Cybersecurity Executive Order

February 14, 2013

Michael DuBose, Kroll Advisory Solutions
Gerald J. Ferguson, BakerHostetler
Jason Straight, Kroll Advisory Solutions
Theodore J. Kobus III, BakerHostetler
Mike DuBose

Michael DuBose is a Managing Director and Cyber Investigations Practice Leader with Kroll Advisory Solutions. Michael and the Cyber Investigations team provides comprehensive investigative services for digital forensics, data breach response, and complex cybercrimes. Prior to joining Kroll, Michael served as Chief of the Computer Crime and Intellectual Property Section (CCIPS) at the United States Department of Justice (DOJ), where he supervised 40 federal prosecutors and managed some of the largest investigations and prosecutions ever brought in the U.S. involving computer network intrusions, international phishing schemes, botnets, hacktivist groups, copyright piracy, theft of trade secrets, and large-scale data breaches.
Gerald J. Ferguson

Jerry Ferguson serves as the Coordinator for the Intellectual Property, Technology and Media Group in BakerHostetler’s New York office and as the National Co-Leader of BakerHostetler’s Privacy and Data Protection Team.

Jerry has assisted clients in creating and implementing national and global privacy policies for more than a decade. He has extensive experience advising companies suffering data security breaches that may trigger obligations under state and federal breach notification laws. He can quickly and efficiently advise clients regarding notification obligations because of his extensive experience with (i) the 46 state breach notification laws; (ii) the breach notification provisions in federal laws, such as Gramm-Leach-Bliley and HIPAA; and (iii) industry self-regulation, such as the Payment Card Industry rules.
Jason Straight

Jason Straight is a managing director at Kroll Advisory Solutions in New York. In this role, Jason provides expert guidance to attorneys, IT professionals, information security directors, compliance officers and risk management personnel, among others, in the areas of data breach response, cyber investigations, computer forensics and data privacy protection. Jason joined Kroll in 2002 and has served in numerous positions since then as part of Kroll’s broad technology practice. As a member of Kroll’s Cyber Investigations practice, Jason has overseen dozens of complex engagements concerning network intrusion incidents, lost mobile devices, intellectual property theft, compromise or exposure of sensitive customer or employee data. Before joining Kroll, Jason was an associate in the NY offices of Fried Frank Harris Shriver and Jacobson.
Ted Kobus is National Co-Leader of the Privacy and Data Protection Team.

Ted advises clients, trade groups and organizations regarding data security and privacy risk management, breaches, response strategies, litigation and regulatory actions affecting organizations. He has counseled clients involved in over 400 breaches, including significant breaches implicating state and federal laws, international laws and other regulations and requirements: HITECH, the Massachusetts Data Privacy Law, California privacy laws (including the California Department of Public Health Law), Connecticut Insurance Department regulations, Puerto Rico’s Citizen Information on Data Banks Security Act, Mexico’s Data Protection Law, Canada’s data privacy requirements and PCI/CISP requirements. He has dealt with Offices of Attorneys General, state insurance departments, Office of Civil Rights (OCR)/Health and Human Services (HHS), Secret Service, FBI and local police and forensics professionals as part of their handling of data breaches.
Agenda

- Introduction
- Threat environment driving administration’s action
- Key provisions of the order
- Standard setting process and associated challenges
- Anticipated regulatory response
- Conclusion/Take-Aways
- Questions
THREAT LANDSCAPE
The Policy Behind the Order

- Section 1 of the Executive Order States the Policy Behind the Order:

  “Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront.”
Rapidly Evolving Risk Landscape Threatening Critical Infrastructure to Unprecedented Extent

MALICIOUS INSIDERS
Disgruntled current and former employees, state-sponsored moles
Driven by opportunism, greed, desire for revenge
Cause 2/3 of all IP cyber IP theft

STATE-SPONSORED HACKING
Economic espionage on rise; steal R&D, trade secrets worth billions; destroy Data, disrupt critical infrastructure.
Increased use of APTs
Hit & Run v. Park and Stay
Anti-virus software ineffective

HACKTIVISM
21st Century civil disobedience;
DDOS and theft
Anonymous, LulzSec goups
Political/public interest causes
Increased used by religious extremist groups (e.g. Middle East)

NEGLIGENT INSIDERS
Unwary insiders susceptible to being fooled into downloading malware (e.g. spear phishing); infected thumb drives;
Failure to embrace “culture of security”

CRIMINAL HACKERS
Opportunists stealing anything of vale – PII, PHI, credit card, bank acct. and passwords.
Growing underground Black Market for exploits/malware; hackers for hire; “HaaS”
Botnets have vastly increased scale and reach of organized crime groups
Threats Driving the Executive Order

- **State-Sponsored Attacks**
  - Cyber “Pearl Harbor”
  - Economic Espionage
  - Data Destruction
  - Terrorism: Al Qaeda and other grps using cyber warfare tools

- **Increasingly Harmful and Unpredictable Hacktivism**
  - Publishing terabytes of classified USG data; DDoS attacks against US banks and other critical infrastructure
  - Religious and political extremist groups

- **Malicious Insiders**
  - Sending R&D, trade secrets to China and other rivals
  - Jeopardizing US competitiveness, strength of economic infrastructure
Other Drivers of Executive Order

- **Need for Consistently High Cybersecurity Standards for Critical Infrastructure**
  - Diverse array of regulated industries following different standards
- **Reluctance of Private Sector to Share Cyber Intelligence with USG**
  - Risk of disruptive law enforcement action or potential third-party liability
- **Inability of Congress to Act**
- **US Engaging in “Pre-emptive” Cyber Warfare**
  - Elevated risk of retaliatory action against critical infrastructure targets
Context of the Order

Congress Has Failed to Enact National Cybersecurity Law

– Federal Security Standards Concerns
– Information Sharing Concerns

• Republicans: Liability Limitation
• Democrats: Civil Liberty Concerns
Characteristics of the Order

Vague
  – Material Terms not defined or discussed
  – Intentionally vague?

Specific Action Deferred
  – Review, Comment, Report
What is Critical Infrastructure?

Defined Broadly and Generally (Section 2)

• Secretary of Homeland Security Will Identify Key Threats (Section 9)
  – Communications, Manufacturing, Energy, Food and Agriculture, Financial, Healthcare Transportation, Shipping
  – Critical Infrastructure Partnership Advisory Council
Does the Order Impose Security Standards

No, maybe, or not yet

• "Cybersecurity Framework" (Section 7)
  – incorporates voluntary consensus standards, industry best practices
  – consistent with international standards and NIST

• NIST reviews and reports
  – Issues Preliminary Framework in 240 Days
  – Issues Final Framework with 1 Year
Does the Order Require Information Sharing?

By the Government: YES (Section 4)

By industry: No, maybe, not yet

- No express discussion of industry providing information to government
- “Consultative Process”
- Seconding industry experts to government
- Provisions protecting industry information
- Presidential Policy Directive 21
Do I have to participate?

No, maybe, not yet

Issues for review and report:

– Preferential treatment for contractors who participate
– Other incentives to participate
How am I protected if I voluntarily cooperate?

No protection from liability
  – Requires legislation

Disclosure subject to FOIA requests
  – Better protection requires legislation

Claims of privacy violations from customers and employees
  – Issue subject to review and reporting
Standard Setting Process
Developing the Cybersecurity Framework

- NIST given 240 days (mid-October) to publish a “preliminary version” of the Cybersecurity Framework. The final Framework must be complete by mid-February, 2014

“The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess and manage cyber risk.”
Framework Development

- Cybersecurity Framework defined as “set of voluntary standards and best practices to guide industry in cyber risks.”
- Order directs NIST to “engage in open public review and comment process” in developing the Framework involving all stakeholders in public and private sectors.
- Patrick Gallagher, NIST Director:

  “Framework will not be a NIST work product; it will be developed by and belong to private industry.”
Framework Development

- NIST to issue RFI to critical infrastructure owners and operators requesting that they share details around:
  - Current risk management practices
  - Use of frameworks, standards, guidelines and best practices
  - Use of “core practices” NIST views as universally applicable such as:
    - Encryption and key management
    - Asset identification and management
    - Security engineering practices

- Will conduct series of sector-focused workshops over next several months to gather additional input
Framework Development

- **NIST Standard Development Process**
  - Extensive risk assessment process to establish requirements for framework
  - Likely to take “defense in depth” layered approach
  - Unique challenges due to diverse security profiles and business needs across “critical infrastructure” sectors

- **Existing NIST Standards Likely to Form Foundation**
  - Smart Grid
  - Identity Management
  - FISMA
  - Electricity Subsector Cybersecurity Capability Maturity Model
  - 800-53 -- Recommended Security Controls for Federal Information Systems and Organizations
What you can do to prepare

- Review NIST RFP, begin formulating responses
- Assess current compliance with existing standards referred to in RFI
- Identify concerns/challenges specific to your business or sector in complying
- Consider participating in or attending NIST workshops
- Identify specific concerns around information sharing
Regulatory Impact

- Risk
- Compliance
- Challenges
Risks

- Inconsistent with SEC disclosures
- Public disclosure (competitors, criminals, hacktivists)
- Enhanced regulatory scrutiny
- Loss of preferred status
Compliance Concerns

• Will information be shared with other regulatory agencies?
• EU initiatives
• Policies, procedures and practices reflective of cybersecurity’s broad scope
Challenges

• IS/IT escalating issues to the C-Suite
• Broaden focus from security of personal information to threats that impact the critical infrastructure
• Protecting the disclosure of employee and consumer personal information (over disclosing)
To Do List

• Update policies & procedures
• Education
• Vendor lists and contracts
• Security audit
• Regulatory strategy
Q&A
Gerald J. Ferguson
Partner
Intellectual Property, Privacy and Data Protection
gferguson@bakerlaw.com
212.589.4238

Theodore J. Kobus III
Partner
Intellectual Property, Privacy and Data Protection
tkobus@bakerlaw.com
212.271.1504
Contact Information

Michael DuBose  
Managing Director,  
Cyber Investigations Practice Leader  
mdubose@kroll.com  
(o) 202.833.6860  
(m) 202.329.6839

Jason Straight  
Managing Director,  
Cyber Investigations/Information Security  
jstraight@kroll.com  
(o) 212.833.3208  
(m) 917.374.3270