BNA, INC.

FEDERAL CONTRACTS

BNA Employee-Owned Since 1947

REPORT

Information Technology

With the federal government increasingly turning to contractors to maintain and manage vast stores of data, contractors face both opportunities and risks. This analysis reviews the information security rules that govern agencies and contractors, and the possible consequences—including congressional scrutiny, contract remedies, and third-party litigation—that can result from their breach.

When Cyber Barbarians Storm the Security Walls: The Mounting Risks of Security Breaches to Federal Agencies & Contractors

BY DAVID Z. BODENHEIMER *

** Mr. Bodenheimer is a partner in the law firm of Crowell & Moring LLP in Washington, D.C., where he specializes in government contracts, homeland security, and privacy. He handles litigation, advises clients, and writes and lectures on a variety of high-technology matters, including privacy and IT security, SAFETY Act coverage, and homeland security technology. He may be reached at (202) 624-2713 or dbodenheimer@crowell.com.*

While 2005 ended as the "Worst Year for Breaches of Computer Security"[1] for corporations and universities, 2006 will be remembered as the year that information security breaches shattered the cyber walls of federal agencies, leaving millions of privacy casualties in their wake. No breach has dominated the headlines like the single lost Department of Veterans Affairs (VA) laptop that jeopardized the privacy of 26.5 million veterans, spawned numerous congressional hearings and bills, and ignited class action suits.

[1] "2005 Worst Year for Breaches of Computer Security," *USA Today* (Dec. 29, 2005).

Unfortunately, the VA does not stand alone, as hordes of privacy breaches have ripped through the federal government, exposing cracks in the information security walls of federal agencies – even those agencies responsible for enforcing privacy rules and guarding the most sensitive personal data.

> ''FTC Reports Laptop is Stolen in the Latest U.S. Data Breach'' *Wall Street Journal* (June 23, 2006)
>
> ''Consultant Breached FBI's Computers,'' *Washington Post* (July 6, 2006)
>
> ''Navy Probes Data Leak on 100,000 Sailors, Marines'' *Reuters*, (July 7, 2006)

With privacy under siege, both Congress and the executive branch have mobilized forces to shore up security defenses, allocating more money to information technology (IT) security, imposing tougher rules for preventing and reporting security breaches, and investigating and punishing those who fail. For federal contractors, this IT security mobilization means big opportunities – and equally big risks. For contractors that can deliver and maintain effective IT security, the federal marketplace is begging for bigger and better defenses against the swelling threat of hackers, identity thieves, and other cyber thugs. For federal contractors that fail to keep their IT security promises, the risks are daunting – congressional investigations, downgraded past performance evaluations, public and private litigation, and contract disputes over privacy and information security requirements.

This analysis discusses the information security rules and risks applicable to federal agencies and contractors, as well as the new initiatives and trends that raise the stakes for security breaches that compromise the privacy of individuals or jeopardize the security of sensitive federal information.

I. Federal Agencies Under Cyber Siege

Why sack the federal data banks? To paraphrase Willie Horton, ''Because that is where the information is.''[2] With its unparalleled treasure trove of information, the federal government is a plump target for anyone looking to pillage data. In recent months, the widely-reported assaults have been both relentless and alarming, exposing the need to reinforce the walls before the next wave of attacks by cyber terrorists and roguenation spies and saboteurs. As a result, the executive branch has marshaled the troops with new directives for information security for federal agencies – but questions remain about whether the new defenses will arrive in sufficient time and force.

A. The Federal Information Kingdom

In the information kingdom, nobody is bigger than the federal government. In the latest E-Government report to Congress, the Office of Management and Budget (OMB) stated: ''The Federal government is the largest single producer, collector, consumer, and disseminator of information in the United States and perhaps the world.''[3] To manage this vast estate, the federal government wields a substantial IT budget of $64 billion, up from $28 billion in 1996.[4]

The federal information treasure chest contains a wealth of data that the government cannot afford to lose – including information on critical infrastructure vulnerabilities, personal information (ranging from Social Security numbers (SSNs) to VA health records to passenger lists), and industry trade secrets. Even excluding classified data, the potential impacts of unauthorized modification, destruction, or disclosure of ''sensitive'' data are disquieting – including ''loss of life; loss of property or funds by unlawful means; violation of personal privacy or civil rights; gaining of an unfair commercial advantage; loss of advanced technology, useful to a competitor; or disclosure of proprietary information entrusted to the Government.''[5] To protect these information treasures, the federal government is projected to increase its spending on IT security by over 18 percent in the next five years, from $5.1 billion in fiscal year (FY) 2006 to $6.3 billion in FY 2011.[6]

B. Guardians of the Information Realm

The federal information kingdom has many defenders, but no clear king. For federal information and IT systems, the OMB director ''shall oversee agency information security policies and practices,'' yet this authority does not extend to ''national security systems'' under the authority of the Department of Defense (DOD) and the Central Intelligence Agency (CIA).[7] For purposes of protecting critical infrastructure against terrorist attacks, the Department of Homeland Security (DHS) Secretary ''will maintain an organization to serve as a focal point for the security of cyberspace,'' which certainly includes federal IT resources.[8] However, DHS has yet to consolidate its power as the cyber ''focal point'' due, at least in part, to delays in finding a cyber czar to serve as the assistant secretary for cybersecurity.[9]

All federal agencies bear responsibilities for safeguarding sensitive information. The source of the duty (and the consequences of failure) may vary, depending upon the nature of the information to be protected.

---

[2] When asked ''Willie, why do you rob banks,'' Willie Horton purportedly said ''Cause that's where the money is.'' (http://en.wikiquote.org/wiki/Organized_crime).

[3] OMB, *FY 2005 Report to Congress on Implementation of the E-Government Act of 2002* at 5 (Mar. 1, 2006) (http://www.whitehouse.gov/omb/inforeg/reports/2005_e-gov_report.pdf) .

[4] Executive Office of the President, *Fiscal Year 2007 Information Technology Budget* at 5 (Mar. 3, 2006) (http://www.whitehouse.gov/omb/egov/g-9-budget_highglights.html); Andrues, ''The Clinger-Cohen Act, 10 Years Later: The Five Percent Solution,'' *GovExec.com* (July 11, 2006); Miller, ''OMB crunches numbers, revises 2007 IT budget forecast,'' *Washington Technology* (Mar. 6, 2006).

[5] 70 Fed. Reg. 57452 (Sept. 30, 2005).

[6] INPUT Press Release, ''INPUT Forecasts Federal IT Security Spending to Reach $6.3 Billion'' (July 12, 2006) (http://www.input.com/corp/press/detail.cfm?news=1254).

[7] 44 U.S.C. § 3543(a), (b).

[8] Homeland Security Presidential Directive (HSPD) 7 (Dec. 7, 2003).

[9] On September 18, 2006, Secretary Chertoff announced the appointment of Greg Garcia to serve in this position. Aplin, ''Chertoff Appoints ITAA's Greg Garcia as DHS Cybersecurity Assistant Secretary,'' *BNA Privacy Law Watch* (Sept. 20, 2006). However, the delays in filling the position raised questions and generated criticism. Krebs, ''A Year Later, Cybersecurity Post Still Vacant,'' *Washington Post* p. A21 (July 13, 2006); ''Democratic Senators, Industry Coalitions Urge DHS to Fill Still Vacant Cyber-Chief Slot,'' *BNA Privacy Law Watch* (July 14, 2006).

  FCR ISSN 0014-9063

Three of the primary obligations flow from the Federal Information Security Management Act (FISMA), the Trade Secrets Act, and the Privacy Act.

1. FISMA

FISMA holds the head of each agency responsible for ''providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of'' agency information.[10] The Act requires the agency heads to ''assess the risk and magnitude'' of potential harms, to implement ''policies and procedures to cost-effectively reduce risks,'' and to ensure periodic ''testing and evaluating'' of ''information security controls.''[11] While FISMA does not punish transgressions with criminal or civil sanctions, it comes with other sharp teeth, including congressional reporting of ''significant deficiencies in agency information security practices'' that may provoke Congress or OMB to take a bite out of the agency's annual IT budget.[12] Within the executive branch, bad IT security may earn an agency a bad report card that OMB sends to the President, as information security is now one of the ''critical components'' for rating agency performance each year.[13] In some circumstances, poor FISMA compliance has become a central issue in litigation over an agency's IT security practices. *See, e.g., Cobell v. Kempthorne,* 455 F.3d 301 (D.C. Cir. 2006) (recounting the saga of relentless litigation over the Interior Department's information security systems for the Indian trust funds). Thus, agencies with failing IT security scores may pay dearly during congressional budget raids, judicial battles, and interagency duals for IT funding.

2. Trade Secrets Act

Behind its information security walls, the federal government holds some of the most precious trade secrets in the world – formulas for blockbuster drugs and pesticides, technical details of anti-terrorism technology, and cost information for multi-billion-dollar acquisitions. Congress has made it a crime for federal officials or employees to divulge trade secrets.[14] While the risk of criminal sanctions under the Trade Secrets Act may be remote, federal agencies have ample reason to be concerned about security breaches not only for fear of being the seminal criminal prosecution under its authority, but also for the threat of officials being ''removed from office or employment.''[15] Aside from the express sanctions under the statute, an improper disclosure of a company's trade secrets may also support an action for damages or injunctive relief.[16]

3. Privacy Act

The Privacy Act establishes a broad rule against disclosure of private information from federal ''systems of records'' in the absence of the individual's consent.[17] While the statute has a number of exceptions and exclusions, they do not extend so far as to excuse the types of security breaches that have recently dominated the headlines. For violations, the Privacy Act offers a broad spectrum of remedies, including criminal, civil, and administrative sanctions.[18] In one of the more heavily publicized Privacy Act cases, Linda Tripp recovered $595,000 from DOD for an unauthorized release of her personal information.

C. Cracks in the Security Walls

The cyber barbarians have long been pounding the security gates of federal agencies, occasionally penetrating the perimeter and reminding everyone of the fragility of the defenses. In November 2002, a British computer administrator hacked into 92 U.S. computer networks (including the Pentagon and National Aeronautics and Space Administration (NASA) networks), using his home computer and automated software available on the Internet to scan tens of thousands of computers on U.S. military networks.[19] More recently, OMB's FISMA report to Congress for FY 2005 acknowledged 3,569 security ''incidents'' involving federal agencies, including 1,806 reports of ''malicious code'' and 304 ''unauthorized access'' penetrations.[20]

For federal agencies, 2006 will go down as the ''Year of Information Insecurity,'' as cyber defenses have bent and cracked under the strain of relentless assaults. Hardly any major federal agency remains unwounded, as federal information continues to bleed into the wrong hands.[21] A sampling of the news coverage on security breaches highlights the unsettling exposure to cyber assaults.

> *State Department*: ''Hackers in China broke into the State Department's computer system in Washington and overseas in search of information, passwords, and other data'' (June 2006).[22]
>
> *FTC*: ''The Federal Trade Commission, the primary regulator enforcing privacy laws, said a laptop containing sensitive consumer data was stolen, adding to a string of disclosures that has exposed lax security practices in the government'' (June 2006).[23]
>
> *DOD Tricare*: For attendees at a Tricare Management Activity conference on health-care fraud, the ''Pentagon has sent warning letters to thousands of people who may have had their personal data stolen,

[10] 44 U.S.C. § 3544(a)(1)(A).
[11] *Id.* at § 3544(a)(2).
[12] *Id.* at 3543(a)(8).
[13] OMB, *FY 2005 Report to Congress on Implementation of the Federal Information Security Management Act of 2002* at 11-12 (Mar. 1, 2006) (hereinafter OMB FY 2005 FISMA Report) (http://www.whitehouse.gov/omb/inforeg/reports/2005_fisma_report_to_congress.pdf).
[14] 18 U.S.C. § 1905 (fine or imprisonment for up to one year).
[15] *Id.*
[16] *Ruckelshaus v. Monsanto,* 467 U.S. 986 (1984) (damages); *Megapulase, Inc. v. Lewis,* 672 F.2d 959 (D.C. Cir. 1982) (injunctive relief).
[17] 5 U.S.C. § 552a(b).
[18] 5 U.S.C. § 552a(i) (criminal misdemeanor with fine up to $5,000 for ''willful'' violations); *id.* § 552a(g) (civil remedies of injunctive relief, attorney fees, correction of records, and/or damages).
[19] General Accounting Office (GAO, now the Government Accountability Office), *Information Security: Further Efforts Needed to Fully Implement Statutory Requirements in DOD* at 10 (July 24, 2003) (GAO-03-1037T) (www.gao.gov).
[20] OMB FY 2005 FISMA Report at 9.
[21] Goldfarb, ''To Agency Insiders, Cyber Thefts and Slow Response Are No Surprise,'' *Washington Post* at A17 (July 18, 2006).
[22] Wright, ''State Dept. Probes Computer Attacks,'' *Washington Post* at A6 (July 7, 2006).
[23] Conkey, ''FTC Reports Laptop is Stolen in the Latest U.S. Data Breach,'' *Wall Street Journal* at B2 (June 23, 2006).

advising them that they may be at risk of identify theft and other fraudulent activities'' (May 2006).[24]

Energy Department: ''A hacker stole a file containing the names and Social Security numbers of 1,500 people working for the Energy Department's nuclear weapons program'' (May 2006).[25]

FBI: ''A government consultant, using computer programs easily found on the Internet, managed to crack the FBI's classified computer system and gain the passwords of 38,000 employees, including that of FBI Director Robert S. Mueller III'' (July 2006).[26]

Transportation Department: ''The Department of Transportation's Office [of] Inspector General Aug. 9 reported the July 27 theft of one of its laptop computers [that] contained the unencrypted personally identifiable information of about 132 Florida residents who have been issued commercial driver's licenses, individual driver's licenses, or pilot licenses'' (August 2006).[27]

Navy Department: ''Personal records for every Navy and Marine Corps aviator or aircrew member who has logged flight hours in the past 20 years have been posted on a public Navy Web site for the past six months, compromising more than 100,000 Social Security numbers'' (July 2006).[28]

Agriculture Department: ''A laptop computer bag was stolen from an Agriculture Department worker's car in Kansas, and the names, addresses and Social Security numbers of about 350 employees may have been accessed . . . . In June, the USDA said 26,000 Washington-area employees may have been affected when a computer hacker broke into the department's system'' (July 2006).[29]

The most infamous security breach of 2006 – the lost VA laptop compromising the privacy of 26.5 million veterans – dominated the headlines,[30] provoked congressional hearings and legislation,[31] ignited a scathing VA Inspector General report,[32] triggered several class action suits, and cost key VA officials their jobs.[33] In testimony before the House Committee on Veterans Affairs, VA Secretary R. James Nicholson said he is ''mad as hell'' about the data breach.[34] And this is a case in which the agency recovered the laptop without the personal data having been actually accessed. In short, any federal agency official who is still slipping information security back to the bottom of the priority pile after the VA debacle is a glutton for congressional roasting, battered public trust, corrosive lawsuits, and short tenure as a public servant.

Even as these security breaches mount, federal agencies remain precariously vulnerable to attack. After receiving an overall grade of ''D+'' on the FISMA report card for information security for FY 2004, federal agencies underperformed yet again for FY 2005:

> This year, the federal government as a whole hardly improved, receiving a D+ yet again. Our analysis reveals that the scores for the Departments of Defense, Homeland Security, Justice, State – the agencies on the front line in the war on terror –remained unacceptably low or dropped precipitously.''[35]

As terrorists and rogue nations turn increasingly to cyber assaults and ''hackers for hire'' to do their dirty work, these vulnerabilities will be further exposed and exploited. As the National Research Council stated, ''Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb.''[36] Indeed, terrorists are becoming more structured to take advantage of 'hackers for hire' '' and ''terrorist leaders can move quickly and virtually through cyberspace to strike at the very heart of the Western economic infrastructure.''[37] For terrorists, the end game for breaching our information security walls is a ''cyber-Katrina'' or ''digital Pearl Harbor,'' with equally devastating consequences.[38] Given the options, the cyber defenses simply must be hardened.

D. Shoring Up the Defenses

After the rash of security breaches and ensuing investigations, federal agencies have received new directives for shoring up the security bastions. Stressing that ''Strict adherence to safeguard standards is critical to protecting sensitive data,'' OMB Deputy Director Clay Johnson in June issued a checklist requiring federal agencies to: (1) encrypt all data on mobile computers and devices; (2) allow remote access only with two-factor authentication; (3) use an automatic ''time-out''

---

[24] Barr, ''Conference Attendees' Personal Data May Be at Risk,'' *Washington Post* at D4 (May 10, 2006).

[25] ''Hacker Steals Personal Info on 1,500 Employees From DOE Nuclear Agency,'' *CBS News* (June 9, 2006) (www.cbsnews.com).

[26] Weiss, ''Consultant Breached FBI's Computers,'' *Washington Post* at A5 (July 6, 2006).

[27] ''DOT's Inspector General Reports Theft of IG Laptop Containing Data on 132,000,'' BNA Privacy Law Watch (Aug. 10, 2006); *see also* Lee and Wilber, ''Computer Theft Puts Floridians at Risk,'' *Washington Post* at A6 (Aug. 10, 2006).

[28] White, ''Personal Data Were Posted on Navy Web Site,'' *Washington Post* at A3 (July 8, 2006).

[29] AP, ''USDA employee data may have been lifted,'' *Star-Telegram.com* (July 19, 2006) (http://www.dfw.com/mld/dfw/news/nation/15072205.htm).

[30] Stout & Zeller, ''Vast Data Cache About Veterans Is Stolen,'' *New York Times* (May 23, 2006).

[31] Senate Committee on Veterans' Affairs hearings, ''VA Data Privacy Breach: Twenty-Six Million People Deserve Assurance of Future Security,'' *Congressional Record Online via GPO Access* at D804-5 (July 19, 2006); H.R. 5835, 109th Cong. (2006) ''Veterans Identity and Credit Security Act of 2006.''

[32] VA Office of Inspector General (OIG), ''Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans'' Report No. 06-02238-163 (July 11, 2006) (http://www.va.gov/oig/51/FY2006rpts/VAOIG-06-02238-163.pdf).

[33] Lee, ''Top VA Officials Criticized in Data Theft,'' *Washington Post* at A13 (July 12, 2006).

[34] *Id.*

[35] Rep. Davis, ''No Computer System Left Behind: A Review of the 2005 Federal Computer Security Scorecards,'' House Comm. on Government Reform (Mar. 16, 2006) (http://reform.house.gov/UploadedFiles/TMD%20FISMA%2006%20Opener.pdf).

[36] House Subcomm. on Cybersecurity, Science, and Research & Development, ''Cybersecurity for the Homeland'' at 10 (Dec. 2004).

[37] *Id.*

[38] *Cybersecurity: U.S. Vulnerability and Preparedness: Hearings Before the House Comm. on Science,* 109th Cong. (Sept. 15, 2005); Rep. Davis, House Comm. on Government Reform, ''Is the Government Ready for a Digital Pearl Harbor?'' (Mar. 14, 2006) (http://reform.house.gov/UploadedFiles/031606FISMA.Hearing.pdf); Lipowicz, ''Study: U.S. not ready by 'cyber-Katrina,'' *Washington Technology* (June 26, 2006).

  FCR ISSN 0014-9063

function for remote access after a 30-minute inactivity period; and (4) keep a log of all computer-readable data extracts from databases.[39] Perhaps of greater significance, the OMB memo establishes certain security assessment methods and procedures outlined by the National Institute of Standards and Technology (NIST) as ''mandatory.''[40] For future litigation arising out of security breaches, these very detailed NIST rules may well define the standard of care and due diligence owed to companies and individuals who have entrusted their precious information assets to federal agencies.

The recent round of reported security breaches has highlighted another problem – a tendency for agency foot-dragging in disclosing such ''incidents.'' To remedy this shortcoming, OMB now requires all agencies to ''report *all* incidents involving personally identifiable information'' to the Federal incident response center ''*within one hour*'' without making any distinction between ''suspected and confirmed breaches.''[41] In the short-run, this directive may elevate the number of security breaches reported. However, it should also boost agency incentives to avoid bad publicity by implementing and enforcing tougher controls to protect sensitive information.

III. Federal Contractors on the Front Lines

To date, the hammer blows of security breaches have fallen largely upon federal agencies, rather than government contractors. However, outsourcing trends guarantee that government contractors will handle ever-expanding shares of the federal information storehouses. As a result, contractors will increasingly serve on the front lines, shielding federal data from the cyber hordes and bearing the blame for any failures resulting in security breaches.

A. Trends Expanding the Cybersecurity Roles of Contractors

As federal agencies battle against the continuing crush of security breaches, government contractors will find themselves shouldering an ever-growing load of the federal responsibility for information security. Three primary trends will swell the ranks of contractor cyber warriors: (1) increased federal outsourcing; (2) heightened security requirements for contractors; and (3) greater scrutiny of contractors' adherence to such requirements.

1. Increased Federal Outsourcing

Federal IT outsourcing is double-edged, as it means more acquisition opportunities for contractors – and more risks of becoming a casualty of a security breach. In the September 2005 Federal Acquisition Regulation (FAR) revisions flowing information security duties down to contractors, the government recognized the link between IT outsourcing and cybersecurity roles:

> American society relies on the Federal Government for essential information and services provided through interconnected computer systems. Both Government and industry face increasing security threats to essential services and must work in close partnership to address those risks. Increasingly, contractors are supplying, operating, and accessing critical IT systems, performing critical functions throughout the life of IT systems.[42]

Of the 10,289 federal IT systems subject to FISMA security requirements in FY 2005, contractors operated more than 10 percent (1,105 systems).[43] The overwhelming majority of contractor-operated systems fall within agencies (Energy, Interior, Defense, and Homeland Security) that received an ''F'' on the FISMA information security report card.[44] Thus, not only will these agencies need the greatest contractor support to bolster the defenses against cyber attacks, but contractors will be guarding the most battered information gates where the cyber attacks are more likely to strike first.

Outsourcing trends guarantee that government contractors will handle ever-expanding shares of the federal information storehouses.

In addition, federal agencies have increasingly turned to commercial sources for data-mining services, rather than attempting to develop new federal databases of personal information in order to detect fraud, track terrorists, and manage risk.[45] In such instances, privacy advocates have complained that these agencies have sought to skirt Privacy Act requirements by outsourcing data collection activities.[46] This trend towards federal acquisition of data mining services – as well as security breaches by data brokers like ChoicePoint – have generated a number of congressional hearings and investigations, with many more likely in the future.

2. Heightened Security Requirements for Contractors

[39] OMB News Release, ''OMB Reinforces Strict Adherence to Safeguard Standards'' (June 26, 2006); OMB Memo to Department and Agency Heads, ''Protection of Sensitive Agency Information'' (June 23, 2006) (M-06-16) (www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf).

[40] *Id.; see* NIST Special Publication 800-53A (2nd Public Draft) (Apr. 2006) (available at http://csrc.nist.gov/publications/drafts.html#sp800-53-Rev1).

[41] OMB Memo to Chief Information Officers, ''Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments'' (July 12, 2006) (M-06-19) (emphasis in original) (http://www.whitehouse.gov/omb/memoranda/fy2006/m06-19.pdf).

[42] 70 Fed. Reg. 57450 (Sept. 30, 2005).

[43] OMB FY 2005 FISMA Report at 17.

[44] *Id.* at 27, 31, 39, 43; Rep. Davis, ''No Computer System Left Behind: A Review of the 2005 Federal Computer Security Scorecards,'' House Comm. on Government Reform (Mar. 16, 2006) (http://reform.house.gov/UploadedFiles/TMD%20FISMA%2006%20Opener.pdf).

[45] ''Industry executives, analysts and watchdog groups say the federal government has significantly increased what it spends to buy personal data from the private sector, along with the software to make sense of it, since the Sept. 11, 2001, attacks. They expect the sums to keep rising far into the future.'' Mohammed & Goo, ''Government Increasingly Turning to Data Mining,'' *Washington Post* at D3 (June 15, 2006); *see also* GAO, *Data Mining: Federal Efforts Cover a Wide Range of Uses* at 10 (May 2004) (GAO-04-548).

[46] *See, e.g., Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Government Use: Hearings before the Sen. Judiciary Comm.,* 109th Cong. (Apr. 13, 2005) (statement of James Dempsey, Center for Democracy & Technology) (http://www.cdt.org/testimony/20050413dempsey.pdf).

While the Privacy Act[47] has long applied to contractors that operate systems of records for federal agencies, the FISMA information security requirements for contractors are of more recent vintage. In a FAR revision, Federal Acquisition Circular (FAC) 2005-06 specifically recognized the applicability of information security requirements to contractors:

> Section 301 of FISMA (44 U.S.C. 3544) requires that contractors be held accountable to the same security standards as Government employees when collecting or maintaining information or operating information systems on behalf of an agency.[48]

According to these FAR revisions, these IT security standards include those spelled out in OMB Circular No. A-130 and NIST rules.[49] The FAR leaves detailed imposition of IT security requirements to the individual agencies. As an example of this agency-level implementation, recent NASA acquisition regulations mandate that contractors have NIST-compliant security plans, risk assessments, contingency plans, periodic training, and screened personnel.[50] Given the rapidly changing NIST standards,[51] contractors will be chasing moving targets in trying to maintain up-to-date IT security programs.

3. Greater Scrutiny for Contractors

For federal contractors, the crackdown on IT security is coming. For FY 2005, OMB asked agency inspector generals (IGs) to ensure that contractors ''meet the requirements of FISMA, OMB policy and NIST guidelines.''[52] In addition, OMB now requires agencies ''to track key performance metrics for FISMA compliance for contractor systems'' that comprise part of the FISMA inventory.[53] In July 2006, OMB issued instructions to all executive departments and agencies stating that government contractors must ''abide by FISMA requirements'' and ''each agency must ensure their contractors are doing so.''[54] The laundry list of NIST rules that agencies must include in contracts specify ''annual reviews, risk assessments, security plans, control testing, contingency planning, and certification and accreditation.''[55] As a result, contractors can expect to be thrown into the heart of the cyber battles in the coming year, with any security breaches or shortcomings being dissected by IGs, reported to Congress, and punished by agencies.

B. The Hazards of Security Breaches

In past years, federal contractors have largely avoided much of the spotlight for security breaches.[56] However, the odds weigh heavily against any company that assumes security breaches only happen to others. In a recent survey, 81 percent of companies responding acknowledged the loss or theft of a portable electronic storage device in the last 12 months.[57] Accordingly, government contractors need to prepare for the consequences in the event that federal data is lost or compromised on their watch.

1. Congressional Hearings and Investigations

When a company spills private information into the public domain, the top corporate officials will likely have multiple opportunities for no-expenses-paid trips to Washington, D.C. to be grilled in congressional hearings. Such has been the fate of ChoicePoint's chief executive officer and president who both had the opportunity to appear before Congress to answer tough questions about the company's security breaches.[58] Such companies have also had the pleasure of being audited by the Government Accountability Office regarding corporate privacy and information security practices.[59] Government contractors can anticipate more of the same anytime that they may be linked to cyber breaches involving federal data.

2. Responsibility and Past Performance

Government contractors with a record of spilling personal information into the wrong hands may find their responsibility and/or past performance in question.[60] For example, a large collection agency seeking private debt collection work from the Internal Revenue Service (IRS) had a long-standing contract suspended by the Ohio Attorney General's office ''after documents containing hundreds of names, addresses, and Social Security numbers of clients turned up in a trash bin behind the company's Columbus, Ohio, office . . . .''[61] Such challenges to contractor eligibility will become more common, as Congress and OMB tighten their FISMA grip on federal agencies that, in turn, will shift the pain to contractors in the form of tougher security and reporting duties, lower past performance ratings, and damaged opportunities for future work.

3. Enforcement Actions and Third-Party Litigation

By their nature, security breaches jeopardize personal information of third parties whose interests are often enforced by public agencies. In some cases, the

---

[47] 5 U.S.C. § 552a(m)(1).

[48] 70 Fed. Reg. 57451 (Sept. 30, 2005).

[49] 70 Fed. Reg. 57451; FAR §§ 7.103(u) and 11.201(d)(3).

[50] 71 Fed. Reg. 43408 (Aug. 1, 2006).

[51] The latest set of changes include the July 26, 2006 revision to NIST Special Publication 800-53 establishing standards for security controls for federal IT systems (http://csrc.nist.gov/publications/drafts.html#sp800-53-Rev1).

[52] OMB FY 2005 FISMA Report at 4.

[53] *Id.*

[54] OMB Memo (M-06-20), ''FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,'' Section A at 9 (July 17, 2006).

[55] *Id.* at 10.

[56] In 2005, the Bank of America lost computer backup data tapes for government travel cards, potentially compromising the personal information of 900,000 DOD employees. ''Secret Service, DCIS Investigating Missing Data on 900,000 DOD Travel Cardholders,'' *BNA Federal Contracts Report* at 201 (Mar. 1, 2005).

[57] ''Survey Finds 81 Percent of U.S. Companies Faced Lost, Stolen Devices with Private Data,'' *BNA Privacy Law Watch* (Aug. 16, 2006).

[58] *Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Government Use: Hearings before Senate Judiciary Comm.,* 109th Cong. (Apr. 13, 2005) (statement of Douglas Curling); *Protecting Consumers' Data: Policy Issues Raised by ChoicePoint: Hearings before House Subcomm. on Commerce, Trade and Consumer Protection of Comm. on Energy and Commerce*, 109th Cong. (Mar. 15, 2005) (statement of Derek Smith).

[59] GAO, *Personal Information: Agencies and Resellers Vary in Providing Privacy Protections* at 2, n.6 (Apr. 4, 2006) (GAO-06-609T).

[60] *See* FAR §§ 9.104-3 (responsibility) and 15.304(c)(3) (past performance).

[61] Freda, ''Firm Fired by Ohio for Lax Privacy Protection Pursuing Outsourced IRS Tax Collection Work,'' *BNA Privacy Law Watch* (Feb. 15, 2006).

  FCR ISSN 0014-9063

FTC will have jurisdiction over the security breach, resulting in fines and mandatory compliance programs to safeguard data. For example, ChoicePoint, which resells data to both government and private customers, paid a record FTC fine of $10 million ''over security breaches that exposed more than 160,000 people to possible identity theft,'' and also agreed to put another $5 million into a fund to compensate anyone injured by the breach.[62] In addition, the FTC ''Stipulated Final Judgment'' requires ChoicePoint to perform compliance monitoring and reporting, keep records, and inform the FTC of any corporate changes affecting such compliance for a 20-year period.[63] Even if the FTC does not take action, companies must still worry about state enforcement actions. More than 20 states now have security breach notification laws creating yet another layer of corporate risk when personal information is compromised.[64]

In addition to federal and state enforcement actions, security breaches have been fertile ground for breeding private litigation, including both class actions and individual suits, with considerable growth looming in the future.[65] Even for individual lawsuits, the cost can be high as illustrated by a recent jury award of $351,000 to a single victim of identity theft.[66] Although the privacy class actions have yet to gain much traction, the stakes can be enormous. For example, even in the absence of a security breach, one company is defending a $50 billion privacy lawsuit merely for sharing customer data with the National Security Agency (NSA).[67] Thus, a federal contractor wrestling with a security breach may quickly find itself engulfed in federal and state litigation by both public and private parties.

4. Contract Breach and Non-Compliance

Reacting to both the VA's pummeling over its security breach and the FAR and OMB directives to upgrade protection of federal information resources, agencies will pepper their IT contracts with new and more extensive FISMA and NIST information security requirements. Such requirements include: (1) submitting IT security plans compliant with NIST SP 800-18; (2) performing risk assessments consistent with Federal Information Processing Standards Publication (FIPS) 199; (3) preparing contingency plans per NIST SP 800-34; (4) assuring adequate security controls per NIST SP 800-53; and (5) conducting annual IT security training.[68] For government contractors experiencing security breaches in today's environment, the backlash will be quick and harsh, as illustrated by a VA subcontractor reporting the loss of a ''desktop computer containing sensitive personal information on thousands of veterans.''[69] Congressional press releases immediately expressed ''outrage'' over the incident, the VA secretary got involved, and the VA subcontractor footed the bill for free credit monitoring for as many as 38,000 veterans.[70] With OMB and Congress cracking down on information security, federal agencies cannot afford – and government contractors cannot expect – mercy when a contractor's lax IT security practices result in a security breach.

III. Conclusion

The cyber barbarians are circling, as the terrorists seek digital Pearl Harbors, the rogue state spies grab at our national secrets, and organized e-criminals look for easy money through cyber scams and identity heists. When our federal cyber defenses rate an overall ''D+'' and security breaches regularly rip through major agencies, the message is clear – the richest information banks in the world are ripe for cyber sacking and pillaging if federal agencies and contractors do not move quickly to shore up IT security defenses. In the short run, both agencies and contractors can upgrade these defenses by implementing – and enforcing – the IT security rules established by recent regulations, OMB directives, and NIST standards. In addition, leadership is critical, as management in both the government and industry must set information security as a priority and drive it from the top down. Finally, the commitment of resources – both in dollars and people – needs to be elevated consistent with the growing level of risk. When the cyber rampage begins, we best be ready.

---

[62] Mohammed, ''Record Fine for Data Breach,'' *Washington Post* at D1 (Jan. 27, 2006); *see* FTC News Release, ''ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress,'' (Jan. 26, 2006) (http://www.ftc.gov/opa/2006/01/choicepoint.htm).

[63] *United States v. ChoicePoint Inc.,* Civil Action No. 1 06-CV-0198, Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief (Jan. 26, 2006) (http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf).

[64] ''In 2006, More States Seek to Add to Body of 23 Data Breach Notice Laws,'' *BNA Privacy Law Watch* (Feb. 17, 2006).

[65] Cutler, ''Attorney Expects More Litigation By, Against Companies Over Privacy,'' *BNA Privacy Law Watch* (June 7, 2006).

[66] Pitts, ''Equifax owes damages in identity-theft lawsuit,'' *Richmond Times-Dispatch* Aug. 5, 2006).

[67] Stone, ''Lawsuit over phone records may grow,'' *USA Today* at 7A (May 15, 2006).

[68] 70 Fed. Reg. 57451; FAR §§ 7.103(u) and 11.201(d)(3) (FAR provisions imposing NIST standards); 71 Fed. Reg. 43408 (Aug. 1, 2006) (NASA acquisition regulations); NIST IT security standards (http://csrc.nist.gov/publications/nistpubs/index.html).

[69] ''Veterans Affairs Announces New Breach Involving Missing Computer, Sensitive Data,'' *BNA Privacy Law Watch* (Aug. 8, 2006).

[70] *Id.;* Lee and Wilber, ''Computer Theft Puts Floridians at Risk,'' *Washington Post* at A6 (Aug. 10, 2006).