Working with Law Enforcement: It Really is Possible

Don M. Blumenthal

Defcon 16

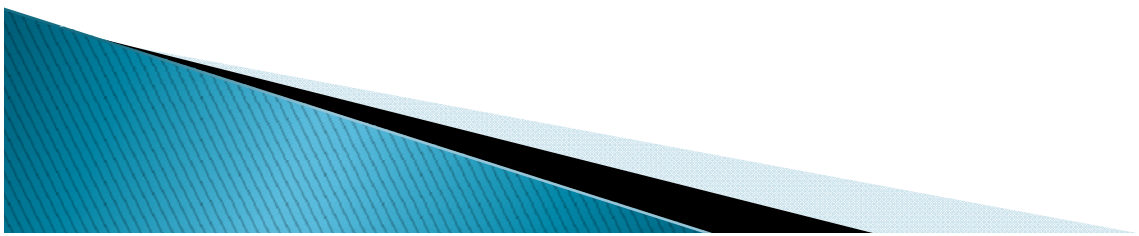
Las Vegas, Nevada

August 9, 2008

© 2008 – Don M. Blumenthal

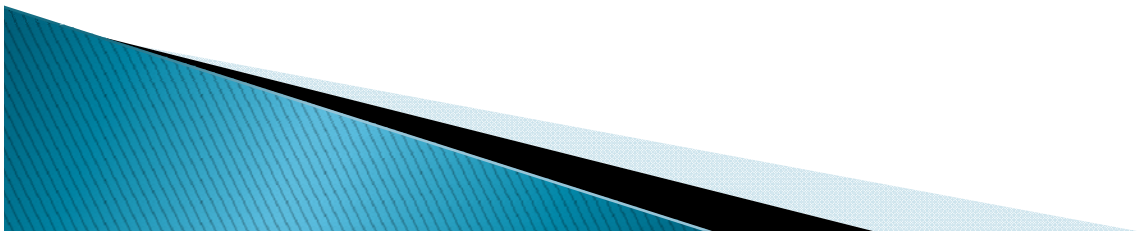
Disclaimer

- Opinions expressed are my own and intended for informational purposes. They should not be attributed to any organization or used as a substitute for direct legal or technical advice.



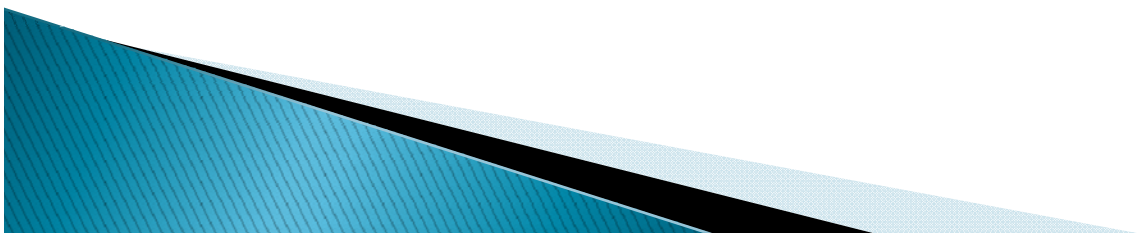
The Basics

- Laws vary
- Regulations vary
- Policies vary
- Procedures vary
- Individuals vary
- Necessary tactics vary
- However….



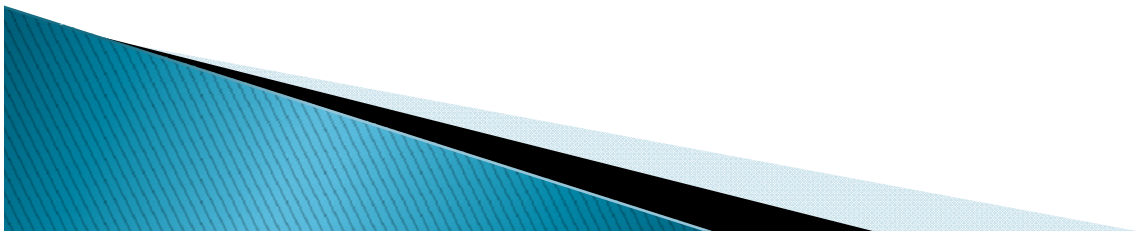
Fundamental Rules

- The fundamental points do not vary
- Show respect
- Don’t play games



Vary with Jurisdiction

- Civil
  - Court
  - Administrative
- Criminal
- Federal
- State



Federal Security/Privacy Examples

- Gramm-Leach-Bliley Act
- Fair Credit Reporting Act/Fair and Accurate Credit Transaction Act
- Health Insurance Portability and Accountability Act
- Family Educational Rights and Privacy Act
- USA Patriot Act
- FTC Act Section 5
- Sarbanes Oxley

© 2008 – Don M. Blumenthal

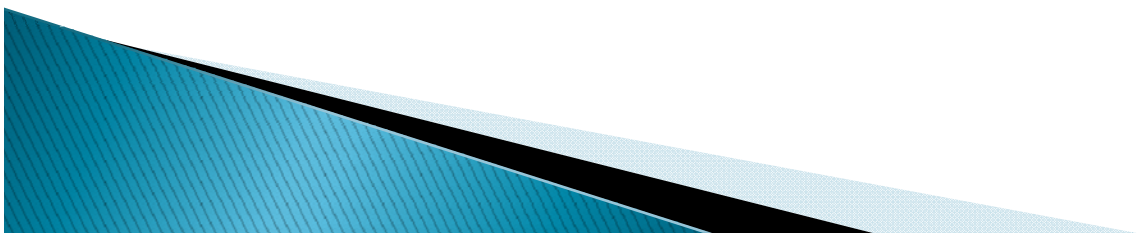
Federal Agencies

- GLBA – eight agencies
- FCRA/FACTA – FTC
- Sarbanes Oxley – SEC
- HIPAA – HHS
- FERPA – DoE
- Patriot Act – DoJ

© 2008 – Don M. Blumenthal

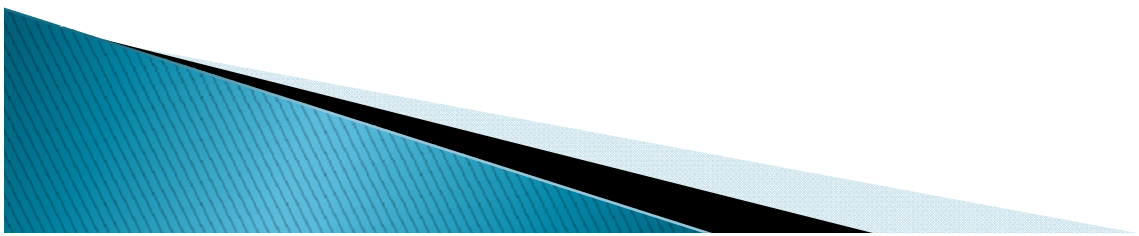
Vary with Context

- Formal investigation
  - Voluntary response
  - Mandatory response
- Target or third party
- “Just between you, me, and the lamp post….”
  - Procedural assistance
  - Investigation assistance
  - General information



Civil Action – Voluntary

- Access letter or similar document
  - AKA Voluntary process
- "We have opened a law enforcement investigation. Please provide documents responsive to the following questions…."

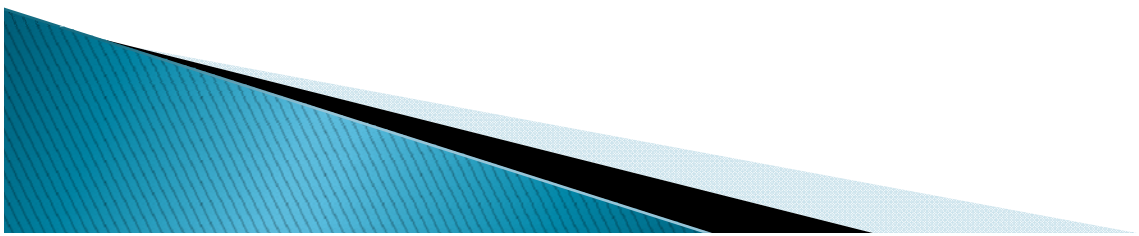


“Documents” Will Be Broad

- The term "documents" means all written, recorded, and graphic materials and all electronic data of every kind in the possession, custody or control of the company, whether on or off company premises….The term "documents" includes electronic mail or correspondence, drafts of documents, metadata, embedded, hidden and other bibliographic or historical data describing or relating to documents created, revised, or distributed on computer systems. . . . Therefore, the company shall produce documents that exist in electronic form, including data stored in personal computers, portable computers, workstations, minicomputers, cellular telephones, electronic messaging devices, pagers, personal digital assistants, archival voice storage systems, group and collaborative tools, portable or removable storage media, mainframes, servers, backup disks and tapes, archive disks and tapes, and other forms of online or offline storage….

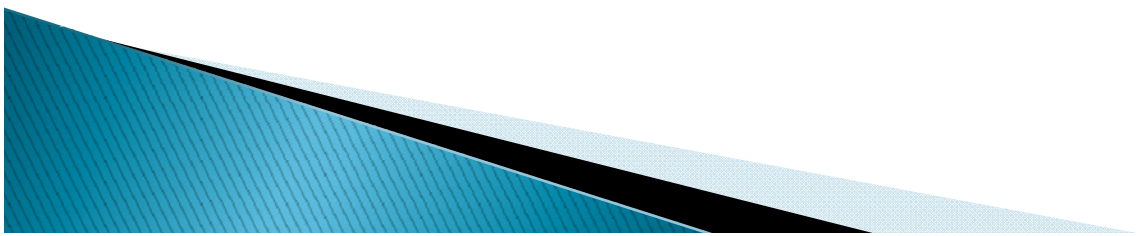
Access Letter

- Don’t ignore
- Review carefully
- Assign best possible person in company for each question
- Engage outsider if warranted
- Find out what documents are where and in what form
- Contact requesting attorney to discuss any issues concerning terms of letter



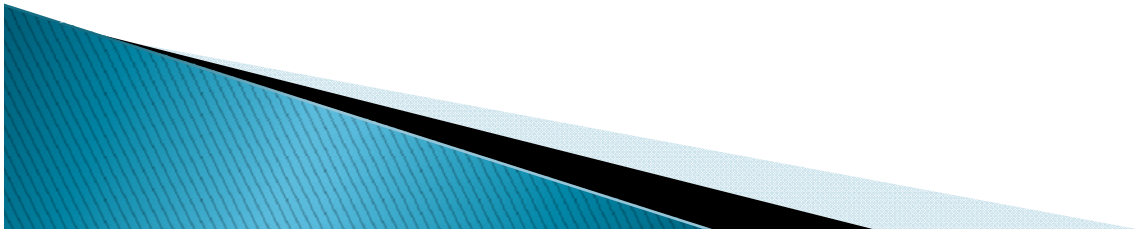
Interpret Requests Sensibly

- Government staff may not have technical knowledge
- Protect yourself – production or negotiation should address unclear or incorrect question structure
  - Too broad may be confusing
  - Too limited may tick off



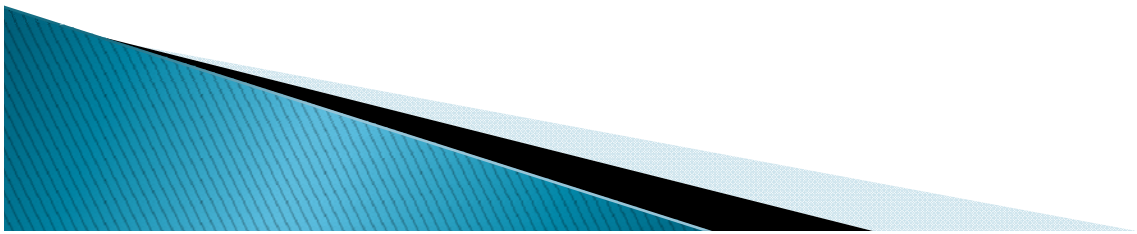
Compliance Issues

- Breadth (including time period) of request
  - May want to narrow
- Ongoing/rolling production
- Originals vs. copies
- Hard copies vs. electronic versions
- Form and location of production
- Bates stamping procedure



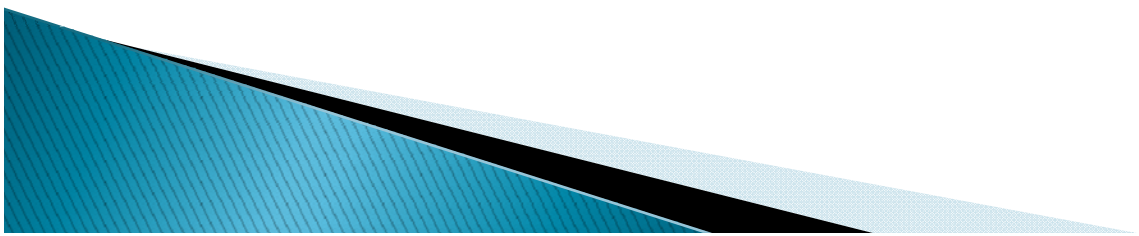
After Review and Contacts

- Be willing to meet with government staff; provides human touch and opportunity to add context and clarification
- Produce in usable and useful form
- Request confidential treatment
- Negotiate; cooperate ≠ be doormat



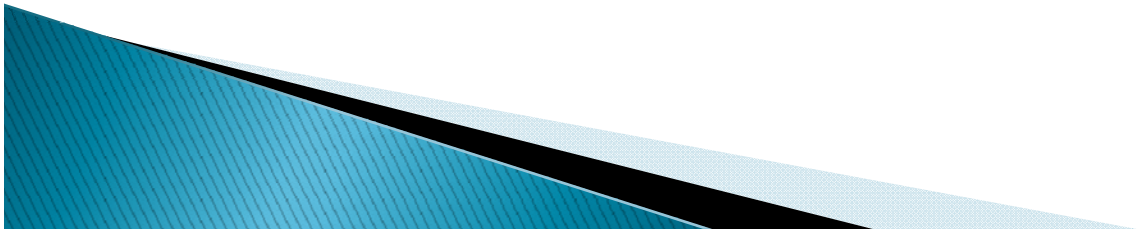
Results

- May resolve issues with no further action
- Lessens burdens if must proceed farther
- Can set atmosphere if must proceed farther



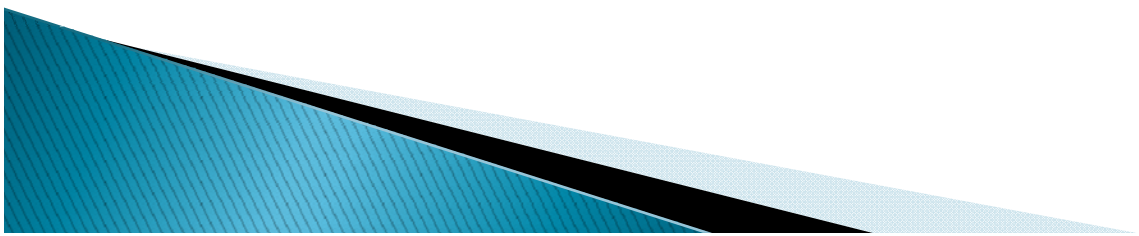
Civil Action – Mandatory

- Civil investigative demand (CID) or subpoena
  - AKA compulsory process
- "We have opened a law enforcement investigation.
  provide documents…
  responsive to the following questions…."



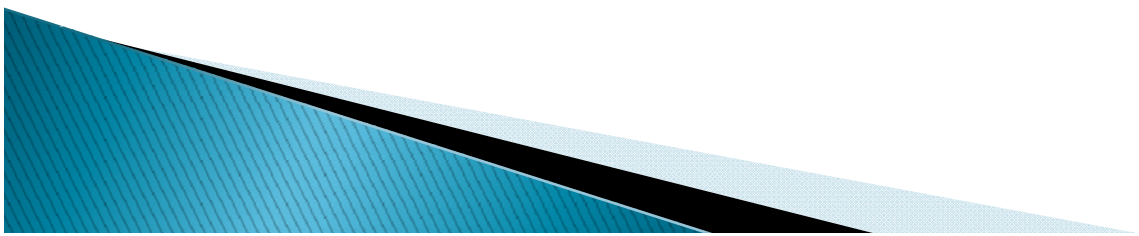
Process Differences

- Compulsory not limited to documents
  - Interrogatory – provide written answers to questions
  - Deposition – provide someone to testify under oath
- Sanctions for non-compliance



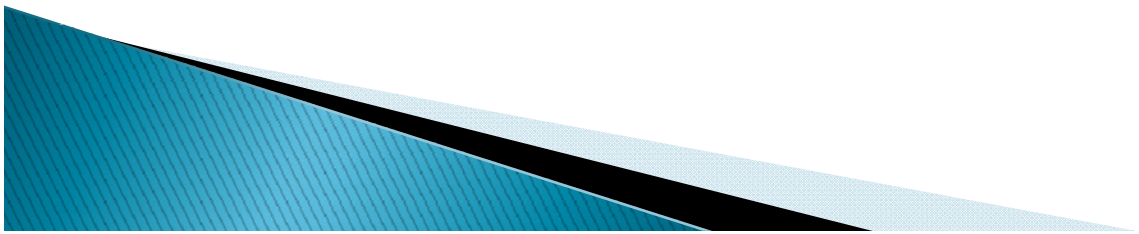
Compulsory Process

- DON'T IGNORE
- Review carefully
- Assign best possible person in company for each question or topic specified in deposition notice
- Contact requesting attorney to discuss any issues



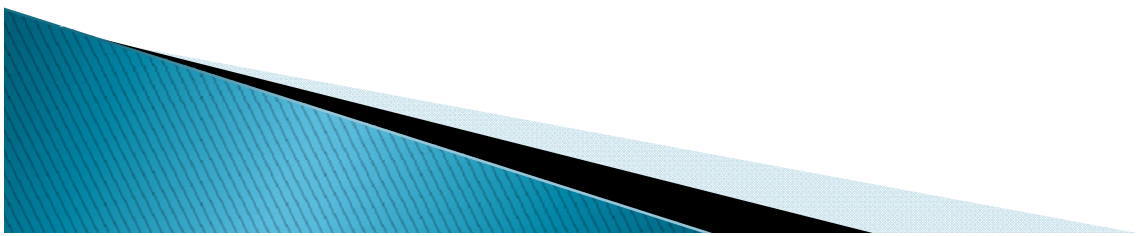
Compliance Issues

- Breadth (including time period) of request
  - May want to narrow
- Ongoing/rolling production
- Originals vs. copies
- Hard copies vs. electronic versions
- Form and location of production/depositions
- Bates stamping procedure



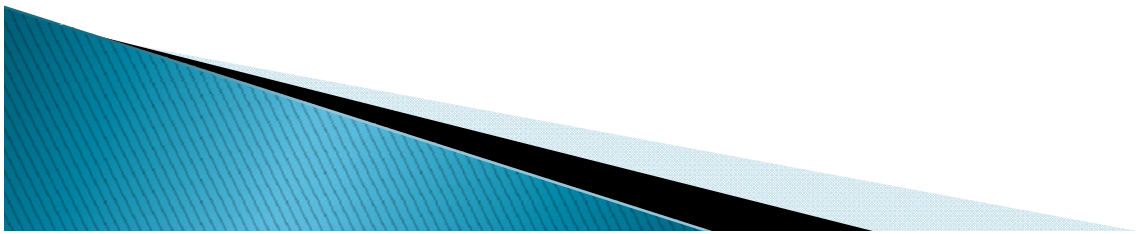
After Review and Contacts

- Negotiate outstanding issues as early as possible
- Raise confidential treatment
- Produce documents in usable and useful form
- Answer interrogatories clearly and completely
- Provide truly qualified people for deposition



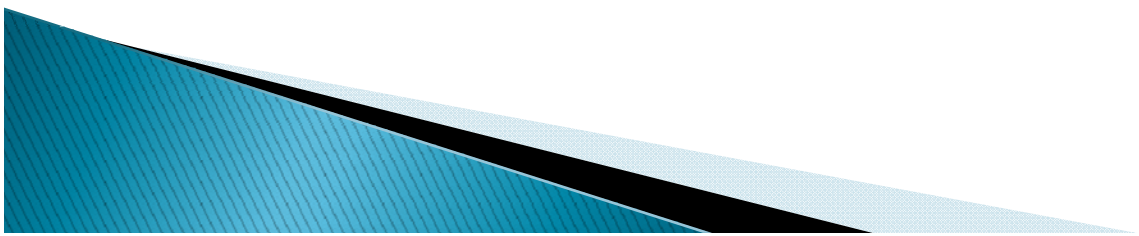
Criminal Action

- Stakes higher
  - Civil penalties are financial and injunctive
  - Criminal actions add the possibility of jail time
- 5th Amendment applies
- More adversarial atmosphere
- Can still have some level of cooperation



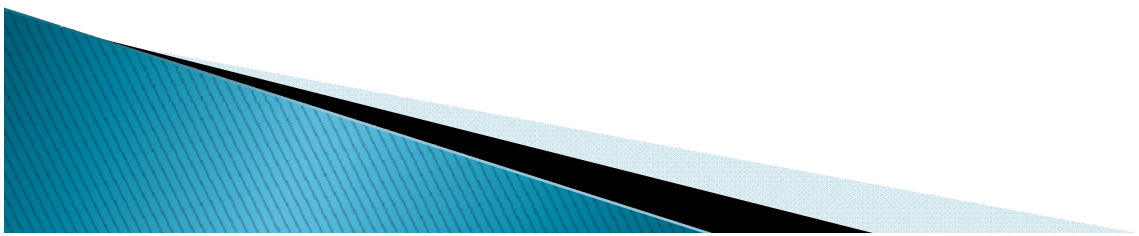
Prosecutor's Initial Decisions

- Grand Jury Subpoena vs. Search Warrant
- Whether government or company should have control over collection of records
  - Does a reasonable basis exist to believe that evidence may be destroyed, altered or removed?



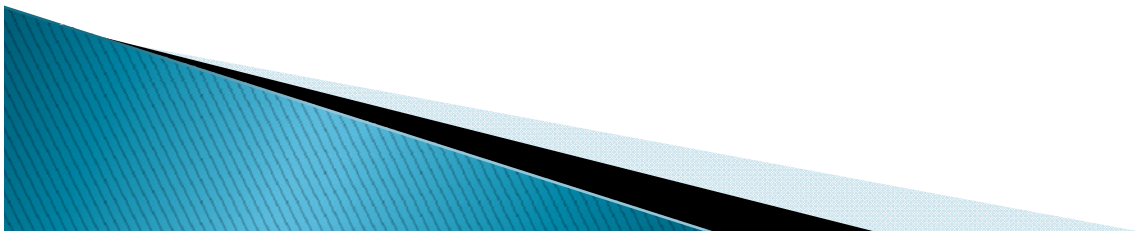
Compliance Issues – Scope

- Constitutional questions
- Grand jury testimony if applicable
- Breadth (including time period) of request
- Seek protective order setting parameters of search if you believe it's overbroad
- Negotiate handling of potentially privileged materials



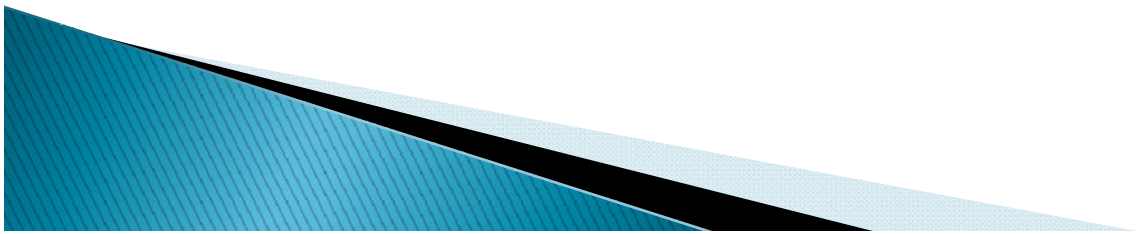
Compliance Issues – Procedure

- Ongoing/rolling production
- Originals vs. copies
- Hard copies vs. electronic versions
- Form and location of production and other elements
- Bates stamping procedure



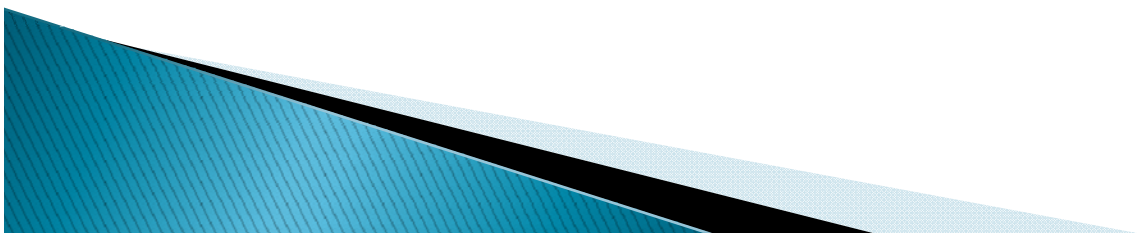
Third Party

- Don't have the protections that a target may have, but
- May still have obligations, or different ones, that a target may have
  - *e.g.,* ECPA
- Similar procedures and strategies
- Less need for confrontation



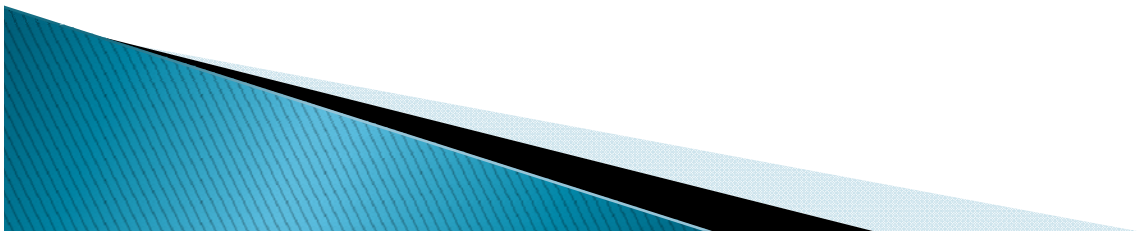
Help LE Find Answers

- Some material may be on public record
- Point to it
  - Helps LE
  - Lessens your burdens



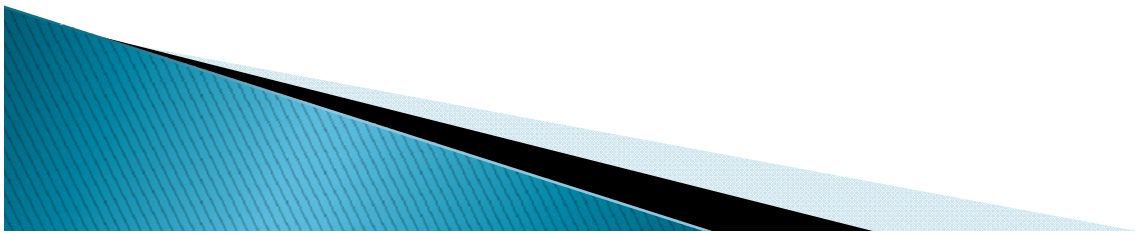
Bend Rules When Clear Risks

- Only after consultation with counsel!!!!!!!!!!
- Less likely in security cases than in other cybercimes
  - But if stolen data or cyber threat puts individual at risk….



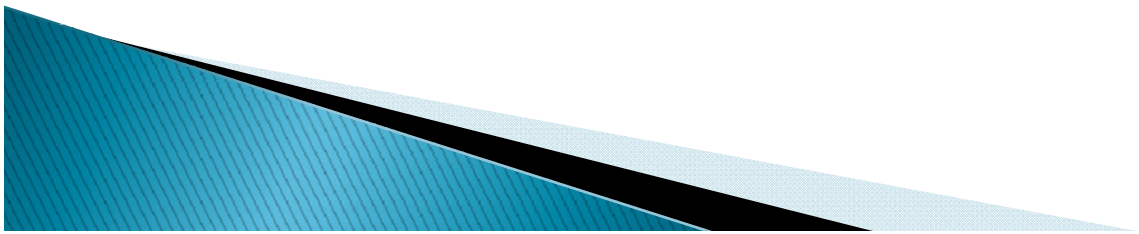
Protect Yourself in Advance

- Have terms of service that keep need for document production in mind
  - *e.g.*, "We will cooperate with law enforcement…."
- Can be in your self-interest depending on customer base



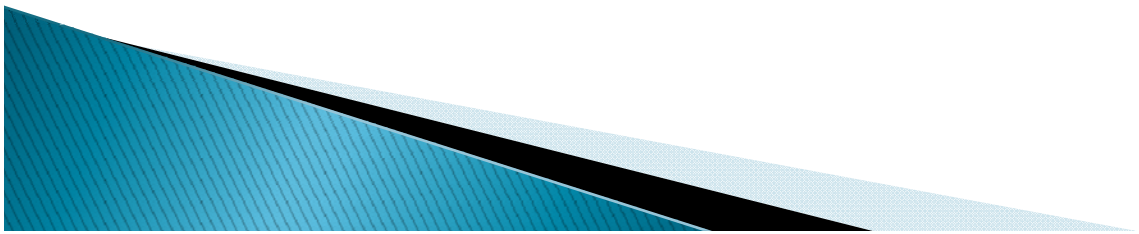
Adapt Business Processes

- Physical facilities for LE use if you have frequent contacts
  - *e.g.,* desk for local sheriff
- Electronic capabilities for LE use
  - Direct contacts for spam and phishing issues, instead of form or abuse@ address
- Designated/dedicated LE contacts and assistance
- Can be cost effective and have other benefits for both sides



Be Proactive

- Perception is important
- Publicize security activities
- Build relationship over time
  - Meetings, conventions
  - Groups such as Infragard
- LE more accessible and receptive if you have problems
- You know LE organization and organization knows you



Questions Later?

Don M. Blumenthal
don@donblumenthal.com
(734) 997-0764
(202) 431-0874 (m)
www.donblumenthal.com

