Breaching Bad: Cyber Security Risks, Regulations & Solutions

Patrick X. Fowler
Snell & Wilmer L.L.P.
One Arizona Center
Phoenix, AZ 85023
602.382.6213
pfowler@swlaw.com

April 22, 2015

SUPPLY CHAIN SECURITY: A MOVING TARGET
Succeeding in the Age of Counterfeits, Cyber Attacks, Seized Shipments & Diminishing Resources

© 2015 Snell & Wilmer

Cyber Security Laws and Regulations

- How we use cyberspace is **still evolving.**
- **New cyber-related technologies** are constantly emerging.
- Cyber Security laws/regulations are **still evolving** too.
- Some laws/regs may **already be obsolete** when enacted.
  - So laws may be written to allow future "flexibility".
- Big policy issues -- Balancing the tension between:
  - **Convenience** and **Security**, and
  - Protecting, but not stifling innovation

© 2015 Snell & Wilmer

The Government's Response to New Problems

© 2015 Snell & Wilmer

The Cyber Threat as Perceived in 2009:

*"It's the great irony of our Information Age – **the very technologies that empower us to create and to build also empower those who would disrupt and destroy**…we've had to learn a whole new vocabulary just to stay ahead of cyber criminals who would do us harm – spyware and malware and spoofing and phishing and botnets."*

-- President Obama, May 29, 2009, discussing his initial "Cyberspace Policy Review"

© 2015 Snell & Wilmer

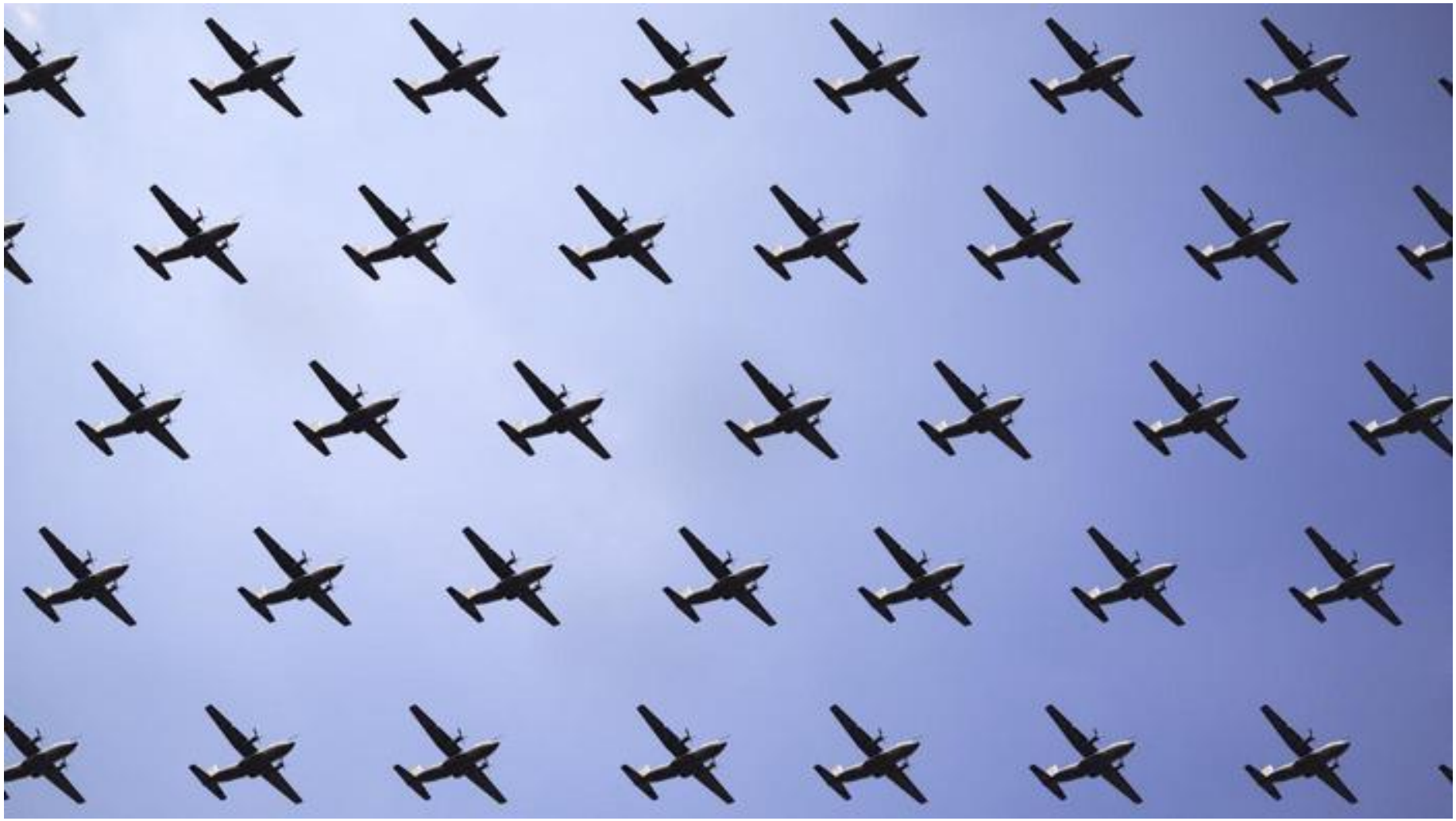
The Cyber Threat as Perceived in 2012:

*"Terrorism remains the FBI's top priority. But in the not too distant future, we anticipate that the **cyber threat** will pose the **number one threat** to our country."*

--F.B.I. Director Robert Mueller
(speaking at the RSA Cyber Security Conference, March 1, 2012)

© 2015 Snell & Wilmer

The Government's Response to Cyber Threats?



© 2015 Snell & Wilmer

Federal Cyber Regulatory Action – Accelerating

- The Executive branch has been accelerating its cyber security regulatory actions. Examples:
  - 2011: SEC issues "Guidance" for public companies regarding disclosure of cyber attacks and cyber-related losses
  - 2014: NIST issues Framework for Improving Critical Infrastructure Cybersecurity
  - 2015: SEC's OCIE Risk Alert, FINRA Cybersecurity Report
  - 2015: EO encouraging "Information Sharing & Analysis Organizations" (ISAO") for private industry and with DHS
  - 2015: EO announcing offensive steps against external malicious cyber threats

© 2015 Snell & Wilmer

Executive Order 13636 of February 12, 2013 - Improving Critical Infrastructure Cybersecurity:

- "The **cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges** we must confront…It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.

© 2015 Snell & Wilmer

Cyber Security – a "High Priority" in 2014

THE FINANCIAL EXPRESS
Read to Lead

Print Close Window

Cyber security on Obama admn's top priority: White House

PTI Posted online: Tuesday, May 20, 2014 at 0000 hrs

Washington : The issue of cyber security is a high priority for the Obama Administration, the White House today said, asserting attacks that badly hit the American national security and economic interests.

"(US) President (Barack) Obama has ... cybersecurity a high priority for his administration. It is specifically the case that the ... counterpart our concern over gove... ...ored cyber-enabled theft of trade secrets and other sensitive business informat... Carney told reporters.

"The issue of **cyber security is a high priority for the Obama Administration**, the White House said today, asserting that it would not tolerate any cyber espionage and other attacks that badly hit the American national security and economic interests."

© 2014 Snell & Wilmer, LLP

Cyber Security – a "National Emergency" in 2015

The White House

Office of the Press Secretary

E-Mail Tweet Share +

For Immediate Release April 01, 2015

Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"

EXECUTIVE ORDER

- - - - - - -

BLOCKING THE PROPERTY OF CERTAIN PERSONS ENGAGING IN

SIGNIFICANT MALICIOUS CYBER-ENABLED ACTIVITIES

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)), and section 301 of title 3, United States Code,

I, BARACK OBAMA, President of the United States of America, find that the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. I hereby declare a national emergency to deal with this threat.

© 2015 Snell & Wilmer

Cyber Security – a "National Emergency" in 2015

- the increasing prevalence and severity of malicious cyber-enabled activities
- originating from, or directed by persons located, in whole or in substantial part, outside the United States
- constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.
- **I hereby declare a national emergency to deal with this threat.**

© 2015 Snell & Wilmer

Contractor-Centric Federal Regulatory Actions

1. NIST's Framework for Improving Critical Infrastructure Cybersecurity (Ver. 1.0, 2014)
2. §941 of the FY 2013 National Defense Authorization Act (NDAA) (rapid reporting for cleared contractors)
3. Department of Defense (DoD) Cyber Rule (UCTI) Nov. 2013 (security and reporting requirements for contractors with UCTI)
4. § 1632 of the FY 2015 NDAA (rapid reporting for "operationally critical contractors")

© 2015 Snell & Wilmer

Contractor-Centric Federal Regulatory Actions

1. NIST's Framework for Improving Critical Infrastructure Cybersecurity (Ver. 1.0, 2014)
2. §941 of the FY 2013 National Defense Authorization Act (NDAA) (rapid reporting for cleared contractors)
3. Department of Defense (DoD) Cyber Rule (UCTI) Nov. 2013 (security and reporting requirements for contractors with UCTI)
4. § 1632 of the FY 2015 NDAA (rapid reporting for "operationally critical contractors")

© 2015 Snell & Wilmer

Framework for Improving Critical Infrastructure Cybersecurity

- Five Core Elements:
  - ***Identify*** potential cyber security risks and how to manage them
  - ***Protect*** the organization's ability to deliver critical services
  - ***Detect*** cyber security events quickly to allow prompt response
  - ***Respond*** to cyber security events in a way to limit their impact
  - ***Recover*** from events and efficiently restore impacted services
- To "be performed concurrently and continuously to form an operational culture that addresses the dynamic cyber security risk."

© 2015 Snell & Wilmer

Framework for Improving Critical Infrastructure Cybersecurity

- NIST encourages organizations to use the Framework as a guide to achieve their own desired outcomes, based on their self-determined "Target Profile".
  - ***"Current Profile"***: Organization's current state of cyber security readiness and outcomes presently achieved.
  - ***"Target Profile"***: Organization's desired but unachieved cyber security outcomes.
- By comparing the two, companies can pinpoint gaps in current cyber security posture and develop an action plan to address them, and reduce overall cyber security risk.

© 2015 Snell & Wilmer

Framework for Improving Critical Infrastructure Cybersecurity

- It's voluntary, but it provides a starting point for federal agencies to impose some basic standards in their contracts.
- November 2013 DoD and GSA Joint Report recommended the creation, where appropriate, of "baseline requirements as a condition of contract award."
  - Elements of the Framework can be used to establish such baseline requirements
  - "Target Profiles" could be included as part of a RFP's "special contracting requirements."
- Could be used as a "standard of care"

© 2015 Snell & Wilmer

Contractor-Centric Federal Regulatory Actions

1. NIST's Framework for Improving Critical Infrastructure Cybersecurity (Ver. 1.0, 2014)
2. §941 of the FY 2013 National Defense Authorization Act (NDAA) (rapid reporting for cleared contractors)
3. Department of Defense (DoD) Cyber Rule (UCTI) Nov. 2013 (security and reporting requirements for contractors with UCTI)
4. § 1632 of the FY 2015 NDAA (rapid reporting for "operationally critical contractors")

© 2015 Snell & Wilmer

§941 of the FY 2013 National Defense Authorization Act (NDAA)

- Calls for **"rapid reporting"** rules for DoD contractors with security clearances who suffer successful penetrations of networks and information systems.
- Also allows DoD personnel access to contractor networks and information to assess the impact of reported penetrations
- NDAA was enacted in January 2013. Directed the DoD to develop rules in 90 days…still waiting)
  - Defense Acquisition Regulation System (DFARS) Case 2013-D018.
  - Draft rule anticipated … soon?

© 2015 Snell & Wilmer

§941 of the FY 2013 National Defense Authorization Act (NDAA)

- Questions for the DoD to address:
  - **What qualifies as a "successful penetration"?**
  - **How "rapid" must the response be? Hours? Days?**
  - **Are such incidents "material events"?**
  - **What if the penetrated network only contained unclassified data?**
  - **What protections will be afforded to contractor trade secrets and sensitive data?**
  - **For how long with DoD be permitted to access contractor networks? Will the contractor still be able to conduct business?**

© 2015 Snell & Wilmer

Contractor-Centric Federal Regulatory Actions

1. NIST's Framework for Improving Critical Infrastructure Cybersecurity (Ver. 1.0, 2014)
2. §941 of the FY 2013 National Defense Authorization Act (NDAA) (rapid reporting for cleared contractors)
3. Department of Defense (DoD) Cyber Rule (UCTI) Nov. 2013 (security and reporting requirements for contractors with UCTI)
4. § 1632 of the FY 2015 NDAA (rapid reporting for "operationally critical contractors")

© 2015 Snell & Wilmer

DFARS Rule on Safeguarding DoD Unclassified Controlled Technical Information (UCTI)

- Nov. 2013: DoD issued final rule. Requires contractors to:
  (1) Provide "adequate security" to safeguard UCTI that is resident on or transiting through the contractor's unclassified information system,
  (2) Timely report (72 hours) to the DoD cyber security incidents and UCTI compromises, and
  (3) Assist the DoD with damage assessments of cyber security incidents.
- This is to be included in all new DoD RFPs and contracts. Presumably applies to all UCTI on contractor's unclassified information systems, not just contract-specific UCTI

© 2015 Snell & Wilmer

DFARS Rule on Safeguarding DoD Unclassified Controlled Technical Information (UCTI)

- **Adequate security** defined as: "protective measures that are commensurate with the consequences and probability of loss, misuse or unauthorized access to, or modification of information."
  - Includes meeting 51 specified security controls from NIST SP 800-53 covering 14 different areas of information security.
- Failure to implement specified controls requires contractor to explain why the control is not required, or propose an alternative control that achieves equivalent protection

© 2015 Snell & Wilmer

DFARS Rule on Safeguarding DoD Unclassified Controlled Technical Information (UCTI)

- **Timely report** cyber incidents to DoD = **within 72 hours.**
- Contractor must assist the DoD in assessing any damage from the cyber incident.
  - Preserve affected information systems for 90 days,
  - Share compromised files with DoD, unless otherwise legally prohibited from doing so.
  - Review their unclassified information systems to identify further evidence of compromise, including specific I.D. of affected UCTI
- Prime contractors must assure that subcontractors also report to DoD all cyber incidents on unclassified systems

© 2015 Snell & Wilmer

Contractor-Centric Federal Regulatory Actions

1. NIST's Framework for Improving Critical Infrastructure Cybersecurity (Ver. 1.0, 2014)
2. §941 of the FY 2013 National Defense Authorization Act (NDAA) (rapid reporting for cleared contractors)
3. Department of Defense (DoD) Cyber Rule (UCTI) Nov. 2013 (security and reporting requirements for contractors with UCTI)
4. § 1632 of the FY 2015 NDAA (rapid reporting for "operationally critical contractors")

© 2015 Snell & Wilmer

§ 1632 of the FY 2015 NDAA

- Cyber incident "rapid reporting" requirements expanded to **"operationally critical contractors"**.
  - Enacted December 2014
- A contractor designated by DoD "as a critical source of supply for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of Armed Forces in a contingency operation."
  - DoD will establish procedures for notifying contractors that have been so designated.

© 2015 Snell & Wilmer

§ 1632 of the FY 2015 NDAA

- "Cyber incidents" include: "actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein."
- The rapid report of each cyber incident will include:
  - **The contractor's assessment of the effect of the cyber incident on the contractor's ability to meet the contractual requirements;**
  - **The technique or method used by the cyber attacker;**
  - **A sample of malware used, if detected and isolated;**
  - **A summary of the information compromised in the cyber incident**
- DoD was directed to establish procedures for contractors to follow to "rapidly report" cyber incidents. Still waiting!

© 2015 Snell & Wilmer

§ 1632 of the FY 2015 NDAA

- § 1632's cyber incident "rapid reporting" requirements build on those in § 941 of FY 2013 NDAA and the DoD's 2013 UCTI cyber rule.
- § 1632 arguably expands the reporting requirements to include cyber incidents on any networks and information systems used by operationally critical contractors ("OCC");
  - Not just those holding UCTI
  - Even if the OCC is not cleared to host or transmit classified info

© 2015 Snell & Wilmer

Questions

© 2015 Snell & Wilmer

Thank you!

Patrick X. Fowler

Snell & Wilmer L.L.P.

One Arizona Center

Phoenix, AZ 85023

602.382.6213

pfowler@swlaw.com

© 2015 Snell & Wilmer