

SEPTEMBER 2007



Forgiving Fraud and Failure

Profiles in Federal Contracting

U.S. PIRG

**Standing Up
To Powerful Interests**

Acknowledgements

Written by Gary Kalman , U.S. PIRG Education Fund.

Special thanks to the Project on Government Oversight, Matthew Barr, Phineas Baxendall, Brittany Brewer and Tony Dutzik for their invaluable contributions to this report.

Cover by Public Interest GRFX

© 2007, U.S. PIRG Education Fund

For a copy of this report, visit our website or send a check for \$20 made payable to U.S. PIRG Education Fund at the following address:

U.S. PIRG Education Fund
218 D Street, SE
Washington, DC 20003
202.546.9707
www.uspirg.org

The U.S. PIRG Education Fund offers an independent voice that works on behalf of the public interest. U.S. PIRG Education Fund works to protect consumers and promote good government. We investigate problems, craft solutions, educate the public, and offer Americans meaningful opportunities for civic participation.

Table of Contents

Executive Summary.....1

Introduction.....2

Part I: (Un)Secure Data.....3

Part II: Dollars After Defrauding.....7

Part III: Rewarding Poor Performance.....9

Conclusion & Recommendations.....12

Endnotes.....13

Executive Summary

Companies with immediate past histories of shoddy work and fraudulent practices are being rewarded with billions of dollars in federal contracts. The data suggest that the process by which the federal government currently spends \$422 billion per year in taxpayer funds is insufficient to ensure that the American people receive good quality for goods and services purchased for the American people.

The rapid increase of federally contracted dollars—100 percent since 2000—makes outsourcing the fastest growing component of discretionary spending. The government's preference for using outside contractors to provide goods and services makes careful scrutiny of the process and the decisions more important than in the past. At present, loose rules, lack of competition, and limited accountability permit so-called 'bad actors' to receive contracts that put taxpayers and our money at risk.

For this report, we reviewed hundreds of records and found numerous cases of contractors with questionable performance or responsibility records receiving contracts without competition or sufficient time to determine the extent of the problems identified. While the report outlines specific contractor practices, it is as much an indictment of the flawed contracting process as it is about any single company.

The profiles included in this report illustrate how little consideration is given to past performance and contractor responsibility. None of the companies faced suspension or debarment from receiving contracts for the incidents detailed in this report. The range of contracts shows the breadth of the problem and a sampling of the companies involved. A few examples include:

Fluor Corporation: Company executives were accused in 2000 of misusing federal contract dollars to buy luxury condos, a fine art collection and a Mercedes-Benz for the company president. The case settled in 2005. Less than a year later, Fluor Corporation's contracts with the federal government increased by \$1 billion; the value of the company's non-competitively bid contracts rose from 5.7 percent to 43 percent. A significant portion of the contracts were for hurricane relief in the Gulf coast.

Bank of America: The company experienced several instances in a single year (2006) in which unencrypted data files were lost or stolen. In one instance, the bank lost records for 1.2 million federal employees including records of United States Senators. Federal agencies including the IRS continued to award the company contracts for data processing and management services. More than 60 percent of the 2006 contract dollars were awarded without competition.

General Electric: Among other concerns, GE allegedly sold the government faulty helicopter and airplane engine blades in 1999 and 2000. In August 2005, the same year that the government decided to trust GE with the better part of a \$2.4 billion contract, the government was forced to get a court order to retrieve documents for its ongoing fraud case. In 2005 almost half of GE's federal contract dollars were awarded without competition.

These are just a few of the examples that illustrate how the current federal contracting system lacks accountability and appears to accept and, by default, reward bad behavior. Changes are necessary to stem the immediate and consistent flow of money to contractors that do not act responsibly with taxpayer funds.

Changes must include:

- **increased disclosure of contract information.** Increase the level of accountability by giving the public access to the actual contracts, track records of companies, compliance records with relevant laws and regulations, and performance evaluations of the work completed.
- **increased competition.** Restore competition to the vast majority of contracts. Sole-source awards should take place only under exceptional circumstances and should be subject to even greater scrutiny and transparency..
- **stronger rules to screen bad actors.** Accountability requires consequences for negligent or fraudulent behavior. Tighter rules should reward responsible contractors and hold non-responsible contractors accountable for their actions.

Introduction

Even before our nation was a nation, political leaders turned to private contractors to supply goods and services.¹ However, the rapid growth in federal contracting in recent years brings greater scrutiny of both the process and the players. Investigations into the actions of contractors have uncovered a series of widely publicized scandals from \$45 cases of soda for soldiers in Iraq to \$24 billion for Coast Guard boats that do not float. In August 2007, the Washington Post reported that no-bid government contract awards tripled since 2000 and rose by \$60 billion in the last year alone.²

The current administration's preference for privatizing functions previously performed by government employees led to a 100 percent increase in the amount spent by federal agencies on outside contractors since 2000. In FY 2006, the most recent year in which complete data is available, \$422 billion dollars of taxpayer funds were paid to more than 160,000 private contractors. The increase from 2000, approximately \$197 billion, makes contracting the fastest growing component of federal discretionary spending.³

Federal agencies that spend taxpayer funds directly are required to open their books. This transparency allows for accountability. Whether through internal audits or as a result of Freedom of Information Act (FOIA) requests, the public has access to information to evaluate and hold public agencies and public officials responsible for the money spent and the goods and services provided.

Work performed by private contractors affords the public far less protection. For example, contractors are not currently covered by FOIA. Except for information in the Federal Procurement Data System, the public is therefore forced to rely on the integrity of the contracting process and the wisdom behind the choices made when taxpayer funds are awarded to private companies.

The current process for handing out contracts does not provide the public with confidence in either the integrity or wisdom behind the decisions made to spend billions of taxpayer dollars. This report highlights just a few of the examples of federal contracts awarded to companies with questionable immediate past perfor-

mance or responsibility records including: (1) data security firms that experienced serious data breaches; (2) firms that defrauded the government; and, (3) firms that failed to deliver on one contract only to be rewarded with another.

The greater the reliance on outside contractors by the federal government, the more the public needs assurance that the money is well spent. The following profiles strongly suggest that the federal contracting process is in need of significant reform.

According to Bernd Schmitt, executive director of Columbia University's Center on Global Brand Leadership, when companies experience scandal, "the restoration process would require immediate and intense crisis management."⁴ In short, corporate malfeasance requires significant steps to counter any backlash from their customers. This report suggests that these same companies need not fear for their federal contracts. Loose rules and the lack of competition allow these bad actors to renew and receive new federal contracts worth billions of dollars without appropriate scrutiny. As a result, taxpayers may not be getting the value or quality of goods and services they have a right to expect.

Federal agencies employing contractors must take specific steps to ensure that the actions and track records of those vying for taxpayer funds are taken into account in a fair but systematic way to avoid the waste, fraud and abuse uncovered by recent high profile scandals. The incidents detailed here suggest that the lack of competition or consideration of company performance needlessly put taxpayers and their money at risk.

Part I: (Un)secure Data

Agencies in the federal government collect enormous quantities of sensitive data. From the IRS to the Social Security Administration, the federal government holds private information about every citizen. Digital data storage makes it easier than in the past to gather and manage data. Technology also enables hackers and identity thieves to steal and use the data for their own purposes.

The federal government has outsourced some data management and hired companies to develop security systems for in-house storage. The profiles below detail how companies are awarded data security and data management contracts—many without a competitive process—immediately following a serious breach. These awards raise questions about whether the public would have been better served by increased scrutiny and an open bidding process that includes consideration of company performance.

Bank of America

Who they are

Bank of America is listed by the Federal Reserve as the second largest bank by assets in the United States. As a commercial bank, its core services include “consumer and small business banking, credit cards, investment banking, brokerage and asset management.”⁵ The company currently services over 33 million consumers in 5700 retail banking offices in 150 countries.⁶ In 2006, Bank of America’s total service revenue reached \$74.2 billion, an increase of more than \$17 billion compared to 2005. A majority of Bank of America revenue (over 53 percent) is obtained from global consumer and small business banking interests; however, the second largest source of revenue (32 percent) is under the category of global corporate and investment banking, which includes contracts with the federal government.⁷

What they did

In 2005, Bank of America suffered three incidents where the security of their data was compromised.

In February 2005 in Charlotte, NC, the location of the corporation’s headquarters, a backup tape went miss-

ing that contained over 1.2 million records of federal employees, including the information of United States Senators. The tapes reportedly contained information on the accounts of the General Services Administration’s SmartPay charge card program—the equivalent of a government issued credit card—which has more than 2.1 million members.⁸ Bank of America was widely criticized for its failure to use encrypted backup tapes that would have protected the data from a security breach. It is still unknown whether any of the lost tapes have actually compromised the accounts of customers, but since only three of the four missing tapes were recovered, the data on the fourth tape could potentially still be accessed and abused.⁹ Following the announcement of Bank of America’s data breach, the Federal Deposit Insurance Corporation and three other government agencies issued a press release that set guidelines to require financial institutions to notify their members about “incidents of unauthorized access to customer information that could result in substantial harm or inconvenience to the customer.”¹⁰

In May 2005, a laptop was stolen from Bank of America, which contained 18,000 records of Californian consumers. The information was not encrypted. At the time it went missing, the laptop with the sensitive data was not in possession of a bank employee, but rather, it was being held by an outside consultant who had been hired to provide technical support. Bank of America declined to answer why the technical support was being performed by a third party, rather than by a bank employee.¹¹

In September 2005, the company experienced its third data breach of the year. Bank of America lost another laptop containing confidential consumer information about “Visa Buxx” users. The laptop was stolen from a third party service provider, including the names, credit card numbers and other banking information of customers.¹² The stolen laptop, again with data unencrypted, contained an undisclosed number of customer records. It remains unknown how many, if any, of the records were compromised by the incident. According to the spokesperson for Bank of America, Diane Wagner, there were no signs of fraud detected; however, she noted that since the information on the laptop was not encrypted, it would be easier for thieves to access.¹³

What they got

Business-to-government consultant Mark Amtower predicted that Bank of America would have difficulty rebuilding its relationship and renewing its federal contracts: “The loss of the SmartPay information could hurt Bank of America’s chances to renew its contract with the government.”¹⁴ Despite Bank of America’s record in 2005, the federal government continued to reward the corporation largely with non-competitive contracts to provide their expertise on financial management matters and tax collection. Following the multiple security mishaps, in 2006 Bank of America received more than \$3 million in federal contracts for a variety of services including automatic data processing. While a relatively small amount by federal government standards, only 36.1 percent of those contracts were awarded under a process of full and open competition.¹⁵ The company’s services were contracted by a number of different government agencies including the Internal Revenue Service and the US Treasury Financial Management Service.

A dip in stock prices immediately followed the Bank of America data loss incidents. In March 2005, following the first data loss, Bank of America’s stock dropped 6 percent. Then again in October 2005, following the September incident, the stock dropped another 4.6 percent.¹⁶ It would appear shareholders were more discerning than the federal government.

LexisNexis

Who they are

LexisNexis has been a member of Reed Elsevier Group since 1994. In 1973, the database originally known as LEXIS, launched publicly as a legal research system that offered full text searching of all Ohio and New York state law cases.¹⁷ Since then, LexisNexis has prided itself in being the leading provider of comprehensive business solutions to all industries, including legal, risk management, corporate, government, law enforcement, accounting and academic. LexisNexis operates in over 100 different countries and employs over 13,000 employees. It serves customers by making available over 5 billion searchable documents from more than 32,000 legal, news and business sources via the LexisNexis Internet database.¹⁸ LexisNexis offers many of the same services to the federal government, including automated news and data services, information retrieval and ADP telecommunications. Agen-

cies like the Internal Revenue Service, the Bureau of the Public Debt, the Transportation Security Administration and the Securities and Exchange Commission utilize the company’s records to research public and business information and legal news.

What they did

In March 2005, thieves hacked into a LexisNexis database and gained access to more than 32,000 private records. The information accessed by the criminals included Social Security numbers, names, addresses and drivers license information.¹⁹ One month later, the company realized that approximately 280,000 additional records had been compromised during the previous incident; thus, the identities of a total of 310,000 people were endangered by the breach. According to LexisNexis CEO, Kurt Sanford, the company took immediate action to “notify individuals where [they] found some indication that they might have some risk of identity theft or fraud, even if the risk did not appear significant.”²⁰ He tried to assure the public that LexisNexis’ products for fraud detection and identity authentication are still useful and effective.²¹

On June 30, 2006, it was reported that two men were arrested in connection with the March 2005 LexisNexis breach.²² The accused individuals ranged in age from 19 to 24 and claimed that they had created LexisNexis accounts to look up the Social Security numbers and other personal information of Hollywood celebrities. A Reed Elsevier investigation verified that the database was fraudulently breached over 59 times using the stolen passwords.²³

What they got

Following the breach in 2005, the company’s contracts with the federal government increased both in number and value. In 2005, the federal government awarded the corporation \$140 million in federal contracts for a variety of goods and services including automatic data processing services. In 2006, the company received \$183 million.²⁴ Prior to the breach, in 2004 the company received ‘only’ \$104 million dollars. Following the incident the federal government rewarded LexisNexis with approximately \$80 million in additional work including the purchase of automatic data processing services. The Patent and Trademark Office, the Army and the IRS were some of the primary purchasers of

LexisNexis' services.

Honeywell International

Who they are

Honeywell International was created after the merger of two companies, Minneapolis Heat Regulatory Company and Honeywell Heating Specialty Company in 1927. After the merger of these two worldwide powerhouses, the Minneapolis-Honeywell Regulatory Company became one of the leading vendors of a variety of products including high quality jeweled clocks, aeronautical equipment, computer systems, and security systems. By 1998, Honeywell had established operations in 95 countries. In 1999 Honeywell merged with Allied Signal and moved into its new headquarters in Morristown, New Jersey. Allied Signal specialized in aerospace, automotive and engineering products that it developed for and supplied to private companies and the government.²⁵

Honeywell's services to the federal government in 2006 comprised over 15 percent of the company's total profits for the year. . In 2005, the company received \$2.3 billion in federal contracts placing them among the top 20 federal contractors. Honeywell provides a variety of products and services to the federal government, including the operation of government owned facilities and the production of aircraft parts. The majority of Honeywell's federal contracts are awarded by the Army, the Department of Energy, the Airforce, National Aeronautics and Space Administration and the Defense Logistics Agency.²⁶

What they did

Honeywell International has had a number of run-ins with the federal government over the years. In 2006, the company was forced to pay \$451 million to help cleanup Onondaga Lake.²⁷ The company has been charged with at least 5 cases of misconduct in the last 16 years and settled additional cases involving misallocating labor charges on a contract, failing to properly test electrical cables installed at a US Treasury facility, and procurement and disclosure fraud.²⁸

In February 2006, Honeywell International exposed over 19,000 records of employee's personal informa-

tion, including their Social Security numbers and bank account information, on a public Web site.²⁹ According to the company, Howard Nugent, a former employee in Arizona, is responsible for the data leak. He reportedly accessed the sensitive information on a Honeywell computer and then caused the "transmission of that information". After being notified of the breach, the company had the page removed from the Internet and assigned someone to monitor the Web site.³⁰

What they got

Despite the company's less than impressive track record, the federal government has consistently strengthened its ties to Honeywell International. In the months following the data breach in February 2006, Honeywell received more than 6000 federal contracts worth over \$2 billion for a variety of goods and services including automatic data processing services. The top federal agencies that purchased services from the company following the breach were the U.S. Army, Air Force, NASA and Department of Energy. Only 43.2 percent of those contracts were awarded under full and open competition.³¹ The remaining contracts were awarded outside the competitive process.

ChoicePoint

Who they are

ChoicePoint Corporation is one of the leading providers of consumer information to government agencies and the private sector since 1997.³² Last year, ChoicePoint's total service revenue passed the \$1 billion mark. The majority of its revenue, nearly 44 percent comes from services provided to the insurance industry. Not far behind is the income from federal contracts.³³ Due to legislation like the 1974 Privacy Act, banning the government from operating its own informational surveillance database, companies like ChoicePoint were relied upon for the surveillance and personal information they provide to government and the private industry.³⁴ In fact, since the company broke away from its parent company, Equifax, in 1997 it has become one of the leading information providers to the federal government.³⁵ ChoicePoint's average revenue from government contracts accounted for approximately 14.4 percent of its total service revenue in 2005 with percentages increasing each year since becoming independent.

What they did

In February 2005, 163,000 ChoicePoint client records including names, addresses, and Social Security numbers were breached by criminals who presented themselves as legitimate businessmen. The criminals reportedly used the stolen information in at least 800 identity theft scams.³⁷ Immediately following the breach, ChoicePoint was advised by law enforcement officials to notify all the individuals in the state of California about the breach because the California Civil Code, enacted in 2003, requires “any company that owns or licenses computerized data, [to] disclose any breach of the security of the system following discovery or notification of the breach... to any resident of California.”³⁸ The federal government has a similar rule for its own data systems but does not extend the notification requirements to cases that involve outside data brokers and third party processors.³⁹ Ironically, ChoicePoint cited the Federal government’s lenient standard to boast on its website that the company exceeded federal requirements in responding to the breach. They omitted any mention of the California requirement.⁴⁰

The public announcement informing customers about the lost information was made in February of 2005. This important notification came 4 months after the company first learned about the breach preventing the affected customers from mitigating the damage.⁴¹

Complicating matters is that this was not the first time the company experienced this particular type of infiltration. In 2002, two thieves tapped ChoicePoint’s consumer information database after posing as legitimate businessmen. The thieves made between 7,000 and 10,000 inquiries on the personal information of consumers and used some of the stolen identities to commit over \$1 million worth of fraud. This discovery came as a surprise to the public that had been under the impression that the 2005 breach was “the first of its kind”. In fact, during the 2005 incident ChoicePoint CEO Derek Smith had affirmed in an interview with The Associated Press that the company “had never been victimized by this kind of criminal breach before.”⁴²

The Federal Trade Commission (FTC) charged ChoicePoint with a failure to uphold security and record-hand-

ling procedures that conformed to consumers’ privacy rights and federal laws.⁴³ ChoicePoint settled the case for \$10 million in civil penalties and \$5 million in consumer rights redress, which according to the FTC, is “the largest civil penalty in FTC history”. The settlement also requires ChoicePoint to verify the identity of businesses handling consumer reports, to establish reasonable procedures to ensure that consumer rights are protected, to undergo an independent audit every two years and to submit to increased oversight by the FTC.⁴⁴

Immediately following the February 2005 security breach, the company suffered a nearly \$10 decline in the price of their shares.

What they got

Agencies like the Internal Revenue Service, the U.S. Army, the Bureau of Citizenship and Immigration and other Offices, Boards and Divisions (including the Attorney General) employ ChoicePoint to perform a significant number of professional services including automatic data collecting and processing. In 2000, ChoicePoint’s federal contracts amounted to a little more than \$7 million. In 2005, the federal government awarded over \$65 million in contracts the majority of them after the February incident. At the same time, the percentage of competitive contracts has decreased. In 2000, 97.3 percent of ChoicePoint’s contracts were awarded under a system of full and open competition. By 2005, only 31.7 percent of the contracts were awarded after a competitive bidding process.⁴⁵

In 2006, just one year after the widely publicized scandal, not much had changed. ChoicePoint continued its relationships with federal agencies including the Office of Personnel and Management, the U.S. Army, the Federal Bureau of Investigation and the Internal Revenue Service.⁴⁶ Less than a third of these contracts (approximately 29 percent) were awarded under a system of full and open competition.

Part II : Dollars After Defrauding

The federal government continues to work with contractors who commit fraud with taxpayer dollars. Contractors who inflate bills or use public funds for personal use are far too often allowed to pay a relatively small fine and receive new contract awards.

The renewal, extension or awarding of new of contracts to companies that defraud the government is not currently in violation of any policy or protocol.

As the following profiles suggest there is little accountability for primary contractors or incentive to ensure subcontractors are responsibly spending the money they receive to provide goods and services to the federal government.

Kellogg, Brown, and Root

Who they are

Kellogg, Brown, and Root (KBR) is an engineering and construction company formed in 1998 when Halliburton purchased Dresser Industries. Dresser's construction subsidiary, M.W. Kellogg merged with Halliburton's construction subsidiary to form what has now become the largest contractor for the U.S. Army, a top-ten contractor for the Department of Defense, and the world's largest defense services provider.⁴⁷ KBR was a Halliburton subsidiary until April 5 2007, when it broke ties with Halliburton and became independent.

What they did

Since 2000, KBR has been accused of defrauding the government on four separate occasions. Three of the complaints resulted in financial penalties to KBR and one is pending. The largest of these instances involved excessive charges in 2004 in KBR-run dining facilities in Iraq and Kuwait. Normally, KBR's subcontractors charge a fixed meal cost using statistics like camp population and billeting records to estimate the number of meals served. However, according to the Defense Contract Audit Agency (DCAA), KBR's subcontractors were billing for up to 36 percent more meals than were actually served. Initially, the government withheld approximately \$176 million until KBR could provide supporting data.⁴⁸ KBR argued that billing for

these excess meals was allowable, since their contract did not specify a billing methodology. Later in 2004 KBR reached an agreement with the Army Materiel Command in which the Army withheld \$55 million of allegedly fraudulent charges.⁴⁹

In 2003, KBR was accused of overcharging the U.S. government for fuel in Iraq. That year, the federal government awarded KBR's parent company Halliburton the \$7 billion Restore Iraqi Oil (RIO) contract. KBR was then tasked with providing oil to Iraq. An investigation by the DCAA found that in December 2003 that KBR had overcharged the government roughly \$61 million for fuel imported into Iraq from Kuwait. KBR charged \$2.27 a gallon for unleaded gasoline from Kuwait, about a dollar per gallon more than another contractor charged for oil from Turkey which had to be transported over a greater distance.⁵⁰ The suspected \$61 million overcharge led the Pentagon to launch an investigation to examine accusations of fraud. By 2006, the DCAA had identified approximately \$279 million in unsupported and questionable expenses. That year, the Department of Defense held back \$10 million in payments to the company.

What they got

In 2005, shortly after negotiating a settlement on allegations of overcharging, the Army contracted for nearly \$5 billion with Halliburton and its subsidiary KBR largely to provide logistics support to U.S. troops. The contracts—57 percent awarded without open competition — amount to an increase of \$1 billion over the company's 2004 contract.

On January 19, 2004, in the midst of the dispute around fuel prices, the government awarded Halliburton and KBR a follow-up to the RIO contract to provide oil to Iraq. Ironically, announcement of the new RIO contract came on the same day that the Defense Department's inspector general referred accusations of fraud to its Criminal Investigative Services Unit.⁵¹

The Fluor Corporation

Who they are

The Fluor Corporation is one of the world's largest engineering, construction, procurement and maintenance

corporations. Founded in 1912, it grew throughout the 20th century, becoming a major international player in construction, notably construction in the natural resources industry. Fluor Corporation has a long history as a U.S. government contractor. In the early 1950's Fluor Corporation began contracting with the government to build major facilities ranging from nuclear power plants to air force bases.

Today, Fluor Corporation is a major government contractor reaping \$2.6 billion from government contracts in 2006, placing them among the top 20 federal contractors. Unlike KBR, Fluor Corporation contracts come largely from the Federal Emergency Management Agency (FEMA) and the Department of Energy. Fluor Corporation received contracts worth more than \$1 billion for recovery assistance after Hurricane Katrina.⁵² The Department of Energy relies heavily on Fluor Corporation for cleanup of radioactive and other dangerous chemicals.

What they did

Fluor Corporation has settled several cases of government fraud in the past ten years. In March 2000 a former employee filed a lawsuit against the company under the False Claims Act. The employee claimed that the company had improperly used a fictitious entity to recover costs from the government. Among the alleged wrongful expenses were multi-million dollar bonuses paid to management, \$10 million for build facilities that Fluor leased to other companies, and money for luxury condos, a fine art collection, and a Mercedes Benz convertible for the company president.⁵³ Following a Justice Department investigation, Fluor finally agreed to settle the suit in 2005, paying \$12.5 million.

In a separate incident, Patrick Hoefer, the company's former director of Government Financial Compliance, accused Fluor Corporation in 2001 of knowingly submitting millions of dollars in false invoices in the mid-1990s. The complaint involved a former division of Fluor entitled the Technology Operation Company (TOC). Under the terms of its federal contracts, Fluor ought to have distributed TOC's overhead costs equally among its many contracts. The federal government should have been responsible for no more than 10 percent of the costs. Instead, Fluor charged the vast majority of TOC's overhead to the federal government.⁵⁴ Eventually, the federal government took over pro-

secution of the lawsuit and the Department of Energy's Office of Inspector General, the Defense Criminal Investigative Service, the Army Criminal Investigative Command, the Department of Transportation's Office of Inspector General and the Defense Contract Audit Agency all became involved in the investigation and litigation. The company settled the lawsuit for \$8.2 million later in 2001.

What they got

Fluor Corporation's relationship with the federal government showed no visible signs of strain as a result of these two incidents. In 2006, the year following the \$55 million settlement, the company's total government contracts increased by about \$1 billion, largely as a result of contracts awarded to the company for recovery efforts after Hurricane Katrina. Contracts awarded outside a competitive process jumped dramatically from 5.7 percent in 2005 to 43 percent in 2006.

In 2002, following the \$8.2 million settlement, the federal government awarded Fluor Corporation \$1.1 billion in contracts, a 10 percent increase over the year before.⁵⁵

Part III: Rewarding Poor Performance

A contractor's past performance is supposed to be considered when renewing, extending or awarding new contracts, according to the Federal Acquisition Regulation.⁵⁶ Companies that cut corners or engage in negligent practices must be held accountable and that includes a contractor's ability to receive future contracts. The consequences can be quite serious. Delivering faulty equipment or failing to test equipment puts individuals at risk and, in the cases profiled below, threatens our national security.

The following profiles suggest that past performance may not be given high priority when determining awards.

General Electric

Who they are

General Electric (GE) is a Fortune 500 company that is consistently listed among the 10 largest corporations in the world. GE has grown, in part, through mergers with other corporations. Currently, it produces and markets products and services ranging from refrigerators to jet engines. GE made \$163 billion in revenue in 2006, more than \$20 billion in profits.⁵⁷

In 2006, GE had about \$1.6 billion worth of contracts with the government (responsible for about 1 percent of its income). The majority of GE's contracts are for gas turbines and jet engines, for which GE had approximately \$1 billion worth of contracts in 2006, placing them among the top twenty federal contractors.⁵⁸ The remainder comes largely from support services and medical equipment like X-Ray machines. A majority of GE's government contracts are with the Department of Defense. The company holds smaller contracts with other agencies such as the Department of Veterans Affairs.

What they did

GE allegedly sold the U.S. military defective helicopter and airplane engine blades. Allegations included problems with the casting and testing of the blades. Several former GE employees filed a lawsuit alleging that

GE rushed to produce engine blades in 1999 and 2000. The problems laid out in the complaint included assertions that the stepped up production led to thousands of cracked engine blades. Even very small cracks in an engine blade can, when exposed to intense heat and pressure, cause a blade to break off. That, in turn, could set off a chain reaction leading to engine failure and metal fragments slicing into the fuselage.⁵⁹ The suit details company attempts to bury evidence of the defects by coating the blades.⁶⁰ The government launched a criminal investigation in November of 2000. GE settled the case for \$11.5 million in July of 2006.

In 1995, GE settled a suit that alleged that several thousand GE jet engines sold to the military did not comply with military electrical bonding and electromagnetic testing requirements. Proper electrical bonding resistance levels protect aircraft from electromagnetic interference that can harm the performance of electronic equipment. The lawsuit, filed in December 1993, claimed that GE delivered the engines to the military knowing that certain electronics did not meet the bonding requirements. Fortunately, no aircraft were found to be unsafe but the Air Force did find that some engine components exceeded bonding specifications. GE agreed to settle the suit for \$7.1 million rather than go to trial.

What they got

GE's government business did not skip a beat during or immediately following either incident. In 1996, the year after GE settled the electrical bonding case, GE produced the engine for the Navy's new F/A 18 Super Hornet and overall sales volume for military engines increased substantially.⁶¹

In August 2005, at the same time GE was defending the company's production of faulty engine blades, the federal government awarded GE the majority of a \$2.4 billion contract to develop its F136 engine as an alternate engine for the new Joint Strike Fighter aircraft.⁶² While negotiations were proceeding on the new contract, government investigators had to obtain a search warrant to gain access to GE's offices for information regarding the earlier contract for helicopter and engine blades.⁶³

While the government had ample reason to question the contractor's actions, the difficulties were appar-

ently insufficient to force full competition. Forty-six percent of GE's government contracts that year were not competitively bid.

Raytheon

Who they are

Raytheon is a large military contractor based in Waltham, Massachusetts. It was founded in 1922 and has a history of producing a diverse array of electronic devices. In the mid-1990s, Raytheon expanded its defense segment with the acquisition of the defense businesses of E-systems and Texas Instruments. Raytheon also acquired the aerospace and defense business of Hughes Aircraft, which included a variety of product lines, including the former General Dynamics missile business.

Today, Raytheon has about 73,000 employees, and annual revenues of about \$20 billion.⁶⁴ Raytheon relies mainly on its military contracting, which provides more than 80 percent of its revenue (in 2006 Raytheon's net sales to the U.S. government were about \$17 billion).⁶⁵ The company is among the top ten federal contractors. Raytheon sells a variety of products and services to the government, ranging from missiles and missile defense systems, to network systems, to intelligence systems.

What they did

In 2000, Raytheon's subsidiary, Hughes Aircraft, admitted under the Department of Defense voluntary disclosure program that they had not performed acceptance and performance tests on components used in radar systems on F-14 and F-15 aircraft required by their contract.⁶⁶ A related investigation determined that Hughes Aircraft inflated the number of labor hours that they billed to the government. Raytheon settled these two cases for about \$2 million.⁶⁷

This was not the first time that Raytheon failed to perform required testing or had serious billing disputes. In 1996 Raytheon settled a case involving a failure to perform required tests on advanced electronic equipment, including radar units for military aircraft, missile guidance units, and delicate tracking equipment.⁶⁸ And in 1993, Hughes Aircraft was convicted of conspiring to defraud the government by knowingly producing equipment that had not been tested properly.⁶⁹

What they got

Despite ten cases of misconduct involving the company and its subsidiaries in the five year period between 1995 and 2000 including the ones profiled above, in 2001 more than half of the government contracts with Raytheon (approximately 56 percent) were awarded outside of open competition.

In 2001, after the radar settlement, Raytheon sold over \$100 million worth of radar equipment to the military. Net sales to the government remained steady at \$16.9 billion in 2001.⁷⁰

Northrop Grumman

Who they are

Northrop Grumman is a large aerospace and defense conglomerate that was created as after the 1994 purchase of Grumman Aerospace by Northrop Aircraft. Since this takeover, Northrop Grumman has bought several other defense-related companies, including ship-builders Litton Industries and Newport News Shipbuilders as well as several electronic and computer companies, including Westinghouse Electronic Systems.

The company made about \$30 billion in revenue in 2006, of which about 85 percent resulted from sales and business with U.S. government and places them among the top ten federal contractors.⁷¹ Northrop sells a variety of products to the Department of Defense, the most notable of which are missile systems, aerospace systems, electronics and ships.

What they did

Since 1995, Northrop Grumman has had to answer for 21 instances of misconduct pertaining to federal contracts. The misconduct involves a variety of problems including installation of substandard parts, overcharging the government, and unfair labor practices.⁷²

In 2003 Northrop Grumman settled cases for allegedly defective unmanned aerial vehicles known as target drones sold to the Navy from the late 1980s through the early 1990s. In a False Claims Act suit, the government asserted that the quality assurance programs

for the drones failed to meet military specifications and that drones bought through eight separate contracts with the Navy contained defective parts. The suit stated that Northrop Grumman was aware of the problems.⁷³ The government alleged that the drones experienced major failures during operations due to defective parts. Northrop Grumman settled the case for \$20 million.

In a 2000 case, two former Northrop Grumman employees alleged that Northrop Grumman did not properly manufacture more than 5,000 replacement parts it made for military aircraft, thus violating a 1992 contract. The contract with the Air Force required Northrop Grumman to convert commercial planes to military use. As part of this contract, Northrop was required to calibrate certain ovens it used to treat aluminum replacement parts for strength and flexibility.⁷⁴ According to the government, Northrop Grumman failed to calibrate and maintain the ovens from March 1993 until October 1995. This failure was documented in internal reports in 1994. The company did not act to correct the problem until 1995. Fortunately, the reduced strength and flexibility did not compromise the safety of the aircraft. That likely accounted for the relatively modest settlement of \$750,000. However, since the company did not perform the tests on the standard parts, Northrop Grumman had no way of knowing if the equipment was safe and functional.

What they got

Within a year after the \$20 million settlement in the case of the defective drones in 2003, Northrop Grumman increased the value of the company's government contracts by more than \$1 billion dollars. Putting aside the concerns of the just signed settlement, the amount awarded to the company in full and open competition dropped from 54 percent in 2003 to 42 percent in 2004.

In March, 2005, less than a year and a half after the target drone settlement, the Navy awarded Northrop Grumman a \$24 million dollar contract for BQM-74 Chukar target drones—the same type of drones that experienced failures due to defective parts Northrop Grumman installed.⁷⁵ This contract was awarded without competitive bidding.

The value of Northrop Grumman's contracts with the federal government has fluctuated since 2000. The largest increase—almost \$4 billion — came in 2001 shortly after the company settled the case involving the 5,000 defective parts.⁷⁶

Conclusions & Recommendations

Increasing reliance by the federal government on outside contractors requires that more attention than ever be paid to the process and choices made in awarding federal contracts. The profiles in this report add to the mounting evidence that serious problems exist in the way the federal government awards contracts and that bad choices have serious consequences that potentially impact the lives, safety and security of all Americans.

Unfortunately, loose rules and a lack of accountability have afforded companies with questionable track records—arguably violations of the Federal Acquisition Regulations—to receive federal contracts without undergoing the rigorous review involved in a competitive process. As a result, tax dollars may be wasted and individuals may be harmed. In the private sector, shareholders have proven themselves willing to punish sloppy, inept or illegal behavior practiced by companies. The federal government should be no less vigilant. They should not ignore such behavior and practices when purchasing goods and services for the American people.

The evidence presents a case that calls for significant reform. The federal contracting process, in its current state, does not have effective safeguards to ensure that taxpayers are receiving quality services.

Recommendations

There are a series of steps that can be taken by federal agencies when contracting out for goods and services. The following policy recommendations represent just a few of the numerous changes necessary to restore integrity to the contracting process.

Increase disclosure of contract information. For the public to have a complete picture of the process and the decisions made, the administration should create a fully searchable, publicly accessible online database of federal contracts. Last year Congress passed legislation to require the creation of such a database. To date, the database is not operational. A database developed by the private nonprofit group

OMB Watch should serve as a model for the administration with some additional information such as publication of the actual contracts, track records and evaluation of work completed by the contractor.

Increase competition. Existing rules allow for far too many contracts to sidestep a competitive review process. Currently, 40 percent of contracts are awarded without a competitive process. There are certainly situations in which competition may not be possible such as legitimate emergencies or a lack of respondents to a contracting request but noncompetitive contract awards should be rare. Instead they are routine. Rules must be changed to ensure that there is meaningful competition for the vast majority of awards. Too many contracts are designed in ways that minimize competition. For example, federal proposals that bundle together a large series of deliverables yield super-sized contracts that limit the ability of small businesses, women and minority owned businesses to compete.

Stepped up rules to screen bad actors. Current rules require contract officers to consider the track records of companies vying for federal dollars, but the guidelines are extremely weak and very subjective. The public should not reward negligent, inept or illegal behavior by granting these companies millions in federal contracts without assurances that the work will be done in a satisfactory and professional manner. We must be very cautious about granting companies who experience serious data breaches to protect sensitive data. We must also consider tighter rules to restrict companies that defraud the government or fail to deliver on existing contracts from receiving new contracts. These ‘bad actors’ should face suspension from receiving federal contracts.

The people involved in the contracting process have come to expect the renewal of federal contracts regardless of the quality of work delivered. But contracting dollars are not entitlements. In the rush to outsource, agencies and the companies with which they work have forgotten that fact. The solution to the abuses detailed in this report is to restore true competition and accountability to the federal contracting process.

Endnotes

1. The Oyez Project, Chisholm v. Georgia case file, available at http://www.oyez.org/cases/1792-1850/1793/1793_0/.
2. Robert O'Harrow Jr., The Washington Post, Federal No Bid Contracts On Rise, August 22, 2007, available at <http://www.washingtonpost.com/wp-dyn/content/article/2007/08/22/AR2007082200049.html?hpid=percent3Dtopnews&sub=AR>
3. Chairman Henry Waxman, House Committee on Oversight and Government Reform, Dollars, Not Sense: Government Contracting Under the Bush Administration, June 19, 2006 available at <http://oversight.house.gov/story.asp?ID=1071>.
4. Knowledge@Wharton, Wharton Business School, Brand Rehab: How Companies Can Restore a Tarnished Image, September 21, 2005 available at <http://knowledge.wharton.upenn.edu/article.cfm?articleid=1279>.
5. Yahoo! Finance, "Bank of America Corporation Company Profile", available at <http://biz.yahoo.com/ic/58/58444.html>.
6. Daniel Weiss, Associate General Counsel, Bank of America, personal communication, April 20, 2004, available at <http://www.ftc.gov/os/comments/canspam/OL-105247.pdf>.
7. Bank of America, Annual Report, 2006 available at http://media.corporate-ir.net/media_files/irol/71/71595/reports/2006_AR/financial_highlights.html.
8. Robert Lemos, CNET New, "Bank of America loses a million customer records," February 25, 2005, available at http://news.com.com/Bank+of+America+loses+a+million+customer+records/2100-1029_3-5590989.html.
- 9/ Robert Lemos, Security Focus, "Backup tapes a backdoor for identity thieves," April 28, 2005, available at <http://www.securityfocus.com/news/11048>.
10. Federal Deposit Insurance Corporation, Press Release: "Federal Regulatory Agencies Jointly Issue Interagency Guidance on Response Programs for Security Breaches," March 23, 2005, available at <http://www.fdic.gov/news/news/press/2005/pr2605.html>.
11. David Lazarus, San Francisco Chronicle, "Breaches in security require new laws," June 29, 2005, available at <http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2005/06/29/BUG1VDG77F1.DTL&type=printable>.
12. Martin H. Bosworth, ConsumerAffairs.com, "Bank of America Loses Consumer Data Again," October 12, 2005, available at http://www.consumeraffairs.com/news04/2005/bofa_laptop.html.
13. Robert McMillan, PC World, "Bank of America Warns Customers After Laptop Theft" October 7, 2005, available at <http://www.pcworld.com/article/id,122943-page,1/article.html?RSS=RSS>.
14. Robert Lemos, CNET New, "Bank of America loses a million customer records," February 25, 2005, available at http://news.com.com/Bank+of+America+loses+a+million+customer+records/2100-1029_3-5590989.html.
15. OMB Watch, FedSpending.org, Contracts to Bank of America 2006, available at http://www.fedspending.org/fpds/fpds.php?company_name=bank+of+america&sortby=u&detail=-1&datatype=T&reptype=r&database=fpds&fiscal_year=2006&submit=GO.
16. Morningstar, Bank of America Corporation Stock Chart, available at <http://tools.morningstar.com/charts/Mcharts.aspx?Country=USA&Security=BAC&sLevel=A>.
17. LexisNexis company website, "Company History," available at <http://www.lexisnexis.com/press-center/mediakit/history.asp>.
18. LexisNexis company website "About LexisNexis" <http://global.lexisnexis.com/about.aspx>.

19. Associated Press, reprinted by MSNBC, "Agents probe LexisNexis security breach," May 19, 2005, available at <http://www.msnbc.msn.com/id/7913667/>.
20. LexisNexis, Press Release: "LexisNexis Concludes Review of Data Security Activity, Identifying Additional Instances of Illegal Data Access," April 12, 2005, available at <http://www.lexisnexis.com/about/releases/0789.asp>.
21. Paul Roberts , PC World magazine, "Hackers Grab LexisNexis Info on 32,000 People," March 9, 2005, available at <http://www.pcworld.com/article/id,119953-page,1-c,privacylegislation/article.html>.
22. Privacy Rights Clearinghouse, "A Chronology of Breaches," June 30, 2006 (update) <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.
23. Caleb Silver , CNNMoney.com, "LexisNexis acknowledges more ID theft," June 2, 2005, <http://money.cnn.com/2005/04/12/technology/personaltech/lexis/?cnn=yes>.
24. OMB Watch, FedSpending.org, Contracts to LexisNexis 2005-6, available at http://www.fedspending.org/fpds/fpds.php?fiscal_year=2006&company_name=lexisnexis&sortby=r&datatype=T&reptype=r&database=fpds&detail=-1&submit=GO.
25. Honeywell International company website, "Our History," available at <http://www.honeywell.com/sites/honeywell/ourhistory.htm>.
26. OMB Watch, FedSpending.org, Contracts to Honeywell International 2006, available at http://www.fedspending.org/fpds/fpds.php?company_name=honeywell+international&sortby=r&detail=0&datatype=T&reptype=r&database=fpds&fiscal_year=2006&submit=GO.
27. MSNBC, "Superfund lake to be cleaned up," October 16, 2006, available at <http://www.msnbc.msn.com/id/15236965/>.
28. Project on Government Oversight, Federal Contractor Misconduct Database, available at <http://www.pogo.org/db/found.cfm>.
29. Privacy Rights Clearinghouse, "A Chronology of Breaches," February 9, 2006, available at <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.
30. Robert McMillan, IDG News Service Info, "Honeywell blames ex-employee in data leak," February 6, 2006, available at http://www.infoworld.com/article/06/02/06/75111_HNhoneymelldata-leak_1.html.
31. OMBWatch, FedSpending.org, Contracts to Honeywell 2006, available at http://www.fedspending.org/fpds/fpds.php?fiscal_year=2006&company_name=honeywell+international&sortby=r&datatype=T&reptype=r&database=fpds&detail=-1&submit=GO.
32. ChoicePoint company website, Business Solutions, available at www.ChoicePoint.com.
33. ChoicePoint, Annual Report 2006, available at <http://phx.corporate-ir.net/phoenix.zhtml?c=95293&p=irol-reportsannual>.
34. Martin Bosworth, ConsumerAffairs.com, "USA PATRIOT Act Rewards ChoicePoint," May 13, 2005, available at <http://www.consumeraffairs.com/news04/2005/patriot01.html>.
35. Electronic Privacy Information Center "ChoicePoint," available at <http://www.epic.org/privacy/choicepoint/>.
36. ChoicePoint's Annual Reports, available at <http://phx.corporate-ir.net/phoenix.zhtml?c=95293&p=irol-reportsannual>.
37. Federal Trade Commission, Press Release: "ChoicePoint Settles Data Security Breach Charges; to Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress," January 26, 2006, available at <http://www.ftc.gov/opa/2006/01/choicepoint.shtm>.
38. California Department of Consumer Affairs, Office of Privacy Protection, "Recommended Practices

on Notice of Security Breach Involving Personal Information,” February 2007, available at <http://www.privacy.ca.gov/recommendations/secbreach.pdf>.

39. Federal Trade Commission, Privacy Initiatives “The Gramm-Leach-Bliley Act”: Safeguards Rule,” available at <http://www.ftc.gov/privacy/privacyinitiatives/safeguards.html>.

40. ChoicePoint company website, Privacy at ChoicePoint, available at <http://www.privacyatchoicepoint.com/>.

41. Harry Weber, Honolulu Star Bulletin, “677 People Possibly Victimized in Breach,” February 22, 2005, available at <http://starbulletin.com/2005/02/22/business/story2.html>.

42. Associated Press, “ChoicePoint suffered previous breach,” March 2, 2005, available at <http://www.msnbc.msn.com/id/7065902/>.

43. Federal Trade Commission, Press Release: “ChoicePoint Settles Data Security Breach Charges; to Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress,” January 26, 2006, available at <http://www.ftc.gov/opa/2006/01/choicepoint.shtm>.

44. Federal Trade Commission, Press Release: “ChoicePoint Settles Data Security Breach Charges; to Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress,” January 26, 2006, available at <http://www.ftc.gov/opa/2006/01/choicepoint.shtm>.

45. OMB Watch, FedSpending.org, Contracts to ChoicePoint 2005, available at http://www.fedspending.org/fpds/fpds.php?reptype=r&detail=-1&sortby=f&datatype=T&reptype=r&database=fpds&database=fpds&parent_id=58295&fiscal_year=2005&record_num=f500.

46. OMB Watch, Fedspending.org, Contracts to ChoicePoint 2006, available at http://www.fedspending.org/fpds/fpds.php?parent_

47. KBR company website, “About KBR,” available

at <http://www.kbr.com/corporate/index.aspx>

48. William H. Reed, Director of Defense Contract Audit Agency, testimony before House Committee on Government Reform, June 9, 2004 available at http://www.contractormisconduct.org/ass/contractors/29/cases/331/246/dcaa_testimony.pdf.

49. Project on Government Oversight, Federal Contractor Misconduct. “Halliburton -- Excessive Subcontract Costs,” available at <http://www.contractormisconduct.org/index.cfm/1,73,222,html?CaseID=331>.

50. Linda Kozaryn, American Forces Information Service, U.S. Department of Defense, “Defense Auditors Investigate Potential KBR Overcharges,” December 11, 2003, available at <http://www.contractormisconduct.org/ass/contractors/29/cases/341/549/dod-pr.pdf>.

51. Halliburton, Press Release: “Halliburton Subsidiary Wins Follow-on Oil Contract in Iraq” January 16, 2004, available at http://www.halliburton.com/news/archive/2004/corpnws_011604.jsp.

52. OMB Watch, Fedspending.org, Contracts to Fluor Corporation 2006, available at http://www.fedspending.org/fpds/fpds.php?parent_id=106273&sortby=u&detail=-1&datatype=T&reptype=r&database=fpds&fiscal_year=2001&submit=GO.

53. Lawrence, Arenella and Satija LLP, Press Release: “Austin Law Firm Lawrence, Arenella, and Satija Wins Multimillion Dollar Settlement in ‘Whistle Blower’ Case,” November 7 2005, available at <http://www.contractormisconduct.org/ass/contractors/25/cases/87/87/attorney-pr.pdf>.

54. United States Attorney John Gordon, Press Release: “Fluor Daniel Agrees to Pay \$8.2 Million to Resolve Charges that it Overbilled on Government Contracts,” May 7, 2001, available at <http://www.contractormisconduct.org/ass/contractors/25/cases/91/93/usao-pr.pdf>.

55. OMB Watch, Fedspending.org, Contracts to Fluor Corporation 2002, available at http://www.fedspending.org/fpds/fpds.php?parent_id=106273&

sortby=u&detail=-1&datatype=T&reptype=r&database=fpds&fiscal_year=2002&submit=GO.

56. Federal Acquisition Regulation 9.104-1 sections c and d, available at http://www.arnet.gov/far/current/html/Subpart%209_1.html#wp1084058

57. General Electric, Annual Report 2006, available at http://www.ge.com/ar2006/cfs_e.htm.

58. OMB Watch, Fedspending.org, Contracts to General Electric 2006, available at http://www.fedspending.org/fpds/fpds.php?database=fpds&reptype=r&detail=-1&sortby=a&datatype=T&parent_id=113546&fiscal_year=2006.

59. Andrew Wolfson, Louisville Courier-Journal, "GE Plant is Assailed in Inquiry," January 26, 2005, available at <http://66.98.181.12/newsources/Feb0105b.htm>.

60. Department of Justice, Press Release: "GE & Two Subcontractors Pay \$11.5 Million to Resolve Allegations of Selling Defective Aircraft Parts to Defense Department," July 21, 2006, available at <http://www.contractormisconduct.org/ass/contractors/27/cases/437/172/doj-pr.pdf>.

61. GE Aviation, Press Release: "GE F414 Powers First Flight of F/A-18/F, Ahead of Schedule," November 30, 1995, available at http://www.geae.com/aboutgeae/presscenter/military/military_19951130.html

62. GE Aviation, Press Release: "GE Rolls-Royce Fighter Engine Team Awarded \$2.4 Billion Engine Development Contract," August 22, 2005 http://www.geae.com/aboutgeae/presscenter/military/military_20050822.html.

63. Andrew Wolfson, Louisville Courier-Journal, "GE Plant is Assailed in Inquiry," January 26, 2005, available at <http://66.98.181.12/newsources/Feb0105b.htm>.

64. Raytheon company website, "About Us," available at <http://www.raytheon.com/about/>

65. Raytheon, Annual Report, 2006, available at http://media.corporate-ir.net/media_files/irol/84/84193/reports/raytheon_AR2006/index.html.

66. Project on Government Oversight, Federal Contractor Misconduct Database, "Raytheon -- F-14 and F-15 Aircraft Contract False Claims Act Violations" available at <http://www.contractormisconduct.org/index.cfm/1,73,222,html?CaseID=209>.

67. Donald Mancuso, Deputy Inspector General, Department of Defense. "Semiannual Report to the Congress," October 1, 1999 to March 1 2000, available at <http://www.contractormisconduct.org/ass/contractors/46/cases/209/499/20001sar.pdf>.

68. Department of Justice, Press Release: "Hughes Aircraft Pays \$4.05 Million to Settle Fraud Case," September 10, 1996, available at <http://www.contractormisconduct.org/ass/contractors/46/cases/213/505/436civ.pdf>.

69. Bowyer, Kevin, University of South Florida, "Goodearl and Aldred Versus Hughes Aircraft: A Whistle-Blowing Case Study," 2000, available at <http://www.cse.nd.edu/~kwb/nsf-ufe/1043.pdf>.

70. OMB Watch, Fedspending.org, Contracts to Raytheon 2001, available at http://www.fedspending.org/fpds/fpds.php?parent_id=234436&sortby=u&detail=-1&datatype=T&reptype=r&database=fpds&fiscal_year=2001&submit=GO.

71. Northrop Grumman, Annual Report, 2006, available at http://media.corporate-ir.net/media_files/irol/11/112386/reports/NOC_AR_06.pdf.

72. Project on Government Oversight, Federal Contractor Misconduct Database, available at <http://www.contractormisconduct.org/index.cfm/1,73,221,html?ContractorID=42>.

73. Department of Justice, Press Release: "Northrop Grumman to Pay \$80 Million for Overcharging the U.S. and Selling Defective Military Equipment to the Navy," August 20, 2003, available at http://www.contractormisconduct.org/ass/contractors/42/cases/190/452/03_civ_465.pdf.

74. Department of Justice, Press Release: "Northrop Grumman to Pay \$80 Million for Overcharging the U.S. and Selling Defective Military Equipment to the Navy," August 20, 2003, available at http://www.contractormisconduct.org/ass/contractors/42/cases/190/452/03_civ_465.pdf.

tors/42/cases/190/452/03_civ_465.pdf.

75. Defense Industry Daily, "\$24M for 60 Target Drones," march 29, 2000, available at <http://www.defenseindustrydaily.com/24m-for-60-aerial-target-drones-0249/>.

76. OMB Watch, Fedspending.org, Contracts to Northrop Grumman Corp 2006, available at http://www.fedspending.org/fpds/fpds.php?fiscal_year=2006&parent_id=205567&sortby=a&datatype=T&reptype=r&database=fpds&detail=-1&submit=GO.