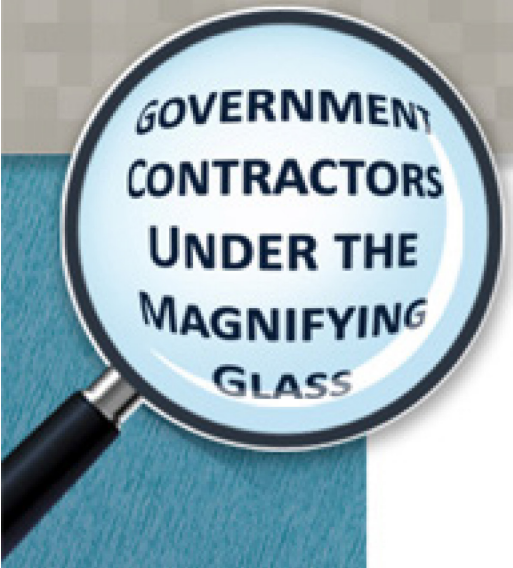


Internet of Things

- "Cyber-physical systems (CPS) [including IoT] are smart systems that include engineered interacting networks of physical and computational components."

  NIST Cyber Physical Systems Public Working Group, *DRAFT Framework for Cyber-Physical Systems*, Release 0.8 (September 2015)

- $11 Trillion Global Economy
  - $2 Trillion Today
  - Est. $11 Trillion in 2025
- More Devices than Humans
  - 25 Billion Devices → 50 Billion devices in 2020
- 127 New Devices/Second Added to Internet
- Exponential increase in data collection and analysis

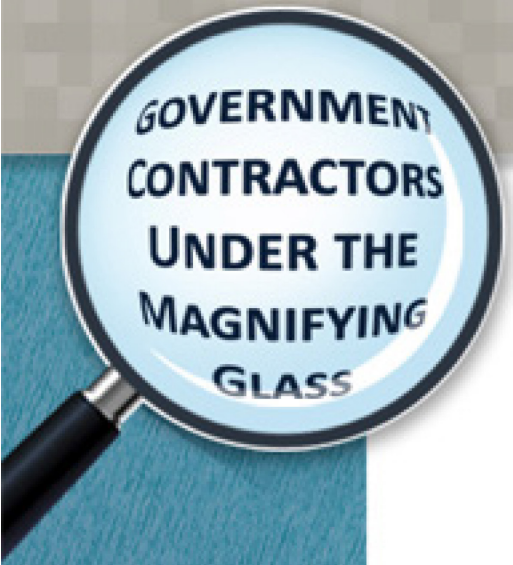


crowell moring

With Benefits Come Risks…

- Ubiquity
- Complexity
- Inconspicuousness
- Limited user interface
- Low cost, little incentive to secure
- Long life: limited patching, upgrades, or technology refresh
- Communications: who else involved?
- Interactions
- And on and on…

- Homes
- Healthcare and medical devices
- Vehicles and drones
- Business environments
- Physical and logical access
- Critical infrastructure
- Industrial and manufacturing processes
- Supply chains
- And on and on…



crowell moring

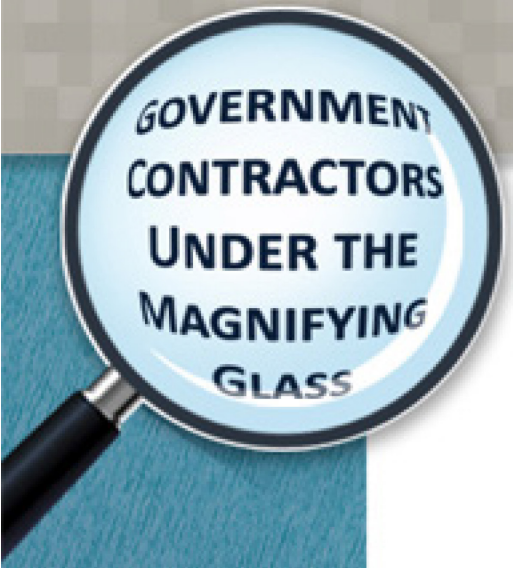
With Risks Come Regulation… and More Risk

- No common IoT standards or interoperability principles or "reasonable security" safe harbors
- Congress: "more than 30 different congressional committees" *Politico* (June 2015)
- Federal Government: Alphabet Soup

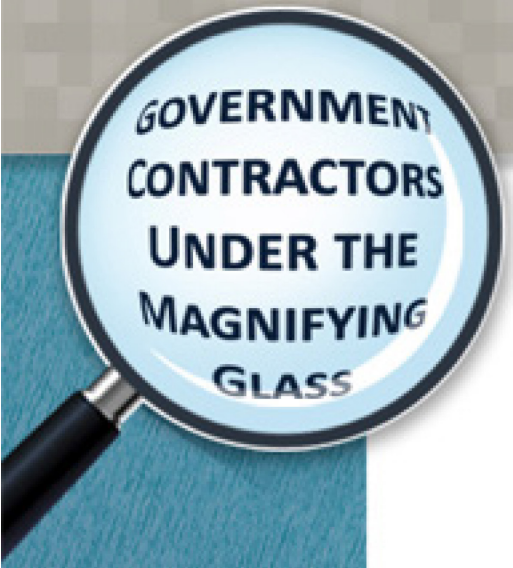
FTC – consumer catch-all	FDA – medical devices
FCC – spectrum	DOE(nergy) – smart grid
DOT – vehicles, aircraft, pipelines	DHS – critical infrastructure
DOJ – law enforcement	DOD – advanced technology
HHS – healthcare	

An estimated two dozen agencies with IoT-related interests …

- State Government: "little FTC Acts," general privacy and data security statutes, IoT-specific legislation
- Private enforcement actions

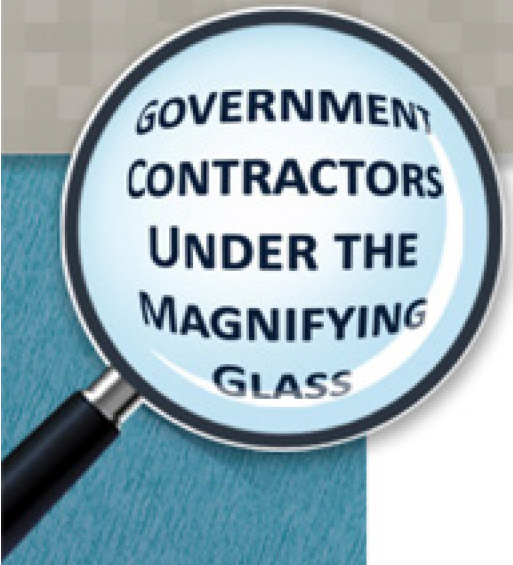


New FAR Safeguarding Rule and "Old" DFARS Safeguarding Rule



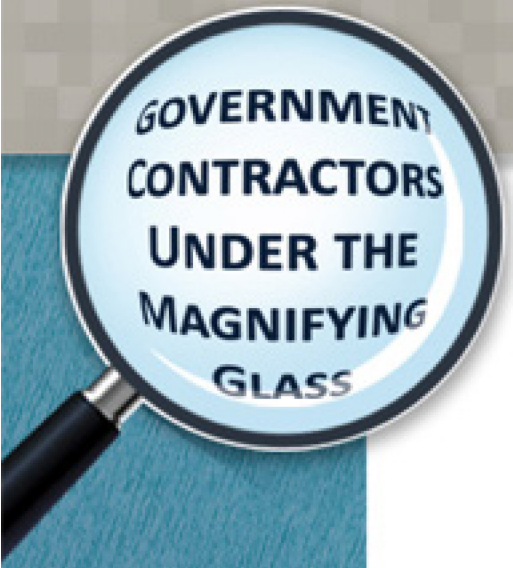
Background

- OPM Breach (along with other high-profile incidents, including IRS, DOE, TRICARE) result in internal initiatives to improve cybersecurity within agencies and across federal government (OMB, GAO, IGs)
- Increased recognition that federal government is out of step with private sector cybersecurity practices
- Return to basics: robust risk management practices, reasonable data security measures, vendor management, and accountability
- Cybersecurity practices aren't (yet) harmonized across federal agencies or within larger agencies.
- Cybersecurity tensions are reflected in agency administration of government contracts as well.



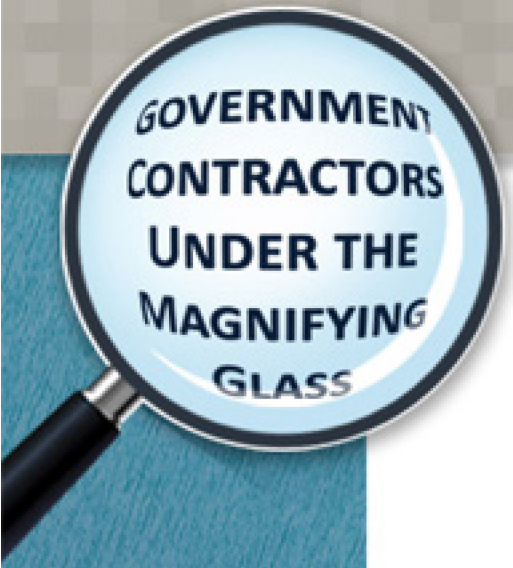
FAR 52.204-21: Basic Safeguarding of Covered Contractor Information Systems

- Newly published (5/16/16), effective in 30 days (proposed rule dates back to 8/4/12)
- Safeguards systems rather than specific information
- Covers any contractor and subcontractor information system that "processes, stores, or transmits" information "not intended for public release" that is "provided by or generated for" the Government
- Does not pre-empt more specific security requirements (DFARS, classified, CUI, agency, etc.), including "forthcoming FAR rule to protect CUI"
- "[I]ntent is that the scope and applicability of this rule be very broad, because [it] requires only the most basic level of safeguarding."
  - No exemption for simplified acquisition threshold
  - Applies to commercial acquisitions, but exempts Commercial Off the Shelf (COTS) items



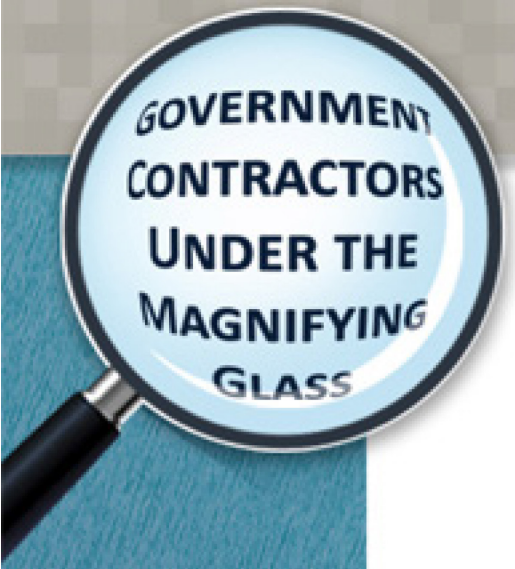
FAR 52.204-21: Basic Safeguarding of Covered Contractor Information Systems

- Requires contractors and subcontractors to implement 15 security controls taken from the security control families in NIST SP 800-171, *Protecting CUI in Nonfederal Information Systems and Organizations*
  - Access Control (4 specific controls)
  - Identification and Authentication (2)
  - Media Protection (sanitization and disposal) (1)
  - Physical Protection (2)
  - System and Communications Protection (2)
  - System and Information Integrity (4)
- "[A]s long as the safeguards are in place, failure of the controls to adequately protect the information does not constitute a breach of contract."

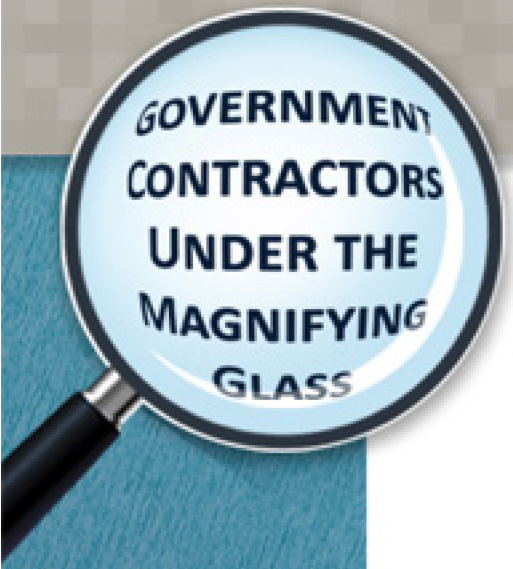


DFARS 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting

- Final Rule pending ("second interim rule" 12/30/15)
- Mandatory in all defense contracts and solicitations
- Requires "adequate security" to protect information systems handling covered defense information
- Requires written DoD CIO approval of "alternative but equally effective security measures"
- NIST SP 800-53 v. NIST SP 800-171
- Imposes cyber incident reporting requirements
- Exposes contractors to potential for extensive audits
- Growing concern over risk of contractor liability
  - Supply chain compliance
  - False Claims Act
  - Suspension & debarment



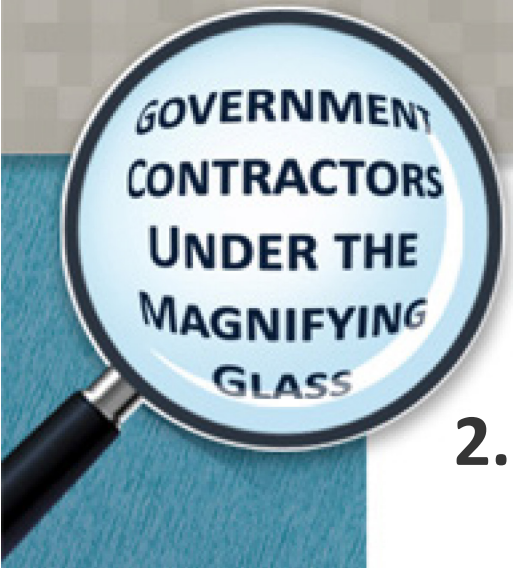
Data Incidents and Litigation



Responding to an Incident

1. Assemble the Team

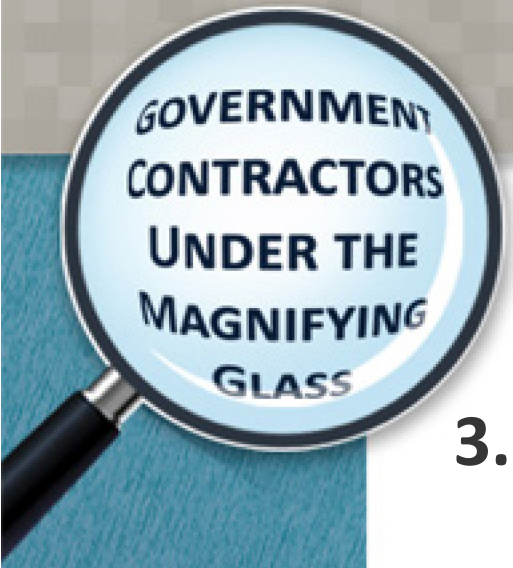
- Form your team per the incident response plan
- Investigative team—internal resources v. outside vendor
  - Consider creating separate team for obtaining legal advice
- Involve in-house/outside counsel immediately
  - Privileged communications/work product
  - Assess claims/positions vs. vendor
  - Strategize for long-run – investigation through class actions
- Involve risk management to assess insurance coverage and report incident to commence/preserve claim
- Involve corporate communications to ensure consistency with media statements
- Ensure effective internal reporting



Responding to an Incident

2. Investigate/mitigate/remediate

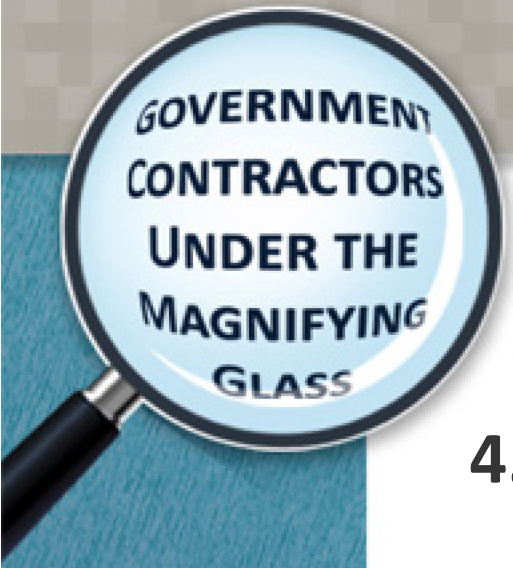
- Forensics
  - Can you identify type of infiltration and impact?
  - Can you show forensically that data not accessed?
  - Can you determine if data exfiltrated?
  - In case of missing device, can you determine what data it contained?
- Mitigate/Remediate
  - Can you track and recover lost data?
  - If technical cause, can it be fixed?
  - Are the cyber attackers still in the system?



Responding to an Incident

3. Notification

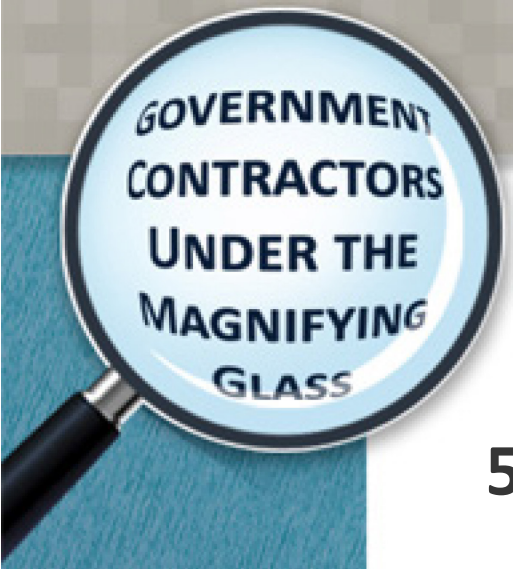
- Numerous constituencies: Law enforcement, Regulators, Customers, Public, Media, Business partners
- DFARS 252.204-7012
- OCR/HIPAA – HITECH
- State/Other Breach Notification Laws
  - Standards vary by state
  - AGs have enforcement authority
  - Timing: "in the most expedient time possible," "without unreasonable delay"
  - If required to notify in some states, notify in all states?
- Don't sugarcoat notification letter
- What do you do if you cannot determine extent of incident?



Responding to an Incident

4. Working with Regulators

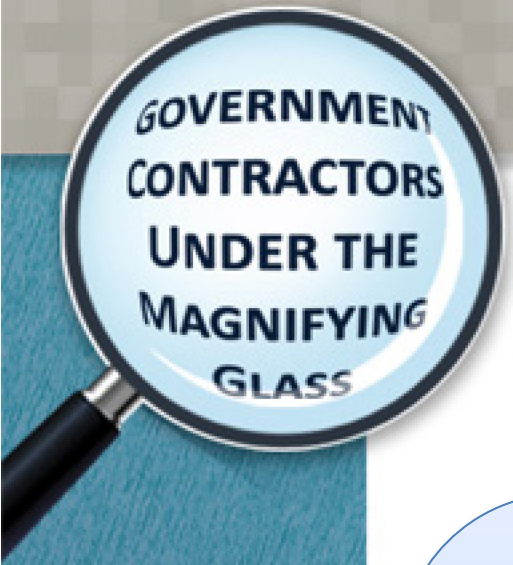
- Be proactive with regulators
- Establish relationship/bring them in the loop
- Beware of turf wars re regulators with overlapping jurisdiction
- Make sure they know that situation is fluid and you will update them



Responding to an Incident

5. Prepare for Litigation

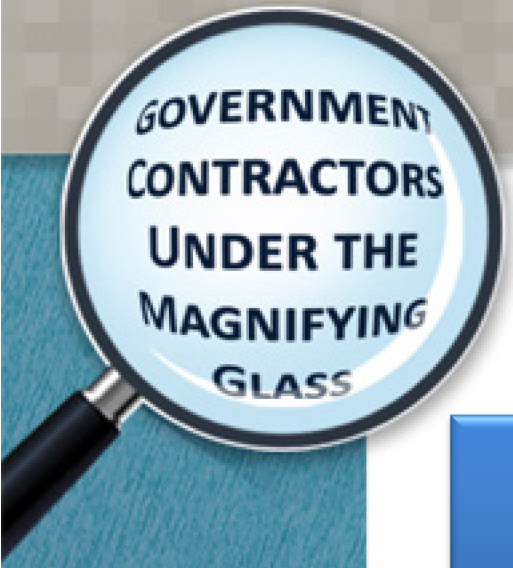
- Include litigation counsel in incident response
- Preserve critical evidence
- Document investigation/remediation efforts



crowell moring

Data Security Incidents Lead to Litigation on Many Fronts

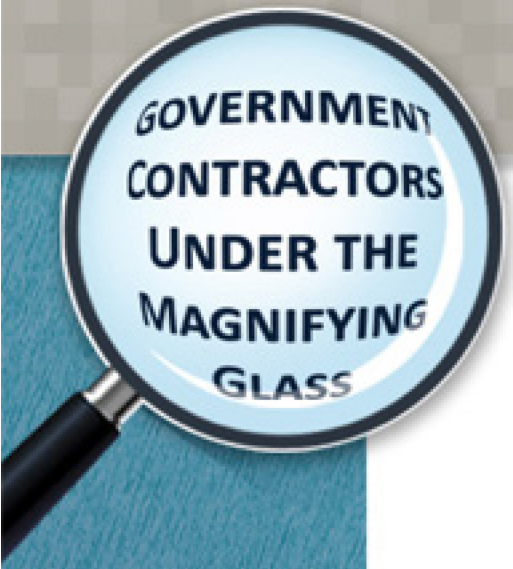
Govt. Customer	Public	Regulators	Prosecutors	Whistle-blowers	Other Impacted Parties
Breach of Contract	Class Actions	Fines	Criminal Penalties	False Claims Act	Ex.: Target credit card class
Indemnity	Statutory damages	Civil penalties			
Suspension	Injunctions	Consent Decrees			



crowell moring

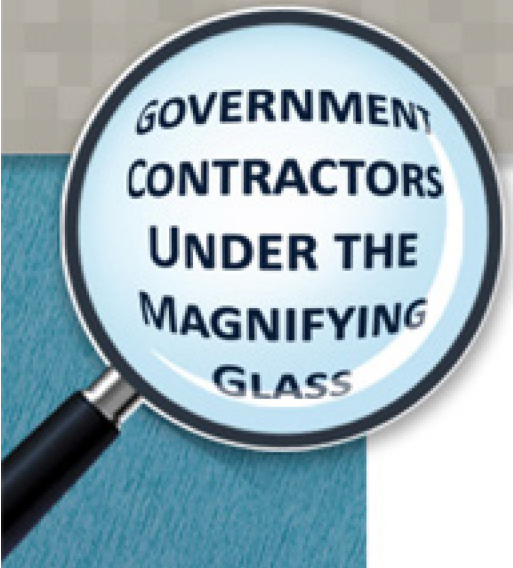
Litigation Trends: Creative Pleading

- Negligence
- Breach of Contract/Warranty
- Unfair Trade Practices
- Misrepresentation
- Violation of Privacy
- State Statutes (e.g. CMIA, Customer Records Act)
- Misappropriation
- Conversion



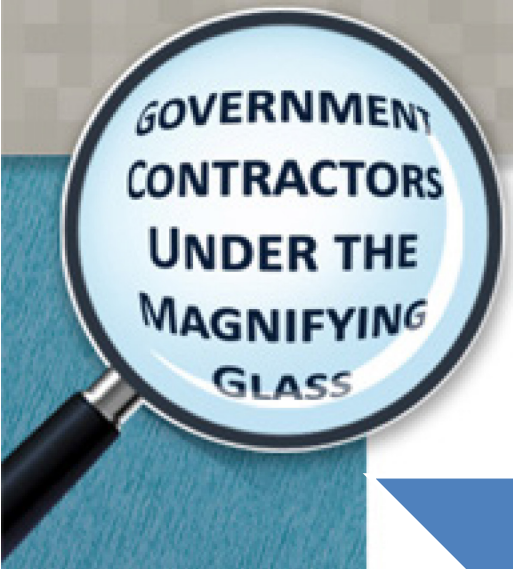
Litigation Trends

- *Spokeo, Inc. v. Robins*
  - Plaintiff alleged a statutory violation of the Fair Credit Reporting Act, even though the violation did not cause an actual injury (as opposed to risk of injury)
  - Trial court dismissed the case, Ninth Circuit reinstated the case
- Issue is standing: does a plaintiff have standing to sue based on a violation of a statute when he has not suffered an actual injury?
- Supreme Court reversed the Ninth Circuit and remanded for further proceedings
  - 6-2 decision, with Justices Ginsburg and Sotomayor dissenting
- Court did not announce a new rule—reiterated earlier rulings that plaintiffs must plead and prove both "particularity" and "concreteness" of harm
  - Ninth Circuit did not analyze "concreteness"
- Concreteness remains a nebulous concept
  - Can't be a "bare procedural violation, divorced from any concrete harm"
  - But, can be:
    - Procedural violation in some circumstances
    - Risk of real harm



Litigation Trends

- Cognizable injury or harm
  - Actual identity theft
  - Fear of future harm
- Causation
  - Connecting harm to the data incident



Manage Cybersecurity Risk for the Life of the Data

Assess the Risks

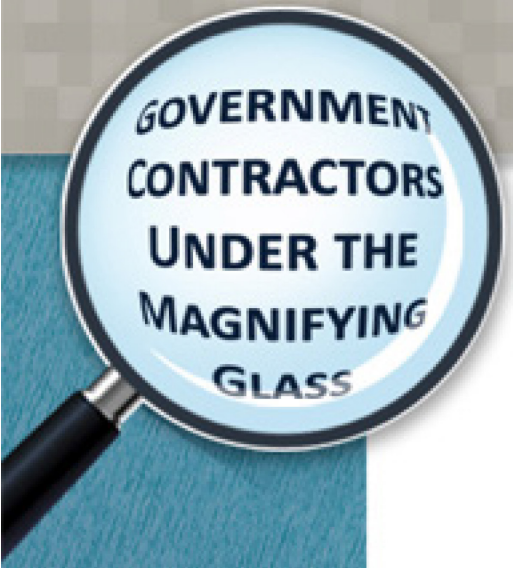
- Identify and classify data and systems
- Identify insider threats
- Identify external threats

Reduce the Risks

- Physical and information security controls
- Clear governance, policies and procedures
- Incident response plan
- Industry and government partnerships

Export, Accept, or Avoid the Risks

- M&A
- Insurance
- SAFETY Act
- Managed services
- Refrain from activity



crowell moring

Contacts

Peter Miller
Senior Counsel
202-624-2506
pmiller@crowell.com

Jennifer Romano
Partner
213-443-5552
jromano@crowell.com

Nathanial Wood
Counsel
213-443-5553
nwood@crowell.com