

Cyber-security policy and procurement trends

Douglas Farry

Managing Director

McKenna Long & Aldridge, LLP

dfarry@mckennalong.com

- Clinton Administration
 - VP Gore's Reinventing Government initiative
 - Goal: Better govt performance through IT
 - Introduced performance measures
 - Included the concepts of interoperability, uniform standards, and integration of data security strategies
 - Not widely adopted

- Bush Administration
 - Response to the September 11, 2001 attacks
 - Examination of IT infrastructure vulnerabilities and limitations
 - Creation of DHS exposed the fragmented fashion in which federal IT infrastructure had been organized and developed
- The interdependence of federal govt. IT and private sector systems has been accelerated
- Increased reliance by the federal government on private sector contractors has increased the need for interoperability
- Increased interdependency has highlighted the vulnerabilities in the government-to-contractor interfaces

Vulnerabilities Exposed

- High-profile security breaches growing:
 - Veterans Affairs
 - Transportation Security Administration
 - Centers for Medicare and Medicaid Services
 - Department of State
 - Department of Commerce's Bureau of Industry and Security

Federal Computer Security Report Card - May 2008

GOVERNMENTWIDE GRADE 2007: C (2006: C-)					
	2007	2006		2007	2006
DEPARTMENT OF JUSTICE	A+	A-	NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	C	D-
AGENCY FOR INTERNATIONAL DEVELOPMENT	A+*	A+	DEPARTMENT OF STATE	C*	F
ENVIRONMENTAL PROTECTION AGENCY	A+	A-	DEPARTMENT OF EDUCATION	C-	F
NATIONAL SCIENCE FOUNDATION	A+*	A+	DEPARTMENT OF COMMERCE	D+	F
SOCIAL SECURITY ADMINISTRATION	A+*	A	DEPARTMENT OF TRANSPORTATION	D	B
HOUSING AND URBAN DEVELOPMENT	A	A+	DEPARTMENT OF LABOR	D	B-
OFFICE OF PERSONNEL MANAGEMENT	A-	A+	DEPARTMENT OF DEFENSE	D-	F
GENERAL SERVICES ADMINISTRATION	B+	A	DEPARTMENT OF THE INTERIOR	F	F
DEPARTMENT OF ENERGY	B+	C-	DEPARTMENT OF TREASURY	F	F
DEPARTMENT OF HOMELAND SECURITY	B+	D	NUCLEAR REGULATORY COMMISSION	F	F
DEPARTMENT OF HEALTH AND HUMAN SERVICES	B	B	DEPARTMENT OF VETERANS AFFAIRS	F	N/A
SMALL BUSINESS ADMINISTRATION	B	B+	DEPARTMENT OF AGRICULTURE	F	F

*Based on Financial Statement reporting and audit results showing "no significant deficiencies" we have confidence these grades accurately reflect agencies' ability to secure data. All other agencies showed "material weakness" or "significant deficiency," which made it more difficult to use FISMA criteria alone to evaluate an agency's information security posture.

**Scoring of DOL, DOT, SSA, GSA, DHS, SBA, NASA, DOS, DOE, DOC, and DOD, was updated in consultation with GAO and some agencies to reflect adjusted methodology.

Prepared by Ranking Member Tom Davis, House Oversight and Government Reform Committee, based on reports required by the Federal Information Security Management Act of 2002.

- FISMA
 - First serious Congressional response
 - FISMA mandated that federal agencies implement information security programs to protect agency information and systems
 - Slow and inconsistent implementation
 - Congress in the process of reauthorizing

- President initiated 60-day Cybersecurity Policy review on first day
- Obama's goals and priorities:
 - Strengthen Federal Leadership on Cyber Security
 - Initiate a Safe Computing R&D Effort and Harden our Nation's Cyber Infrastructure
 - Protect the IT Infrastructure That Keeps America's Economy Safe
 - Prevent Corporate Cyber-Espionage
 - Develop a Cyber Crime Strategy to Minimize the Opportunities for Criminal Profit
 - Mandate Standards for Securing Personal Data and Require Companies to Disclose Personal Information Data Breaches

S 773 - Introduced by Senators Rockefeller (D-WV) and Snow (R-ME)

- NIST to establish standards the procurement of civilian government IT
- NIST to establish standards for all **government contractor**, or grantee critical infrastructure information systems and networks.
Goal: consistency with more stringent requirements at DoD
- Money for Regional Cybersecurity Centers for small business
- Creates incentives and **liabilities** for IT companies to ensure the cyber security of their products for key “Critical infrastructure”
- New “Secure Products and Services Acquisitions Board” for software and hardware purchased for federal government use

- Introduced April 2009
- Passed Committee with a substitute amendment in March 2010
- Senate Homeland Security Chairman Lieberman working on a separate bill
 - DHS, not a White House czar, primary authority to protect federal civilian and private computer networks.

Comprehensive National Cyber Security Initiative (CNCI)

- Signed by Bush in January 2008
- Spells out which executive branch organization is responsible for what
- DOD and the Office of the Director of National Intelligence are designated executive agents for the effort
- A dozen components designed to:
 - Better protect computer networks and systems
 - Improve information technology processes and policies
- Details of the program remains classified
- The Trusted Internet Connections (TIC)
 - Most established piece of the initiative
 - Based on the idea that the fewer connections agencies have, the easier it will be to monitor them and detect security incidents
- Total estimated cost to implement - \$40 billion

Trends in Cybersecurity at the Department of Defense

Perceived Threat: Security of commercial products

- Dubious pedigree for the origin, development, production and involvement of personnel from outside the United States
- Chief concern is creation of “portals” within the supply chain

Response:

- Identify “tiers” of criticality; assign a level of required assurance for each “tier”; place all DOD missions into a “tier”.
- Likely that DOD’s tendency will be to overprotect
- IT acquisitions are more likely to be classified, and classified at a higher level, with a greater information assurance requirement
- Likely to be an ancillary spillover effect for IT consulting and management services

Defense Industrial Base (DIB) Initiative

Background:

- Theft of classified information on the Joint Strike Fighter
- Mined unclassified data from prime's commercial IT network

Response: DIB to force prime contractors to secure their corporate networks

- Potentially significant implications:
 - Teaming with or entering into prime-subcontractor relationships with major defense companies involved in classified programs is likely to become more difficult
 - Opportunities fewer in the absence of a facility clearance

NSPD 54/HSPD 23

- Both directives are classified but generally spell out which executive branch organization is responsible for what
- Goal is to take cybersecurity, information assurance, and other IT-related initiatives at DOD and to expand to other executive branch departments and agencies
- DOD and the Office of the Director of National Intelligence have been designated executive agents for this effort
- New IT requirements are likely to be imposed through new DFAR clauses
- Compliance with ISO standard 15026 and the Engineering for Software Assurance Guidebook

Conclusions

- There is a paradigm shift federal government laws and regulations on IT products and services impacting the entire sector.
- The immediate impact will be on Federal procurement decisions,
- The intent, trend, and direction will be to have those requirements, standards, and procedures apply to private sector sales as well
- “Critical infrastructure” most impacted:
 - Telecommunications companies
 - Financial institutions
 - State and local governments