Washington Update: The Feds Impact Cybersecurity Without Passing Major New Laws

Brian Finch – Pillsbury Winthrop Shaw Pittman

Brian Caudill – American Gas Association

Introduction

- The Threat
  - Insider
  - Suppliers/Agents
  - Foreign
- Regulatory/Legal Landscape Updates
  - Proposed Laws
  - Recent Cybersecurity Related Cases
  - Pending Legislation
  - New Regulations
- New Strategies for Corporations to Tackle Cybersecurity
  - Liability Protections – Safety Act
  - Managed Security Services/Technology

pillsbury

The Threat

pillsbury

Data Breaches and Cyber Attacks

- Exposure of corporate secrets, trade secrets, and other proprietary information
- Exposure of personally identifiable information (employees and customers), including health information
- Disruption/destruction of operations

- Attacks are cheap: ($2 for crashing a website; $30 for malware verification; $5,000 for “zero day”)
- Malware now tends to be “one time use”

pillsbury

Who is Conducting Cyber Attacks?

pillsbury

Other Threat "Vectors"

- End-of-Life issues
- "Insider Threat"

pillsbury

Counterfeit Parts/SCRM

pillsbury

Who Is To Blame?

pillsbury

The In-Law Problem

pillsbury

Regulatory/Legal Landscape Updates

pillsbury

Overview of Cybersecurity Legal Authorities

Who is Responsible?

- Federal
  - Department of Homeland Security
  - Department of Energy
  - Department of Treasury
  - Department of Commerce
    - NIST, NSF, FTC
  - Department of Justice
  - Department of Defense
  - Securities Exchange Commission
  - Nuclear Regulatory Commission
- States
  - State Attorney Generals
  - Offices of Consumer Affairs and Business Regulation
- Trade Associations / Industry Groups

As a result, an ever complex array of domestic and global regulations is being enacted to protect the public from cyber attacks

pillsbury

Case Law: FTC v. Wyndham

- FTC v. Wyndham decided on April 7, 2014
  - Facts: Three separate security breaches that occurred between 2008 and 2011
  - Claim: Wyndham claimed that the FTC had no authority to pursue enforcement actions related to data security
  - Ruling: Court affirmed that the FTC has the authority to pursue corporate cybersecurity weaknesses under its existing regulatory powers (Section 5 of the FTC Act) to address unfair or deceptive acts or practices affecting commerce.
  - Significance:
    - Only a Motion to Dismiss – Not a Ruling on Wyndham's Liability
    - The FTC can act on unreasonable cybersecurity practices under existing laws without further legislation
- What is Reasonable Security?
  - Courts offering no consistent guidance

pillsbury

Administrative Penalties

- Just **LAST WEEK**, the Federal Communications Commission jumped into the field of data security regulation for the first time Friday, hitting a pair of telecommunications companies with a $10 million fine for allegedly failing to adequately safeguard customers' sensitive personal information.
- In a 3-2 vote, the commissioners decided to assess the fine against TerraCom Inc. and YourTel America Inc. for allegedly placing the personal data of up to 300,000 consumers at risk by storing Social Security numbers, names, addresses, driver's licenses and other sensitive customer information on unprotected Internet servers that “anyone in the world" could access.

pillsbury

Federal: Pending Legislation

- Countless cybersecurity proposals in the last three Congresses focused around ten themes:
  - Information sharing and cross-sector coordination
  - National strategy and the role of government
  - Reform of FISMA
  - Protection of critical infrastructure Breaches resulting in theft or exposure of personal data
  - Cybercrime offenses and penalties
  - Privacy in the context of electronic commerce
  - International collaboration
  - Research and development (R&D)
  - Training the cybersecurity workforce

H.R. 3696 – Game Change?

- HR 3696 passes the House **unanimously**:
  - Adds “qualifying cyber incident” after “act of terrorism”
  - Adds “cybersecurity technology” after “anti-terrorism technology”
  - Covers disrupting or jeopardizing the integrity, operation, confidentiality, or availability of IT systems/devices
  - Also (1) covers theft/disruption/destruction of data – including IP and PII, (2) disruption/destruction of systems, and (3) physical harm
- The main benefit of legislative changes is to clarify the authority of the Homeland Security Secretary, **NOT** to expand the SAFETY Act liability protections. **THE SAFETY ACT ALREADY COVERS CYBER ATTACKS NOT CONNECTED TO “TERRORISTS” AS THAT TERM IS COMMONLY USED.**

pillsbury

Remember - Congress Will Act Either Way

- Section 941 of the NDAA imposes disclosure requirements:
  - "Cleared Defense Contractors" have to report to DoD any time they suffer a network or information system "penetration"
  - DoD can inspect systems as they see fit
- Other new rules:
  - CR language banning Chinese IT system acquisitions
  - Supply chain risk management requirements
  - Disclosure of non-classified information system penetrations
  - More to come!
- Defense Department stepping up security requirements for transportation contractors

pillsbury

Executive Order 13636 – Procurement Changes

- *Institute Baseline Cybersecurity Requirements as a Condition of Contract Award for Appropriate Acquisitions* – For acquisitions that present cyber risks, the government should only do business with organizations that meet basic cybersecurity hygiene baseline requirements in both their own operations and in the products and services they deliver. This baseline should be expressed in acquisitions' technical requirements and include performance measures to ensure the baseline is maintained and risks are identified.
- *Address Cybersecurity in Relevant Training* – The government should incorporate acquisition cybersecurity into required training for appropriate workforces and require contractors to receive training about acquisition cybersecurity requirements.
- *Develop Common Cybersecurity Definitions for Federal Acquisitions* – The government should increase the clarity of key cybersecurity terms in federal acquisitions by defining key terms in the FAR.

pillsbury

E.O. 13636 (cont'd)

- *Institute a Federal Acquisition Cyber Risk Management Strategy* – The government should identify a hierarchy of cyber risk criticality for acquisitions and develop "overlays" for similar types of acquisitions, starting with acquisitions that present the greatest cyber risk.
- *Include a Requirement to Purchase from Original Equipment Manufacturers (OEMs), Their Authorized Resellers, or Other "Trusted" Sources, Whenever Available, in Appropriate Acquisitions* – The government should obtain required items only from OEMs, their authorized resellers, or other trusted sources, in certain circumstances, and the cyber risk threshold for application of this limitation should be consistent across the federal government. Again, DoD has already taken a step in this direction by issuing new supply chain risk rules.5
- *Increase Government Accountability for Cyber Risk Management* – The government should identify acquisition practices that contribute to cyber risk and integrate security standards into acquisition planning and contract administration. It should also incorporate cyber risk into enterprise risk management and ensure key decision makers are accountable for managing cybersecurity risks.

pillsbury

New Strategies for Corporations to Tackle Cybersecurity

pillsbury

Many Theories of Liability

- Shareholder claims/ SEC Disclosures
- Loss of IP/trade secret claims
- Negligent selection, design or contracting
- Failure to take “reasonable” security measures for threats that a company knew or “should have known” about
- Strict liability
- FTC/State UDAP claims, international regulator liability

pillsbury

What Would Litigation Look Like?

- Failure to:
  - remedy “known security vulnerabilities” such as allowing insecure server/network connections
  - employ commonly used methods to require user IDs and passwords that are difficult for hackers to guess
  - adequately inventory computers in order to manage network devices
  - employ reasonable measures to detect and prevent unauthorized access or to conduct security investigations
  - follow proper incident response procedures, including failing to monitor computer network for malware used in a previous intrusion
  - adequately restrict 3d party vendor access
  - share threat information/act upon shared information

pillsbury

9/11 Type Claims

- Courts have found that terrorist attacks are reasonably foreseeable, and a duty is owed to plaintiffs (victims)
  - The danger of a plane crashing as a result of a hijacking was "the very risk that Boeing should reasonably have foreseen"
- Other 9/11 cases:
  - Negligence/Negligent selection
  - *Res Ipsa Loquitor*
  - Strict liability
  - Negligent design and/or manufacture
- How can you make sure you are taking "reasonable" cyber security measures?

pillsbury

What, Sue Me?

- Recover From Terrorists?
  - The widow of murdered journalist Daniel Pearl has withdrawn a lawsuit seeking damages against al-Qaida, a dozen reputed terrorists and Pakistan's largest bank. [L]awyers noted that the defendants in the case had not answered the lawsuit.
- Recover From State Sponsors?
  - Beirut Bombing: A Federal judge ordered Iran to pay $2.65 billion to relatives of the 241 American military people killed in a 1983 bombing in Lebanon and to 26 survivors of the attack, a ruling that is likely to remain **symbolic**. How the nearly 1,000 plaintiffs can recover the damages is unclear, since Iran is estranged from the U.S., has denied responsibility for the attack, **and did not even respond to the lawsuit**.
- That leaves security vendors and property owners as the deep pockets, so YES YOU WILL BE SUED.

pillsbury

The SAFETY Act

"**S**upport **A**nti-Terrorism by **F**ostering **E**ffective **T**echnologies Act"

- Part of the Homeland Security Act of 2002
- **Eliminates** or minimizes tort liability for sellers of DHS-approved "technologies" should suits arise after an attack (physical or cyber), including:
  - SAFETY Act protections obtained only by submitting an application to DHS
  - ***Applies to services, products, policies***
    - This includes ***self-deployed programs***
  - Protections apply even if approved technologies are sold to **commercial** customers or if the attack originates from **abroad** so long as US interests implicated (i.e., economic losses)

pillsbury

Act of Terrorism = Cyber Attack

- Any cyber security product, service, and/or policy is eligible for SAFETY Act protections
- Cyber attacks are encompassed under this definition
- There is NO requirement that the attacker's identity or motivation be identified/proven:
  - Only mention of "intent" potentially relates to intent to cause injury or loss, NOT traditional "terrorist" intent
- This means that ANY cyber attack could potentially trigger SAFETY Act liability protections

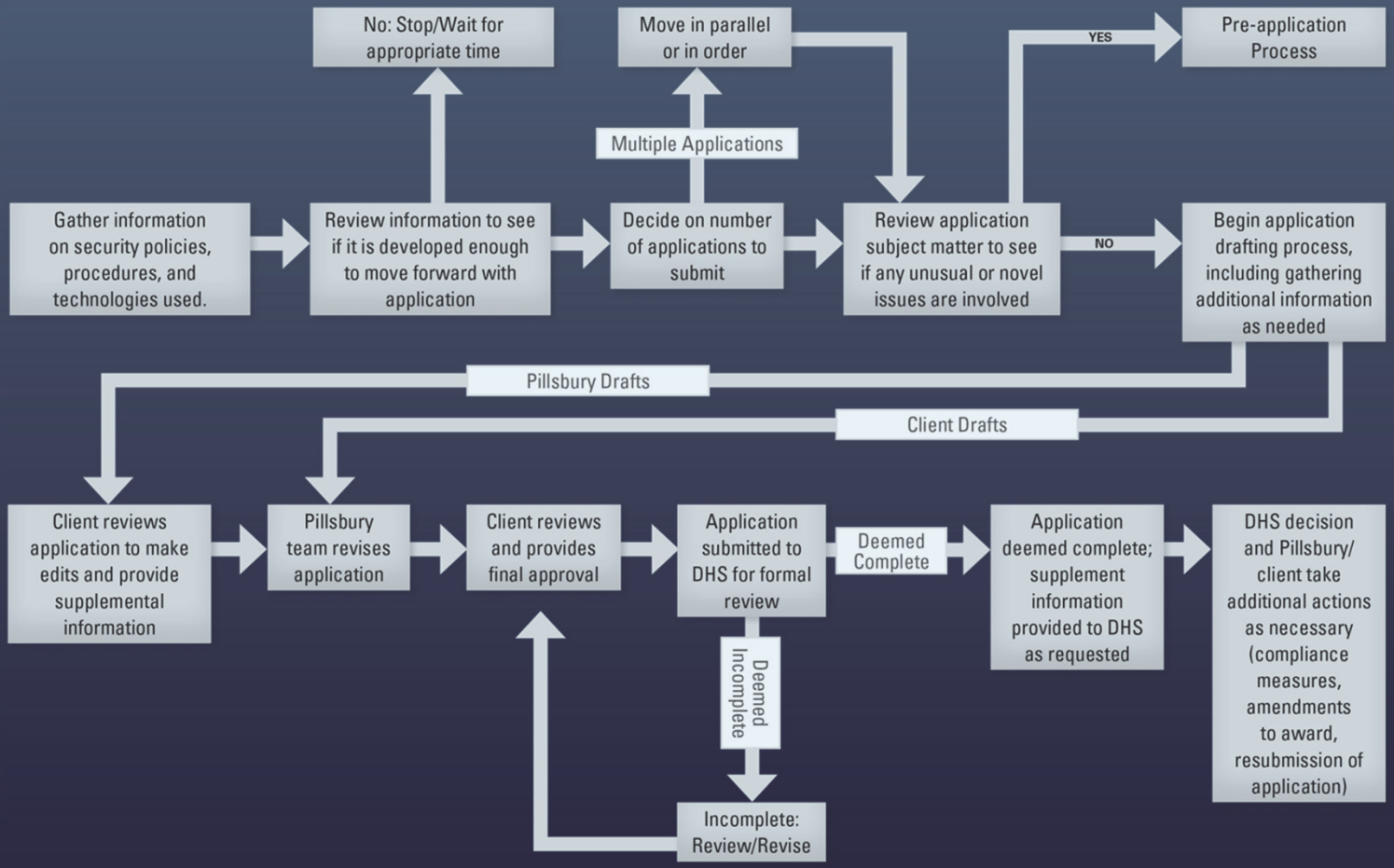
pillsbury

Designation vs. Certification

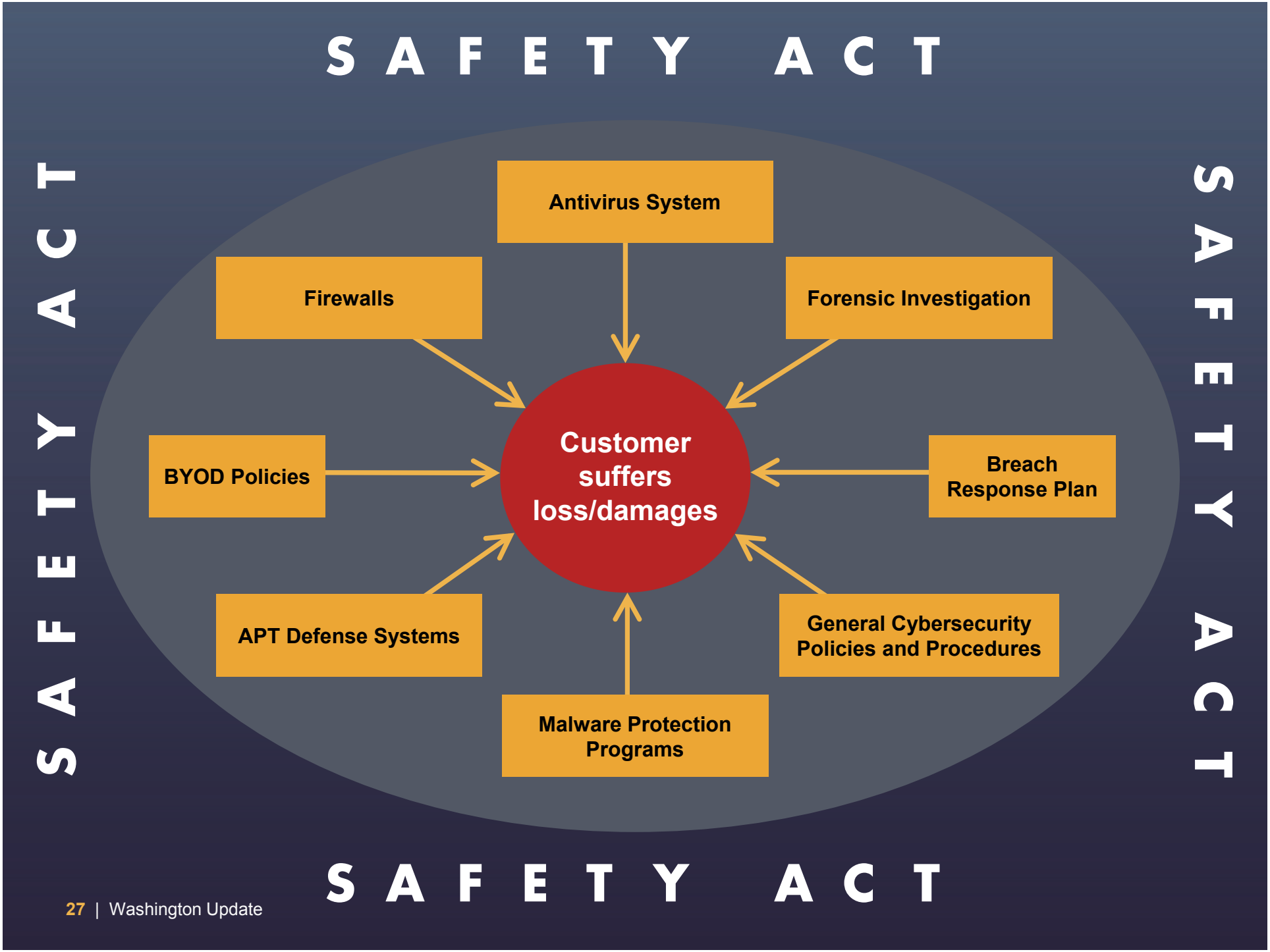
- Two levels of protection under the SAFETY Act
- Under “Designation”:
  - Claims may only be filed in Federal court
  - Damages are capped at a level set by DHS
  - Bar on punitive damages and prejudgment interest
- Under “Certification” sellers also receive a presumption of immediate dismissal
- In both circumstances claims against **CUSTOMERS are to be immediately dismissed**

pillsbury

The Application Process



pillsbury


SAFETY ACT
SAFETY ACT
SAFETY ACT
SAFETY ACT
Antivirus System
Firewalls
Forensic Investigation
BYOD Policies
Customer suffers loss/damages
Breach Response Plan
APT Defense Systems
General Cybersecurity Policies and Procedures
Malware Protection Programs

Key Questions and How To Use

- Any costs for filing a SAFETY Act application? **NO**
- What kind of cybersecurity products are eligible for SAFETY Act protections?
  - All *PRODUCTS, SERVICES, AND/OR POLICIES, INCLUDING INTERNAL POLICIES*.
- What is the practical effect of obtaining SAFETY Act protections?
  - ***A cap on damages or immunity*** from damages arising out of or related to cyber attacks.
- Can I realize SAFETY Act benefits just by purchasing and using SAFETY Act approved cyber security solutions? **YES**
- Can I require SAFETY Act approval in procurements? **YES**
- What kind of claims will this help mitigate/eliminate?
  - **Negligence, third party liability, failure to take reasonable mitigation steps, D&O claims**

pillsbury

SAFETY Act vs. Cyber Insurance

SAFETY Act

- Jurisdictional defenses (Federal Ct., no punitive damages, no prejudgment interest)
- Cap on 3d party damages
- Possible immunity
- Government "endorsement" of security plans and technologies

Cyber insurance

- Reimbursement for damages, but no cap
- No jurisdictional defenses
- No government "sanction" of security plans and technologies
- Less certainty as to coverage
- Tying SAFETY Act to cyber insurance can result in reduced premiums

pillsbury

Brian Finch
Partner / Public Policy
Washington, DC
brian.finch@pillsburylaw.com

Brian Caudill
Sr. Director, Federal Affairs American Gas Association
Washington, DC
bcaudill@aga.org