Off-Limits Information and Employee Mobility

Peter Eyre

Trina Barlow

Valerie Goo

Yuan Zhou

crowell moring

Agenda

- Common Scenarios
- Legal Considerations
- Reacting to Suspected Receipt of Off-Limits Information
- Best Practices for Preventing and Deterring Receipt of Off-Limits Information

crowell moring

Common Scenarios

- Employee mobility
- Hiring former government employees
- Inadvertently sent documents
- Deliberately obtained off-limits information
- Competitive intelligence

crowell moring

Legal Considerations

crowell moring

Trade Secrets

- Definition: Information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
  - (1) derives independent economic value from not being generally known to the public; and
  - (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy

80% of trade secret loss from employees, contractors, and trusted insiders

- Departing or disgruntled employees
- Intentional (malicious)
- Inevitable (knowledge acquired)
- By ignorance

crowell moring

Trade Secrets

Broad Scope of Trade Secrets

- Customer Lists
- Training Materials, Programs, and Methodology
- Pricing and Cost Data
- Strategic Plans and Forecasts
- Competitive Analyses and Intelligence
- Mechanical and Physical Processes
- Blueprints, Designs, and Prototypes
- Algorithms and Formulas
- Software and Source Code

crowell moring

Trade Secrets Spectrum

Tell
No One

Share with
Confidentiality

Publication

Perfect
Secrecy

No
Secrecy

"Secrecy Continuum"

crowell moring

Defend Trade Secrets Act

- Near unanimous support in both houses of Congress
- Signed into law May 11, 2016
- What's changed?

Unchanged	New
• Definition of trade secrets • Definition of misappropriation • All UTSA remedies still available • Statute of limitations	• Jurisdiction • Whistleblower provision • Ex parte seizure • International provisions • Sealing provision

crowell moring

Defend Trade Secrets Act

- Whistleblower Protection: Immunity from criminal or civil liability under state or federal law for disclosure of trade secret:
  - If made in confidence to federal, state or local official solely for purpose of reporting or investigating suspected violation of law
  - If disclosed in complaint or other document filed in lawsuit or other proceeding if made under seal
- Notice of immunity required in any contract (after May 2016) or agreement with employee (includes contractors and consultants)

crowell moring

Defend Trade Secrets Act

- Ex Parte Seizure
- "Extraordinary" additional remedy
  - Applicant must meet specific (and burdensome) requirements
  - Court must follow very specific procedure
  - Fees and/or damages allowed if remedy is unwarranted

crowell moring

Contractual Confidentiality Obligations

- Non-competes
  - Historically enforceable where narrowly tailored
  - But, non-competes increasingly disfavored by courts (concerns about job insecurity and employee mobility)
  - Executive Order 13495
- Non-solicits
- Confidentiality/nondisclosure
- Continuity of services
  - Relevant FAR clauses
- Contract clauses and teaming agreements

crowell moring

Off-Limits Procurement Information

- Implications of private disputes v. government overlay
- The government must establish a level playing field
- This includes making sure that:
  - (1) companies do not obtain an unauthorized competitive advantage by virtue of receiving non-public information; and
  - (2) Government decision making is free from the appearance of impropriety
- Exchanging or obtaining certain types of procurement information may:
  - Expose employees and the company to liability
  - Have bid protest implications
    - Result in exclusion from the competition
    - "Appearance of impropriety" may be sufficient to sustain protest

crowell moring

Procurement Integrity Act

- Prohibitions on knowingly disclosing and obtaining contractor bid or proposal or source selection information:
  - Subsection 2102(a):
    - Disclosure prohibition
    - Applicable to current or former government officials and certain acquisition support contractors/consultants
  - Subsection 2102(b):
    - "Obtaining" prohibition (term undefined)
    - Applicable to "a person" (term interpreted by caselaw)

crowell moring

Procurement Integrity Act

- Covered information is inclusive of some trade secrets
- "**Contractor bid or proposal information**" means the following if submitted to a Federal agency as part of, or in connection with, a bid or proposal to enter into a Federal agency procurement contract, if that information previously has not been made available to the public or disclosed publicly:
  - Cost or pricing data
  - Indirect costs and direct labor rates
  - Proprietary information about manufacturing processes, operations, or techniques marked by the contractor
  - Information marked as "contractor bid or proposal information"

crowell moring

Procurement Integrity Act

- "**Source selection information**" means information prepared for use by a Federal agency to evaluate a bid or proposal to enter into a Federal agency procurement contract, if that information previously has not been made available to the public or disclosed publicly
  - Source Selection and Evaluation Plans
  - Proposed costs or prices submitted in response to a Federal agency solicitation
  - Cost/Price and Technical Evaluation reports
  - Independent Government Cost Estimates
  - Competitive range determinations
  - Rankings of bids, proposals, or competitors
  - Catch all: anything else marked "Source Selection Information"

crowell moring

Procurement Integrity Act

- PIA obligations exist until contract award
- Requires government nexus
- The Savings Provision (41 U.S.C. § 2107):
  - The PIA does NOT restrict a contractor from disclosing its own bid or proposal information or the recipient from receiving that information
- Presents challenges with information provided to employees, teaming partners, consultants, etc.

crowell moring

Procurement Integrity Act

- Requirement for Prompt Reporting of Potential PIA Violations (41 U.S.C. § 2106)
  - No protest alleging a PIA violation unless the person, **no later than 14 days after the person first discovered the possible violation**, reported to the agency responsible for the procurement the evidence of the offense
  - Protests are only ripe when the agency completes its investigation after the 14-day notice has been made
  - Must file challenge at GAO within 10 days of notice unfavorable investigation outcome. *See SRS Techs.*, B-277366, July 30, 1997, 97-2 CPD ¶ 42

crowell moring

Organizational Conflicts of Interest

- FAR Definition (FAR 2.101): "An OCI arises when, because of other relationships or circumstances, a contractor may be unable, or potentially unable, to render impartial advice or assistance to the government, the contractor's objectivity in performing the contract work is or might be impaired, and/or the contractor would have an unfair competitive advantage"
- Three types:
  - A "biased ground rules" OCI has been found where one offeror provides assistance in drafting the RFP, SOW, or specifications (i.e., set ground rules for another gov't contract)
  - Impaired objectivity if a contractor is in the position of evaluating its own performance or products, or the performance or products of a competitor.
  - Unequal access to information that the contractor was fully entitled to access.
- Potentially result in disqualification or can prevent contractor from pursuing future work

crowell moring

Unfair Competitive Advantage

- The government must maintain a level playing field and avoid any appearance of impropriety
- Disqualification is potential risk if one offeror receives information that is competitively useful but not available to all offerors
- Particular risk for former government employees; notable GAO case law

crowell moring

Reacting to Suspected Receipt of Off-Limits Information

crowell moring

Reacting to Suspected Receipt of Off-Limits Information

- Preparation and planning (Code of Conduct)
- Training
  - Know what to look out for
    - Form of information (not necessarily written)
    - Types of markings (e.g., "proprietary," "source selection sensitive")
  - Educate employees on what to do
- IT/Vendors
  - Document retention & forensic analysis
  - Computer use restrictions – CFAA (tool to protect competitively sensitive data)
  - Private right of action against person
    - Who knowingly and with intent to defraud
    - Accesses a protected computer without authorization, or exceeds authorized access ….
    - Underscores need to maintain computer use policy restricting employees' authorized access to and use of company computers

crowell moring

Reacting to Suspected Receipt of Off-Limits Information

- Immediate steps
  - Quarantine the off-limits information
  - Conduct forensic analysis of the off-limits information (e.g., receipt date, access, other metadata)
  - Investigation of source of off-limits information
- Longer-term steps
  - Assess use of off-limits information
  - Assess public availability of such information
- Disclosures
  - To potential third parties
  - To Government
- Lessons and common pitfalls

crowell moring

Best Practices for Preventing and Deterring Receipt of Off-Limits Information

crowell moring

Best Practices for Preventing and Deterring Receipt of Off-Limits Information

On-boarding

- Determine protection strategy
  - Which employees will sign which agreements?
  - What are you trying to protect?
  - How are you trying to protect it?
  - Establish a repeatable process with HR
- Training: Educate employees about what constitutes trade secrets and protected off-limits information
  - Provide clear definitions of what is protected
  - Reinforce education and company commitment to safeguarding trade secrets/impropriety of off-limits information
  - Reflected in policies & procedures

crowell moring

Best Practices for Preventing and Deterring Receipt of Off-Limits Information

On-boarding

- Validation and controls
- Requesting and reviewing any pre-existing non-competes or non-solicits a new recruit may have
- Getting a certification that employee is not violating a non-compete or improperly using prior employers' information
- Special steps for former government employees
- Be mindful of "presumption of use"

Off-boarding

- Reiterating obligations to departing employees during the off-boarding process
- Conduct exit interview & ask the right questions
- Demand return of everything; verify return of emails, hard drives, portable media and storage

crowell moring

Best Practices for Preventing and Deterring Receipt of Off-Limits Information

Rules of the Road

- Before Proposal Submission
  - Comply with RFP requirements about communications with the Agency
  - Agency "point of contact" – use formal channels only
- After Proposal Submission
  - Generally there should be no attempt to communicate unilaterally with the government after submission of proposals

crowell moring

Best Practices for Preventing and Deterring Receipt of Off-Limits Information

Rules of the Road

- <u>After Completion of Procurement</u>
  - Some otherwise protected information may be releasable by the government (e.g., FOIA, Post-award debriefings)
  - Government must make this determination through official channels
  - Nonetheless, contractors must remain vigilant even after a procurement for potential risks
- <u>At all times</u>
  - If employees are offered or receive information and are unclear whether they're authorized to receive the information, then (1) immediately contact the Legal Department *before* reviewing the information; and (2) *do not share* the information with anyone else unless they have obtained clearance from the Legal Department (do not print, forward by email, or copy)

crowell moring

Best Practices for Preventing and Deterring Receipt of Off-Limits Information

Internal Controls

- IT controls (e.g., document retention, USB/hardware triggers, monitoring access & audits)
  - Physical security for access to trade secrets
  - Data security protocols
    - » Password protection / reminder pop-ups for employees
    - » Combination of protections for highly valued information
    - » Regularly run security checks to ensure systems have not been compromised and take action if they have
    - » Employee remote access issues
    - » Monitoring devices/software to protect most valuable assets
- Creating a Culture: training & awareness

crowell moring

QUESTIONS?

Trina Barlow
(202) 624-2830
tbarlow@crowell.com

Peter Eyre
(202) 624-2807
peyre@crowell.com

Valerie Goo
(213) 443-5505
vgoo@crowell.com

Yuan Zhou
(202) 624-2666
yzhou@crowell.com