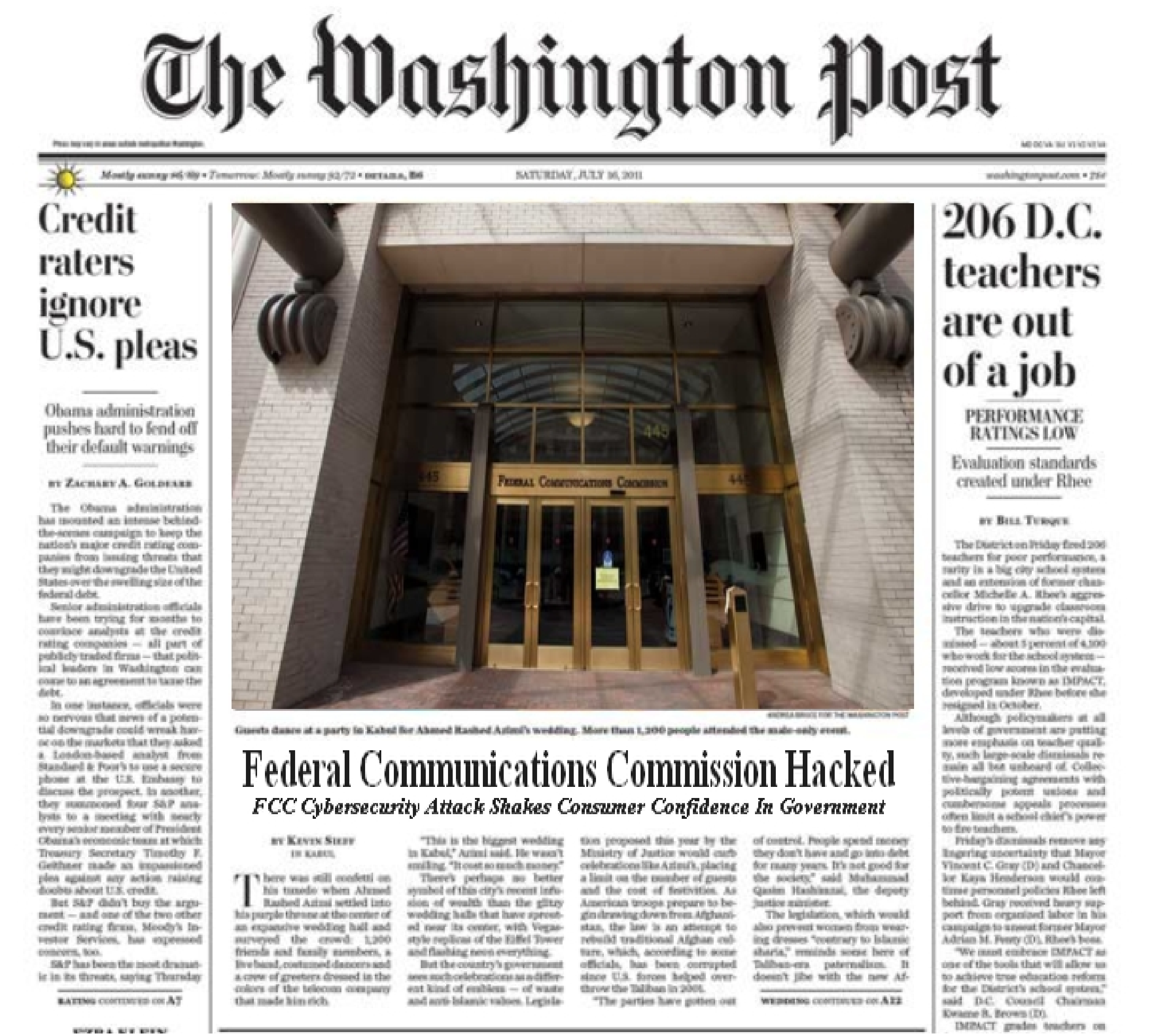
Federal Communications Commission
Cyber Security
Executive Update

July 25, 2011



The Washington Post

[illegible]

[illegible]

Mostly sunny 86/69 • *Tomorrow: Mostly sunny 92/72* • DETAILS, B6

SATURDAY, JULY 16, 2011

washingtonpost.com • *75¢*

Credit raters ignore U.S. pleas

Obama administration pushes hard to fend off their default warnings

BY ZACHARY A. GOLDFARB

The Obama administration has mounted an intense behind-the-scenes campaign to keep the nation's major credit rating companies from issuing threats that they might downgrade the United States over the swelling size of the federal debt.

Senior administration officials have been trying for months to convince analysts at the credit rating companies — all part of publicly traded firms — that political leaders in Washington can come to an agreement to tame the debt.

In one instance, officials were so nervous that news of a potential downgrade could wreak havoc on the markets that they asked a London-based analyst from Standard & Poor's to use a secure phone at the U.S. Embassy to discuss the prospect. In another, they summoned four S&P analysts to a meeting with nearly every senior member of President Obama's economic team at which Treasury Secretary Timothy F. Geithner made an impassioned plea against any action raising doubts about U.S. credit.

But S&P didn't buy the argument — and one of the two other credit rating firms, Moody's Investor Services, has expressed concern, too.

S&P has been the most dramatic in its threats, saying Thursday

RATING CONTINUED ON A7

EZRA KLEIN

ANDREA BRUCE FOR THE WASHINGTON POST

Guests dance at a party in Kabul for Ahmed Rashed Azimi's wedding. More than 1,200 people attended the male-only event.

Federal Communications Commission Hacked

FCC Cybersecurity Attack Shakes Consumer Confidence In Government

BY KEVIN SIEFF
IN KABUL

There was still confetti on his tuxedo when Ahmed Rashed Azimi settled into his purple throne at the center of an expansive wedding hall and surveyed the crowd: 1,200 friends and family members, a live band, costumed dancers and a crew of greeters dressed in the colors of the telecom company that made him rich.

"This is the biggest wedding in Kabul," Azimi said. He wasn't smiling. "It cost so much money."

There's perhaps no better symbol of this city's recent infusion of wealth than the glitzy wedding halls that have sprouted near its center, with Vegas-style replicas of the Eiffel Tower and flashing neon everything.

But the country's government sees such celebrations as a different kind of emblem — of waste and anti-Islamic values. Legislation proposed this year by the Ministry of Justice would curb celebrations like Azimi's, placing a limit on the number of guests and the cost of festivities. As American troops prepare to begin drawing down from Afghanistan, the law is an attempt to rebuild traditional Afghan culture, which, according to some officials, has been corrupted since U.S. forces helped overthrow the Taliban in 2001.

"The parties have gotten out of control. People spend money they don't have and go into debt for many years. It's not good for the society," said Muhammad Qasim Hashimzai, the deputy justice minister.

The legislation, which would also prevent women from wearing dresses "contrary to Islamic sharia," reminds some here of Taliban-era paternalism. It doesn't jibe with the new Af-

WEDDING CONTINUED ON A22

206 D.C. teachers are out of a job

PERFORMANCE RATINGS LOW

Evaluation standards created under Rhee

BY BILL TURQUE

The District on Friday fired 206 teachers for poor performance, a rarity in a big city school system and an extension of former chancellor Michelle A. Rhee's aggressive drive to upgrade classroom instruction in the nation's capital.

The teachers who were dismissed — about 5 percent of 4,200 who work for the school system — received low scores in the evaluation program known as IMPACT, developed under Rhee before she resigned in October.

Although policymakers at all levels of government are putting more emphasis on teacher quality, such large-scale dismissals remain all but unheard of. Collective-bargaining agreements with politically potent unions and cumbersome appeals processes often limit a school chief's power to fire teachers.

Friday's dismissals remove any lingering uncertainty that Mayor Vincent C. Gray (D) and Chancellor Kaya Henderson would continue personnel policies Rhee left behind. Gray received heavy support from organized labor in his campaign to unseat former Mayor Adrian M. Fenty (D), Rhee's boss.

"We must embrace IMPACT as one of the tools that will allow us to achieve true education reform for the District's school system," said D.C. Council Chairman Kwame R. Brown (D).

IMPACT grades teachers on

That Newspaper Headline Could Happen At Anytime!

Is this the legacy we want?

Agenda

- Introductions
  - Chief Information Officer (CIO) – Robert B. Naylor
  - Chief Information Security Officer (CISO) – Phillip Ferraro
- Information Technology Approach
- What is Cyber Security?
- Cyber Security State of the Union
- 2011 Major Attacks and Breeches in the News
- Meet the Hackers
- What about FCC – Are We At Risk?
- What are the Risks for FCC?
- FCC CIO and CISO Activities Since April 2011
- FCC Cyber Security Vision
- The “Plan”
- FISMA – Federal Information Security Management Act 2002
- Conclusion

Introductions

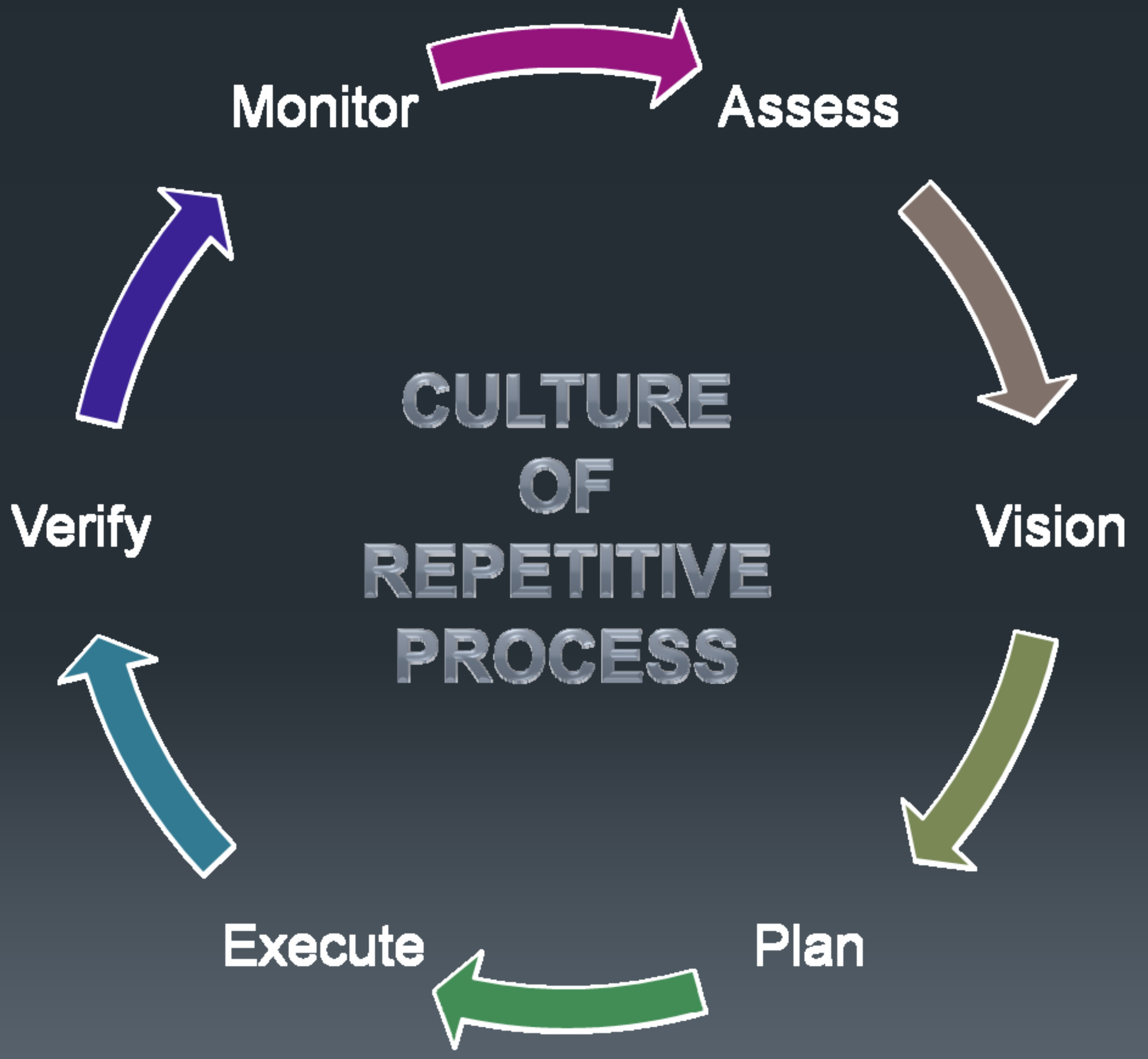
CIO - Robert B. Naylor

- Chief Information Officer for 25 Years
- Small International Business Owner for 10 Years
- International Security Consultant
  - Network Assessments
  - Check Point Firewall Implementations
  - RSA SecurID Two Factor Authentication
  - Intrusion Detection/Prevention Systems (IDS/IPS)
  - Web Monitoring/Blocking/Protection Deployments
- CIO and Chief Privacy Officer for the US Small Business Administration (SBA)
- Executive CIO Council
  - Co-Chair of the IT Workforce Committee
  - CIO Council 5 Years Strategic Goal Committee
  - Cyber Security Staff/Skill Development
  - Collaboration with 14 Federal CIO's and IG's
  - Presented to the United Nations Under Secretary General and CIO
- White House Committees
  - International Data Research Policy
  - Ideation / Social Media Committee (OSTP)
- IT and Security Auditing Background – Tracking/Accountability
  - Sarbanes-Oxley Internal Corporate Auditor
  - Closed 450 Audits at SBA within 8 Months
  - Created Audit Tracking and Accountability System - 13 Agencies Interested

CISO – Phillip Ferraro

- Federal Communications Commission Chief Information Security Officer Since June 2010
  - Published FCC Directive 1479.4 *FCC Cyber Security Program*
  - Re-wrote all FCC Cyber Security Policies (Interim Policy Published July 2011)
  - Certified and Accredited FCCNet (First Time Since 2004)
  - Refocused FCC Efforts on Mitigating FISMA Findings
- Department of Defense - United States Army, Europe Chief Information Security Officer
  - Secured Hundreds of Networks and Over 50,000 Users Across Europe
- DOD - United States Southern Command Chief Information Security Officer
  - First CISO at USSOUTHCOM – Developed Cyber Security Program from Inception
  - FISMA Rating from the Lowest of Fifteen Combatant Commands, Services, and Agencies to the Highest Rating Possible in One Year.
- Director of Network Security – Corporate Insurance Industry
- International Security Consultant – (USAID, FedEx, Fischbach, Louis Berger)
- U.S. Army Special Forces
- FISMA, HIPAA, SEC, and Government Regulatory Requirements Experience
- Certifications Include:
  - Certified Information Systems Security Professional (CISSP)
  - Certified Information Security Manager (CISM)
  - Certified Ethical Hacker (CEH)
  - Cisco Certified Network Associate (CCNA)
  - Checkpoint Certified Security Engineer (CCSE)
  - Microsoft Certified Security Engineer (MCSE)

Information Technology Approach



What is Cyber Security?

Cyber security refers to preventative methods to protect information from attacks and unauthorized access, modification, or destruction. It requires an understanding of potential information threats, e.g., viruses, denial of service, and malicious code. Cyber security strategies include identity management, risk management and incident management.

Security is the ability of a system to protect information and system resources with respect to confidentiality and integrity.

Cyber Security State of the Union

- President Obama Makes Cyber Security an Administration Priority; Describing the growing number of attacks on our cyber networks as “one of the most serious economic and national security threats our nation faces.”

- Both the House and Senate Recognize Need for New Cyber Security Legislation

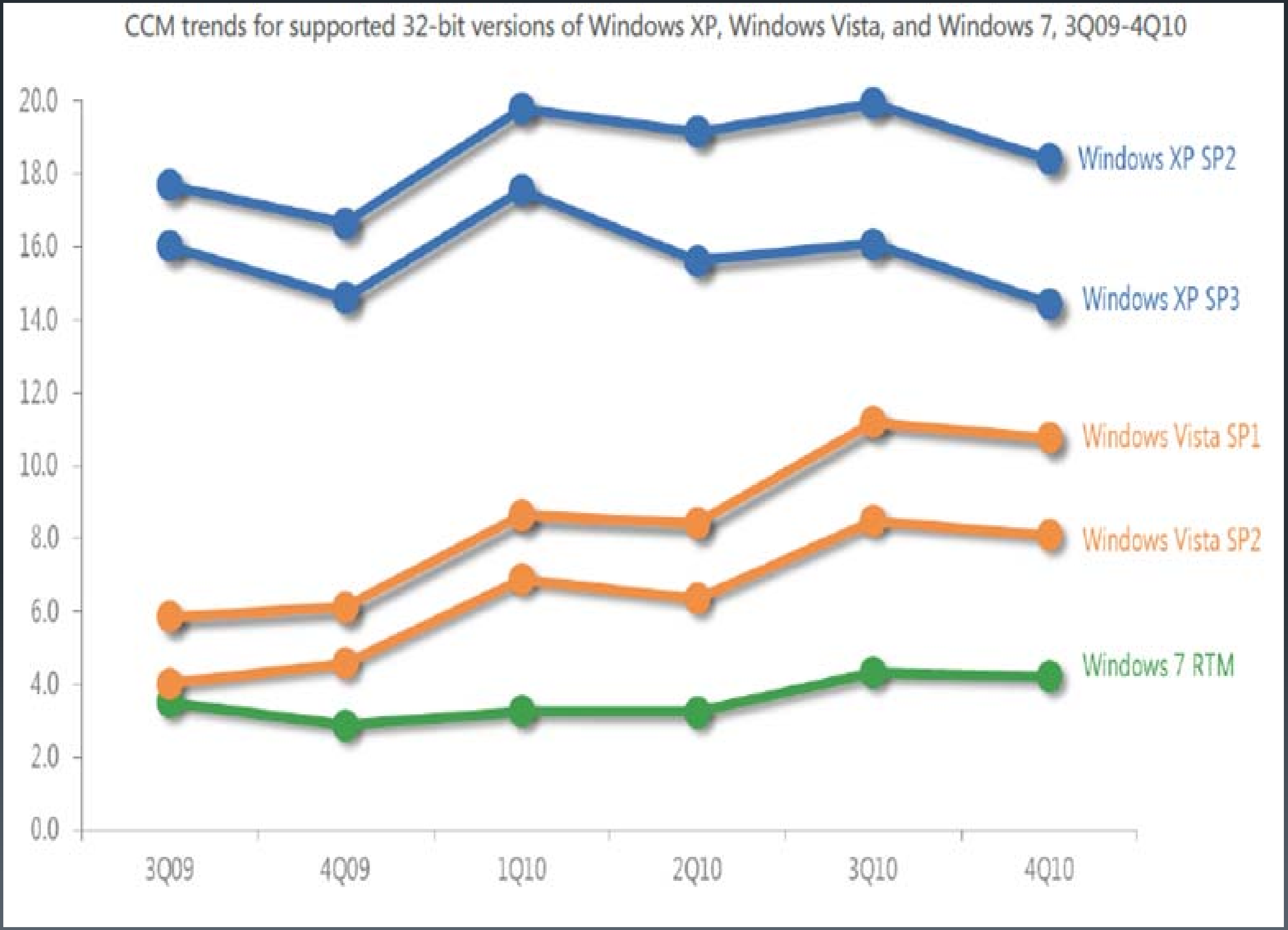
- FCC Promotes Cyber Security on May 18, 2011,
  Chairman Genachowski Held the Cyber Security Roundtable:
  Protecting Small Businesses

- 2011 Shows a Significant Increase in Cyber Security Attacks;
  Particularly on US Government Sites (Including Government Contractors and Affiliates)

- The Department of Defense (DoD) Detects Three Million Unauthorized “Scans” or “Attempts” to Access Official Networks Everyday

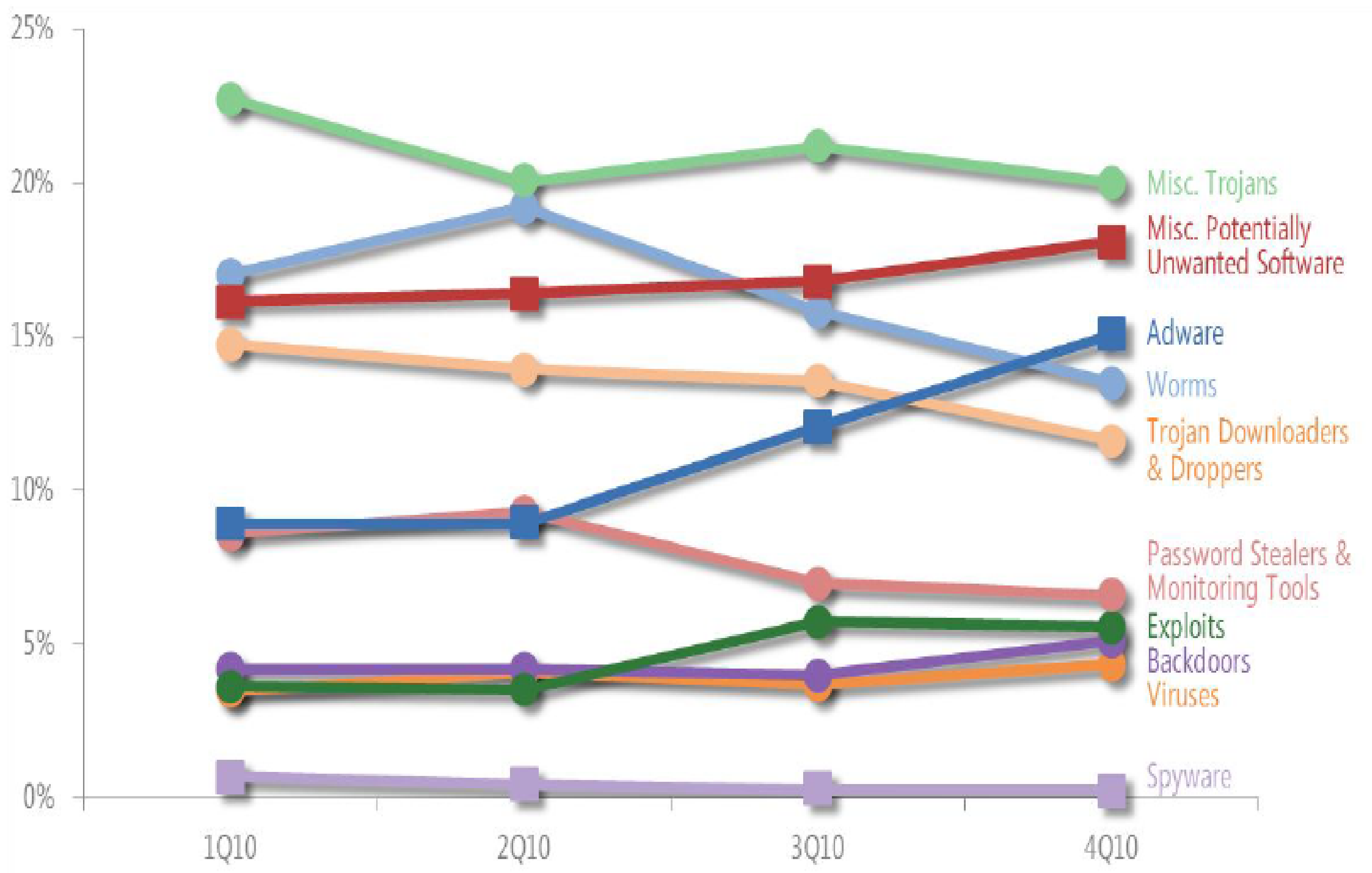
- Department of Homeland Security (DHS) Recorded Over 37,000 Attempted Breaches on Government and Private Systems as well as Over 80,000 Attacks on Systems within the Pentagon Per Year, Approximately Doubling Each Year Since 2008

Security Threat Assessment



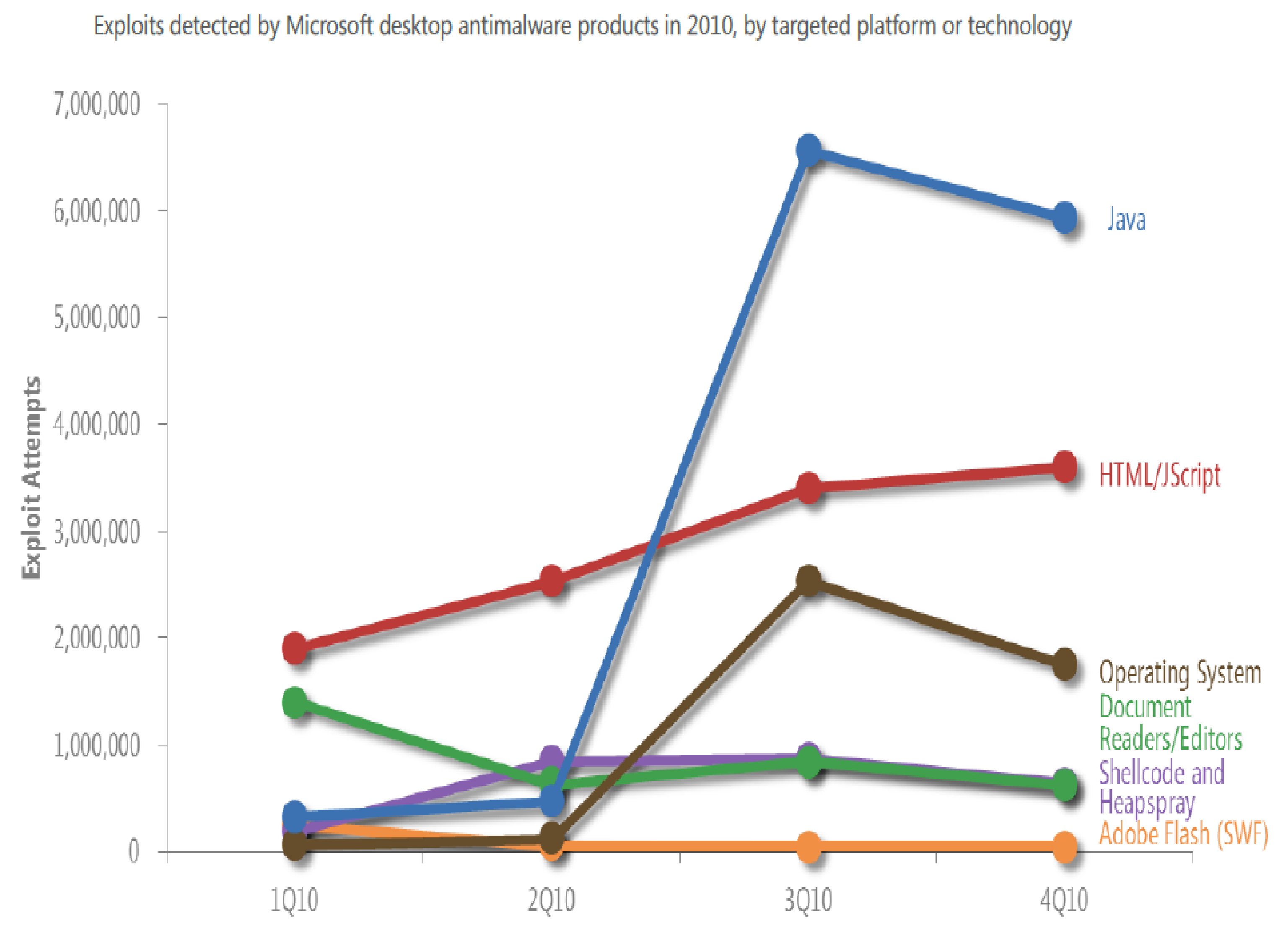
Security Threat Assessment

Detections by threat category each quarter in 2010, by percentage of all computers reporting detections



Round markers indicate malware categories; square markers indicate potentially unwanted software categories.

Security Threat Assessment



2011 Major Attacks and Breeches in the News

January 21 - U.S. Army’s Communications-Electronic Command

February 5 – NASDAQ OMX Networks

February 22 – Voice of America

March 3 and April 13 – WordPress

March 17 – RSA Security

March 24 – Trip Advisor

March 29 – Australian Parliament

2011 Major Attacks and Breeches in the News

April 4 – April 25 – May 5 – July 5 – Sony and PlayStation

April 17 – Department of Energy - Oak Ridge National Laboratory

April 25 – New York Yankees

May 13 – July 4 – Fox Broadcasting Company

May 17 – NASA

May 27 – Lockheed Martin

May 29 – Public Broadcasting Service

2011 Major Attacks and Breeches in the News

June 1 – Google Mail

June 1 – L3 Communications

June 3 – InfraGard (FBI affiliate)

June 6 – Nintendo

June 9 – Citigroup

2011 Major Attacks and Breeches in the News

June 13 – United States Senate

June 15 – Central Intelligence Agency (CIA)

June 17 – Sega

June 25 – Brazilian Government Sites

June 26 and 27 – The Washington Post

2011 Major Attacks and Breeches in the News

DEPARTMENT OF PUBLIC SAFETY ARIZONA

June 27 – Arizona Department of Public Safety

July 4 – Apple (iTunes)

Microsoft

July 4 – Microsoft Brazil

Booz | Allen | Hamilton
delivering results that endure

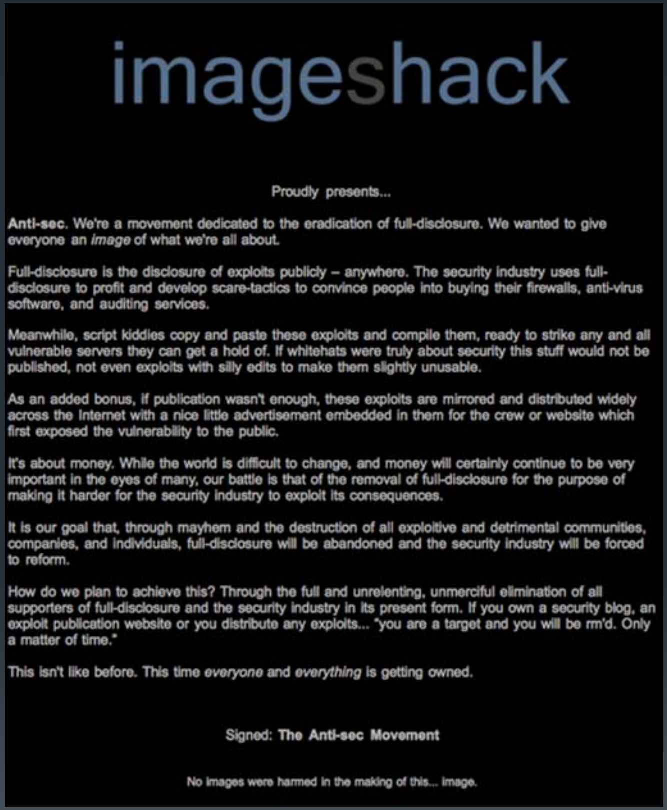
July 12 – Booz Allen Hamilton

Meet The Hackers

Known Major Hacking Organizations:

LulzSec

Anonymous



Proudly presents...

Anti-sec. We're a movement dedicated to the eradication of full-disclosure. We wanted to give everyone an *image* of what we're all about.

Full-disclosure is the disclosure of exploits publicly – anywhere. The security industry uses full-disclosure to profit and develop scare-tactics to convince people into buying their firewalls, anti-virus software, and auditing services.

Meanwhile, script kiddies copy and paste these exploits and compile them, ready to strike any and all vulnerable servers they can get a hold of. If whitehats were truly about security this stuff would not be published, not even exploits with silly edits to make them slightly unusable.

As an added bonus, if publication wasn't enough, these exploits are mirrored and distributed widely across the Internet with a nice little advertisement embedded in them for the crew or website which first exposed the vulnerability to the public.

It's about money. While the world is difficult to change, and money will certainly continue to be very important in the eyes of many, our battle is that of the removal of full-disclosure for the purpose of making it harder for the security industry to exploit its consequences.

It is our goal that, through mayhem and the destruction of all exploitive and detrimental communities, companies, and individuals, full-disclosure will be abandoned and the security industry will be forced to reform.

How do we plan to achieve this? Through the full and unrelenting, unmerciful elimination of all supporters of full-disclosure and the security industry in its present form. If you own a security blog, an exploit publication website or you distribute any exploits... "you are a target and you will be rm'd. Only a matter of time."

This isn't like before. This time *everyone* and *everything* is getting owned.

Signed: **The Anti-sec Movement**

No images were harmed in the making of this... image.

Anti-Sec Movement

Goatse Security

Meet The Hackers

James was the first juvenile to be sent to prison for hacking. He was sentenced at 16 years old. In a PBS interview, he professed, "I was just looking around, playing around. What was fun for me was a challenge to see what I could pull off."

James's major intrusions targeted high-profile organizations. He installed a backdoor into a **Defense Threat Reduction Agency** server. The DTRA is an agency of the **Department of Defense** charged with reducing the threat to the U.S. and its allies from nuclear, biological, chemical, conventional and special weapons. The backdoor he created enabled him to view sensitive emails and capture employee usernames and passwords.

James also cracked into **NASA** computers, stealing software worth approximately $1.7 million. According to the Department of Justice, "The software supported the International Space Station's physical environment, including control of the temperature and humidity within the living space." **NASA** was forced to shut down its computer systems, ultimately racking up a $41,000 cost.

Jonathan James

Meet The Hackers

Lamo's claim to fame is his break-ins at major organizations like The New York Times and Microsoft. Dubbed the "homeless hacker," he used Internet connections at Kinko's, coffee shops and libraries to do his intrusions. In a profile article, "He Hacks by Day, Squats by Night," Lamo reflects, "I have a laptop in Pittsburgh, a change of clothes in D.C. It kind of redefines the term multi-jurisdictional."

Lamo's intrusions consisted mainly of penetration testing, in which he found flaws in security, exploited them and then informed companies of their shortcomings. His hits include Yahoo!, Bank of America, Citigroup and Cingular. When he broke into The New York Times' intranet, things got serious. He added himself to a list of experts and viewed personal information on contributors, including Social Security numbers. Lamo also hacked into The Times' LexisNexis account to research high-profile subject matter.

Adrian Lamo

Meet The Hackers

The Department of Justice describes Kevin Mitnick as "the most wanted computer criminal in United States history." He started out exploiting the Los Angeles bus punch card system to get free rides. Then, like Apple co-founder Steve Wozniak, dabbled in phone phreaking. Although there were numerous offenses, Mitnick was ultimately convicted for breaking into the Digital Equipment Corporation's computer network and stealing software.

Mitnick's mischief got serious when he went on a two and a half year "coast-to-coast hacking spree." The CNN article, "Legendary computer hacker released from prison," explains that "he hacked into computers, stole corporate secrets, scrambled phone networks and broke into the **national defense warning system**." He then hacked into computer expert and fellow hacker Tsutomu Shimomura's home computer, which led to his undoing.

Kevin Mitnick

Meet The Hackers

Also known as Dark Dante, Poulsen gained recognition for his hack of LA radio's KIIS-FM phone lines. Law enforcement dubbed him "the Hannibal Lecter of computer crime."

Authorities began to pursue Poulsen after he hacked into a federal investigation database. During this pursuit, he further drew the ire of the **FBI** by hacking into federal computers for wiretap information.

His hacking specialty, however, revolved around telephones. Poulsen's most famous hack, KIIS-FM, was accomplished by taking over all of the station's phone lines. In a related feat, Poulsen also "reactivated old Yellow Page escort telephone numbers for an acquaintance who then ran a virtual escort agency." Later, when his photo came up on the show Unsolved Mysteries, 1-800 phone lines for the program crashed.

Kevin Poulsen

Meet The Hackers

Morris, son of former National Security Agency scientist Robert Morris, is known as the creator of the Morris Worm, the first computer worm to be unleashed on the Internet. As a result of this crime, he was the first person prosecuted under the 1986 Computer Fraud and Abuse Act.

Morris wrote the code for the worm while he was a student at Cornell. He asserts that he intended to use it to see how large the Internet was. The worm, however, replicated itself excessively, slowing computers down so that they were no longer usable. It is not possible to know exactly how many computers were affected, but experts estimate an impact of 6,000 machines.

Robert Tappan Morris

Meet The Hackers

Scottish-born, London-based hacker McKinnon (aka Solo) wasn't just in it for fun; he had a political axe to grind.

Conspiracy-theorist McKinnon broke into computers at the **U.S. Department of Defense**, **Army**, **Navy**, **Air Force** and **NASA** sometime in 2001 and 2002. What exactly was he looking for? Evidence of really fuel-efficient alien spacecraft, for one.

McKinnon believes the U.S. government was hiding alien technology that could solve the global energy crisis. Now, in the process of snooping around for this stuff, the self-taught hacker concedes he may have deleted a whole bunch of other files and maybe some hard drives as he attempted to cover up his tracks.

The U.S. government claimed McKinnon's hack job cost them $700,000 to fix. They also kind of doubt the whole UFO story and wonder if his snooping had more earthly intentions. Back in the U.K., Gary's lawyers insist that their client, who suffers from Asperger's Syndrome, deserves special mental health considerations.

Gary McKinnon

Meet The Hackers

In 2002, the Deceptive Duo (20-year-old Benjamin Stark and 18-year-old Robert Lyttle) were responsible for a series of high-profile break-ins to government networks, including the **U.S. Navy**, **NASA**, **FAA** and **Department of Defense**.

Like so many other hackers, California-based Lyttle and Florida-based Stark, claimed they were merely trying to expose security failures and protect Americans in a post-911 world. The two hackers posted messages, left email addresses and defaced Web sites in an attempt to get the government's attention...and get the government's attention, they did.

Benjamin Stark

Robert Lyttle

Meet The Hackers

Ryan Cleary

June 2011, a suspected hacker has been charged with attacking Britain's biggest agency fighting organized crime.

Ryan Cleary, 19, also faces up to 70 years behind bars in the US if he is extradited and found guilty of hacking sites there. He is believed to be responsible for the **CIA**, **US Senate**, and **Sony** hacking over the past few months.

Police sources in the UK said the computer geek was arrested in his bedroom allegedly launching a cyber war on the Serious Organized Crime Agency's website.

Meet The Hackers

NEWS OF THE WORLD
THE WORLD'S GREATEST NEWSPAPER 1843-2011
THANK YOU & GOODBYE
RACIS VIDEO SHAME
HARRY AT DRINK AND DRUG BASH
'SELLS' ANDY FOR £500k
TV JAMIE: MY VICE GIRL SHAME
MYLEENE FO ME TO QUIT
HUNTLEY HIS CELL

When we think about hackers, we tend to think of computer “geeks” or sophisticated criminals, we do not usually think that newspaper and television reporters are hacking into systems for privacy information. Today’s reality is that hacking comes from all types of people and organizations.

News International, the publisher of the News of the World, announced on April 8, 2011 that it would admit liability in some of the breach of privacy cases being brought in relation to phone hacking. The company offered an unreserved apology and compensation to eight claimants.

On July 9, 2011, Britain's best-selling Sunday tabloid the News of the World signed off with a simple front page message — "THANK YOU & GOODBYE" — leaving the media establishment in the UK, and now the USA, reeling from the expanding phone-hacking scandal that brought down the muckraking newspaper after 168 years.

What about FCC – Are We At Risk?

Absolutely! We have both physical and reputational risks!

At a recently visited large government organization, who have at least three levels of the best and latest technology security tools analyzing in real-time all in and outbound network traffic, they have a fourth tool which captures and analyzes an average of 10 exploits of malicious traffic (out of thousands of attacks) per day that penetrates their first three layers.

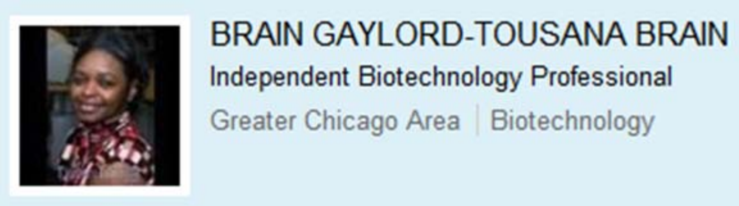
Our defenses are not quite that mature…yet!

Can our data be affected?

Absolutely! A recent COALS event should demonstrate the risk!

Over the past two years, a disgruntled individual (not a hacker by any means) has created well over 24,000 fraudulent FRN's in CORES, over 1,200 entity representative organizations, over 5,700 IBFS filings, and most recently changed the legal names of two large cable providers in COALS.

If a non-hacker can do this, what can a sophisticated attacker do?



BRAIN GAYLORD-TOUSANA BRAIN

Independent Biotechnology Professional

Greater Chicago Area | Biotechnology

FCC Cyber Security SWOT Analysis

STRENGTHS

- Strong Support for Cyber Security from FCC Senior Executives
- New CIO and CISO with Extensive Cyber Security Experience
- Defense in Depth

WEAKNESSES

- Significantly Understaffed
- Cyber Security is Underfunded
- NSOC Aligned Under IT Infrastructure
- Disparate Group of Outdated Security Tools Do Not Provide Real-time, Centralized, Continuous Monitoring of FCC Networks and Systems

OPPORTUNITIES

- Collaboration with Other Government Agencies to Leverage Lessons Learned, New Ideas, Tools, and Best Practices
- Pending Legislation Significantly Increases Agency Head Cyber Security Responsibilities. Excellent Opportunity, as a Model Agency, to Make Positive Program Changes in Advance of the Legislation
- End of Year Funding Can Resolve Many FCC Weaknesses

THREATS

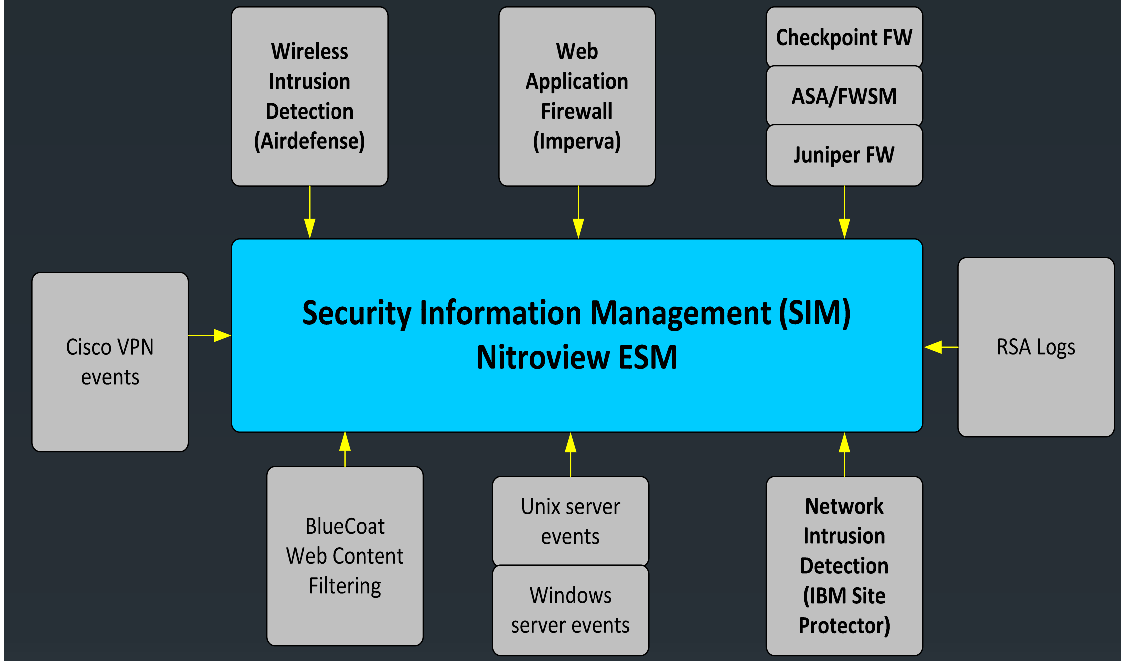
- Status Quo – Not Taking Advantage of Opportunities to Change Weaknesses to Strengths and Improve the Overall FCC Cyber Security Program will Negatively Impact the Agency
- Budget Cuts, Disapproval or Low Prioritization of Cyber Security Unfunded Requirements Will Negatively Impact Our Support of the Agency’s Mission
- Any Cyber Breach Could be Front Page News on the Washington Post, CNN, The Hill, etc., and Permanently Damage the FCC Reputation

What are the Risks for FCC?

- Internal Threats
  - Users, Users, Users
    - Internet Browsing Can Lead to Web-based Drive-by Malware on PC's
      - Recently on the FCC Intranet, in Today's Headlines, there was a link to a Business Week article and the web site was virus infected. We had over 700 hits to that web page.
    - Vulnerable Desktop/Laptop Applications (Adobe Reader, Flash, Java)
    - High Level of Malware Polymorphism/Zero-day Exploits (No Patches Available)
    - Targeted Phishing E-mail (Spear Fishing)
    - E-mail with Attached Malware or Embedded Malicious Links
    - Users Refusing to Complete Mandatory Annual Cyber Security Awareness Training
  - The Insider Threat – Disgruntled Employees – Unauthorized Family Users

- External Threats
  - "Hactivists" Determined to See if the FCC Practices What it Promotes
  - Other Hackers, Nation States, Terrorist, and Cyber Criminals
  - FCC Becomes an Immediate Target When Promoting Cyber Security

Where are we?



Wireless Intrusion Detection (Airdefense)

Web Application Firewall (Imperva)

Checkpoint FW

ASA/FWSM

Juniper FW

Cisco VPN events

Security Information Management (SIM)
Nitroview ESM

RSA Logs

BlueCoat Web Content Filtering

Unix server events

Windows server events

Network Intrusion Detection (IBM Site Protector)

Network Access Control
(Still Secure, *Symantec NAC*)

Network Anomaly Detection
(Riverbed Cascade)

Threat Protection
(Active Scout)

Laptop Disk Encryption
(McAfee Safeboot)

Packet Recorders
(Niksun Netvcr)

Managed Encrypted Thumbdrives
(Ironkey)

Automated Vulnerability Scanning
(Foundstone)

- A Good Set of Tools; However, Only About Half of Our Tools Are Connected to a Central Monitoring System (SIM)
- CIO and CISO Currently Have No Visibility Into the SIM (No Executive-Level FCC Dashboards)
- Limited Personnel Resources Impact Our Ability to Continuously Monitor (12x5 vs. 24x7)
- Does Not Include Patch Management or FISMA Compliance Monitoring Tools
- Several of the Tools are Outdated and Require Hardware and/or Software Upgrades

FCC CIO and CISO Activities Since April 2011

Department of State Visit
•Reviewed Continuous Monitoring Process and Tools
•Received SharePoint Templates (iPost) and Tools

Department of Homeland Security Visit
•Request Blue Team Assessment
•Discussed Networx Transition and Einstein Configuration
•Plan to Move from Intrusion Detection System to Intrusion Prevention System

Department of Veterans Affairs Visit
•Reviewed Continuous Monitoring Process and Tools
•Discussed Return on Investment of Specific Tools

National Security Agency Visit at FCC
•Request Blue Team Assessment
•Discussed NSA and FCC Partnership for Training and Processes
•Plans for CIO and CISO to Attend NSA Security Boot Camp
(2 Weeks of Security Training)

FCC CIO and CISO Activities Since April 2011

U.S. House of Representatives Visit

- Reviewed Continuous Monitoring Process and Tools
- Reviewed Security Operations Support Center
- Collaboration on Security Architecture for FCC

Federal Bureau of Investigations Visit

- Reviewed Microsoft Enterprise Implementation
- Discussed Remote Access, VPN Alternatives and Secured Networks

Microsoft Meetings and Visits

- Attended Security Threat Assessment Briefing and Overview
- Reviewed Existing FCC Microsoft Owned Tools and Architecture

McAfee CTO Meeting at FCC

- Discuss FCC McAfee Tools Already Owned and Future Collaboration

Core Security Technologies Meeting at FCC

- Implemented 90 Evaluation of Impact Program and Enterprise Suite

FireEye Meeting at FCC

- Implemented 90 Evaluation of FireEye Threat Prevention Program

FCC CIO and CISO Activities Since April 2011

- Since April 15, the CIO and CISO Focused Efforts on Improving FCC’s Cyber Security Posture By:
  - Publishing FCC Directive 1479.4, Cyber Security Program
    - Updated FCC Cyber Security Policies (Interim Policy Released July 2011)
  - Developing an FCC Cyber Security Strategic Plan Aligned with the FCC Vision and Mission
  - Conducted Meetings to Review Network Security Vulnerability Assessments of FCC Networks and Systems – 10 Organizations With Multiple Discussions Over 12 Weeks
  - Conducted Detailed Analysis of Current FCC Tools and Security Architecture to Cost-effectively Implement Changes to Better Protect FCC Systems and Data
  - Implemented Web Filtering Agency-wide
  - FCC Field Office Visits – Gettysburg, Pennsylvania and Atlanta, Georgia
  - Collaboration with USAC to Review FISMA Requirements and FCC Security Plans

FCC CIO and CISO Activities Since April 2011

- Installed Audit Tracking and Accountability SharePoint Templates from SBA
- In Process of Creating an IT Audit Tracking Response and Monitoring Team
- CIO Invited to Chair the Cyber Security Panel for the Australian Government at the FutureGOV Congress in Canberra, Australia and Learn from Their Breech Experiences
- CIO and CISO Invited to Lead in the Anti-Phishing Working Group (APWG) - A Non-profit Global Pan-industrial and Law Enforcement Association Focused on Eliminating the Fraud, Crime and Identity Theft That Result from Phishing, Pharming, Malware and E-mail Spoofing of All Types
- CIO Invited to Present FCC Security Vision and Strategy in the Fall 2011 at the NIST Information Security and Privacy Advisory Board (ISPAB)
- Similar to the Veteran Affairs CISO Visit to McAfee, the FCC CIO and CISO Have Been Invited to Meet the McAfee CEO at Their Executive Briefing Center to Conduct a Deep Dive on Global Threat Intelligence – Conducted Similar Meeting at Microsoft

FCC Cyber Security Vision

- The FCC will be a Center of Excellence in Federal Cyber Security
- We will Maintain Ongoing Security Collaboration with Other Agencies
- The FCC will Incorporate and Create Best Practices for Continuous Monitoring and Executive Dashboards
- Cyber Security Personnel will be Cross Trained and Properly Skilled
- FCC will have NO FISMA Findings
- NSA and DHS Blue Team Penetration Testing Results will be Clean
- NSA Red Team Active Attacks will NOT be Successful – Proving that we are Secure
- FCC will Take Leadership Security Roles In the Federal Community

The “Plan”

- CIO and CISO will:
  - Develop a Rapid Response Team
  - Create a 24x7 Security Operations Center (move from Auctions bullpen where there is no central monitoring ability)
  - Update Emergency Contacts and Procedures
  - Continue to Integrate FCC Public Safety (PSHSB)
  - Continue to Work with Other Agencies and Vendor Executives
  - Represent the FCC on Government Cyber Security Boards and Panels
  - Develop and Implement User Training and Awareness Programs
  - Periodically Practice Real Life Breech and Data Integrity Scenarios
  - Acquire and Implement Remaining Industry Standard Security Tools
  - Architect, Configure, and Centralize Security Data Collections
  - Establish Executive and Operational Level Security Dashboards
  - External Testing of Our Security by Certified Experts (NSA, DHS, etc.)

FISMA – Federal Information Security Management Act 2002

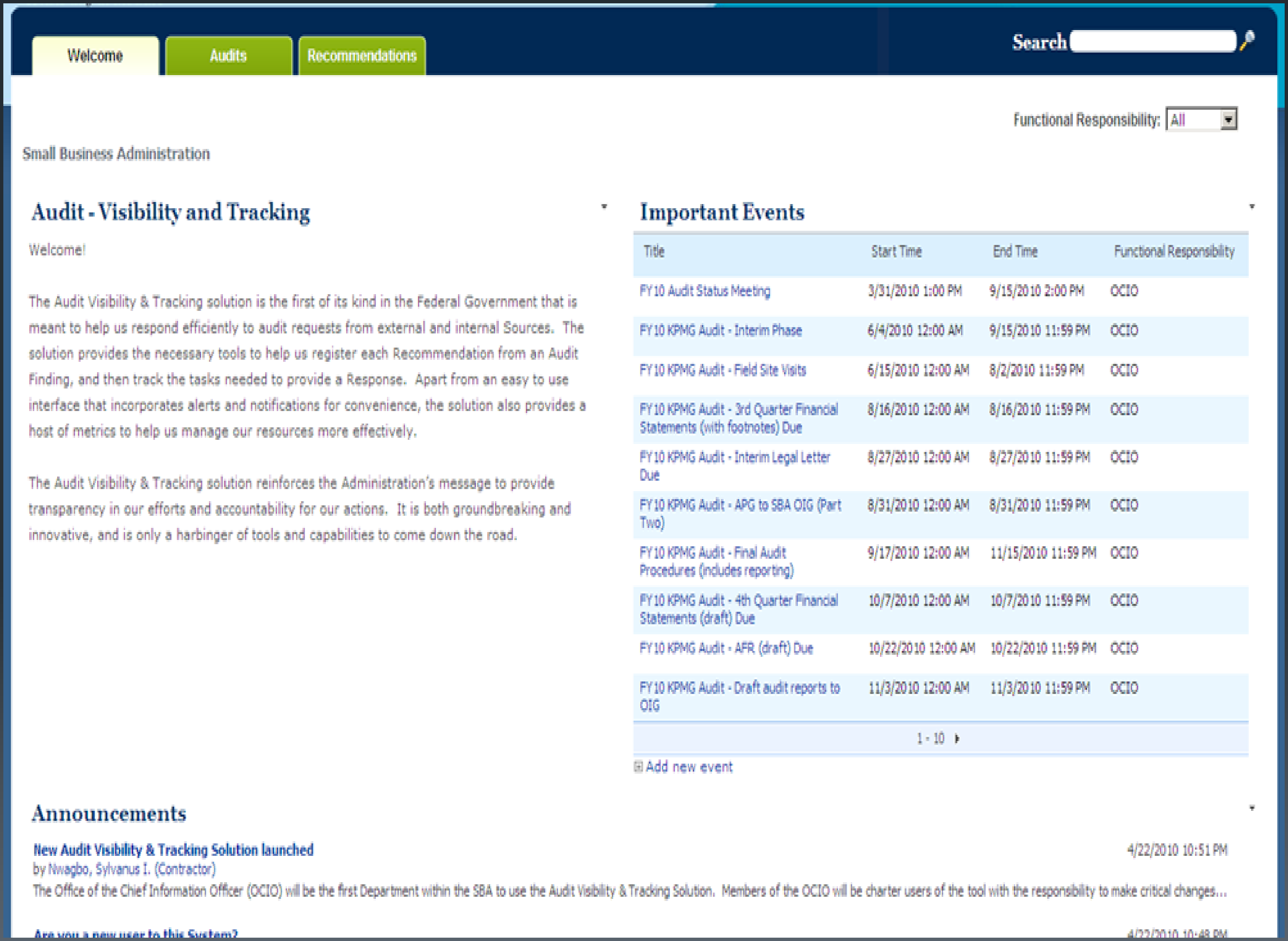
- Although FISMA Compliance is Mandatory, Over the Past Few Years the FCC has Been Slow to Mitigate Audit Findings

- Each year OIG contracts for an independent FISMA audit, and Following the FY2010 Audit, the CISO Developed a Corrective Action Plan (CAP), Mitigating Approximately 50% of the Findings

- At the Start of This Year’s Audit, the Auditors Stated that the FCC Could Receive a Material Weakness Finding, Due to the Large Number of Repeat Findings from Year to Year and the Lack of Progress in Properly Addressing These Findings – Basically IT Process Culture Concerns

- CIO is Implementing Automated Tools to Improve the Tracking and Mitigation of All Audit Findings and is Implementing a Culture Change Within ITC - All Staff Understand the Significance of Cyber Security and the Need to Focus Resources to Mitigate Security Findings

Audit Tracking and Accountability Tools



Functional Responsibility: All

Small Business Administration

Audit - Visibility and Tracking

Welcome!

The Audit Visibility & Tracking solution is the first of its kind in the Federal Government that is meant to help us respond efficiently to audit requests from external and internal Sources. The solution provides the necessary tools to help us register each Recommendation from an Audit Finding, and then track the tasks needed to provide a Response. Apart from an easy to use interface that incorporates alerts and notifications for convenience, the solution also provides a host of metrics to help us manage our resources more effectively.

The Audit Visibility & Tracking solution reinforces the Administration's message to provide transparency in our efforts and accountability for our actions. It is both groundbreaking and innovative, and is only a harbinger of tools and capabilities to come down the road.

Important Events

Title	Start Time	End Time	Functional Responsibility
FY10 Audit Status Meeting	3/31/2010 1:00 PM	9/15/2010 2:00 PM	OCIO
FY10 KPMG Audit - Interim Phase	6/4/2010 12:00 AM	9/15/2010 11:59 PM	OCIO
FY10 KPMG Audit - Field Site Visits	6/15/2010 12:00 AM	8/2/2010 11:59 PM	OCIO
FY10 KPMG Audit - 3rd Quarter Financial Statements (with footnotes) Due	8/16/2010 12:00 AM	8/16/2010 11:59 PM	OCIO
FY10 KPMG Audit - Interim Legal Letter Due	8/27/2010 12:00 AM	8/27/2010 11:59 PM	OCIO
FY10 KPMG Audit - APG to SBA OIG (Part Two)	8/31/2010 12:00 AM	8/31/2010 11:59 PM	OCIO
FY10 KPMG Audit - Final Audit Procedures (includes reporting)	9/17/2010 12:00 AM	11/15/2010 11:59 PM	OCIO
FY10 KPMG Audit - 4th Quarter Financial Statements (draft) Due	10/7/2010 12:00 AM	10/7/2010 11:59 PM	OCIO
FY10 KPMG Audit - AFR (draft) Due	10/22/2010 12:00 AM	10/22/2010 11:59 PM	OCIO
FY10 KPMG Audit - Draft audit reports to OIG	11/3/2010 12:00 AM	11/3/2010 11:59 PM	OCIO

1 - 10 ▸

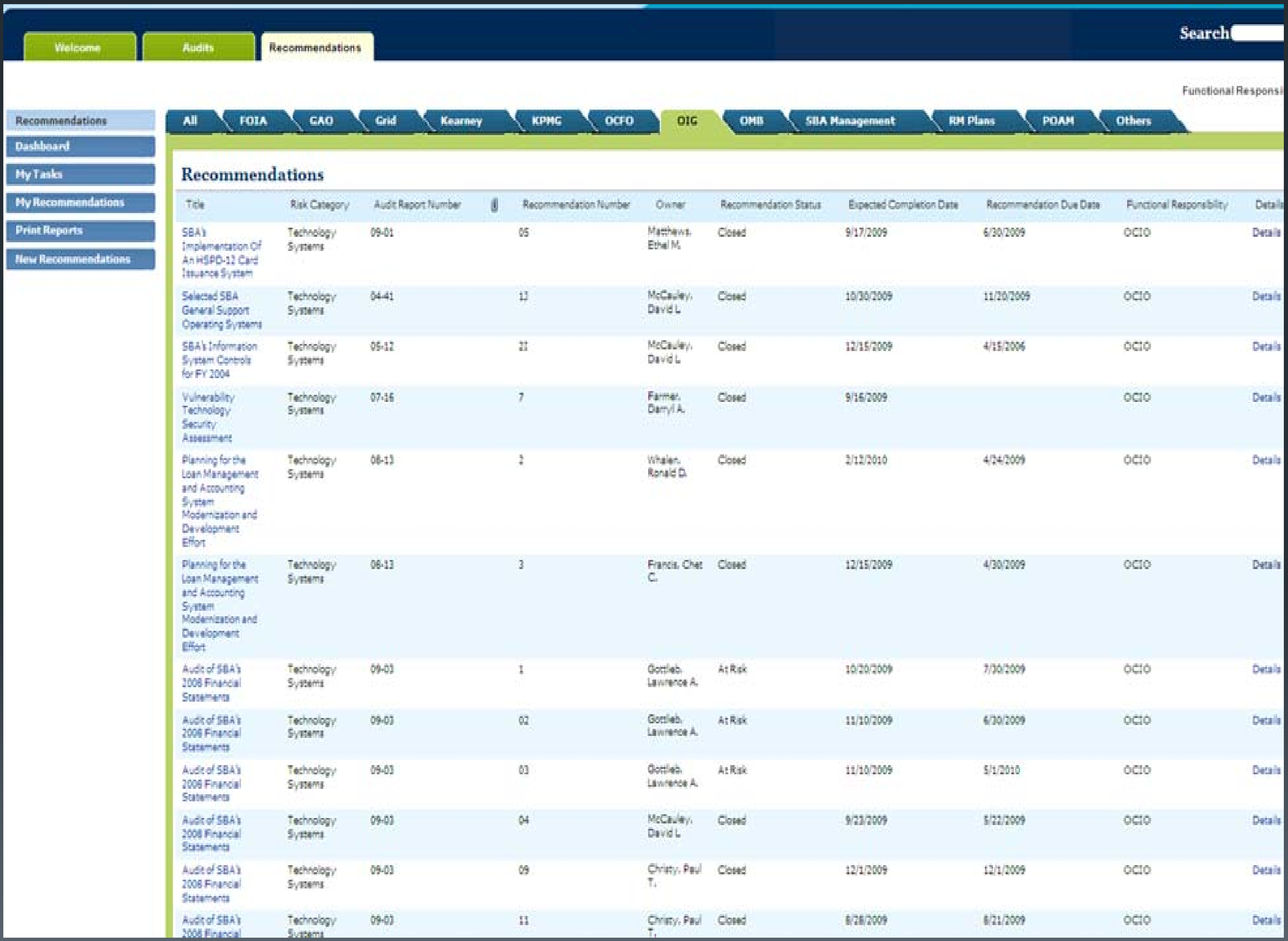
⊞ Add new event

Announcements

New Audit Visibility & Tracking Solution launched 4/22/2010 10:51 PM
by Nwagbo, Sylvanus I. (Contractor)
The Office of the Chief Information Officer (OCIO) will be the first Department within the SBA to use the Audit Visibility & Tracking Solution. Members of the OCIO will be charter users of the tool with the responsibility to make critical changes...

Are you a new user to this System? 4/22/2010 10:48 PM

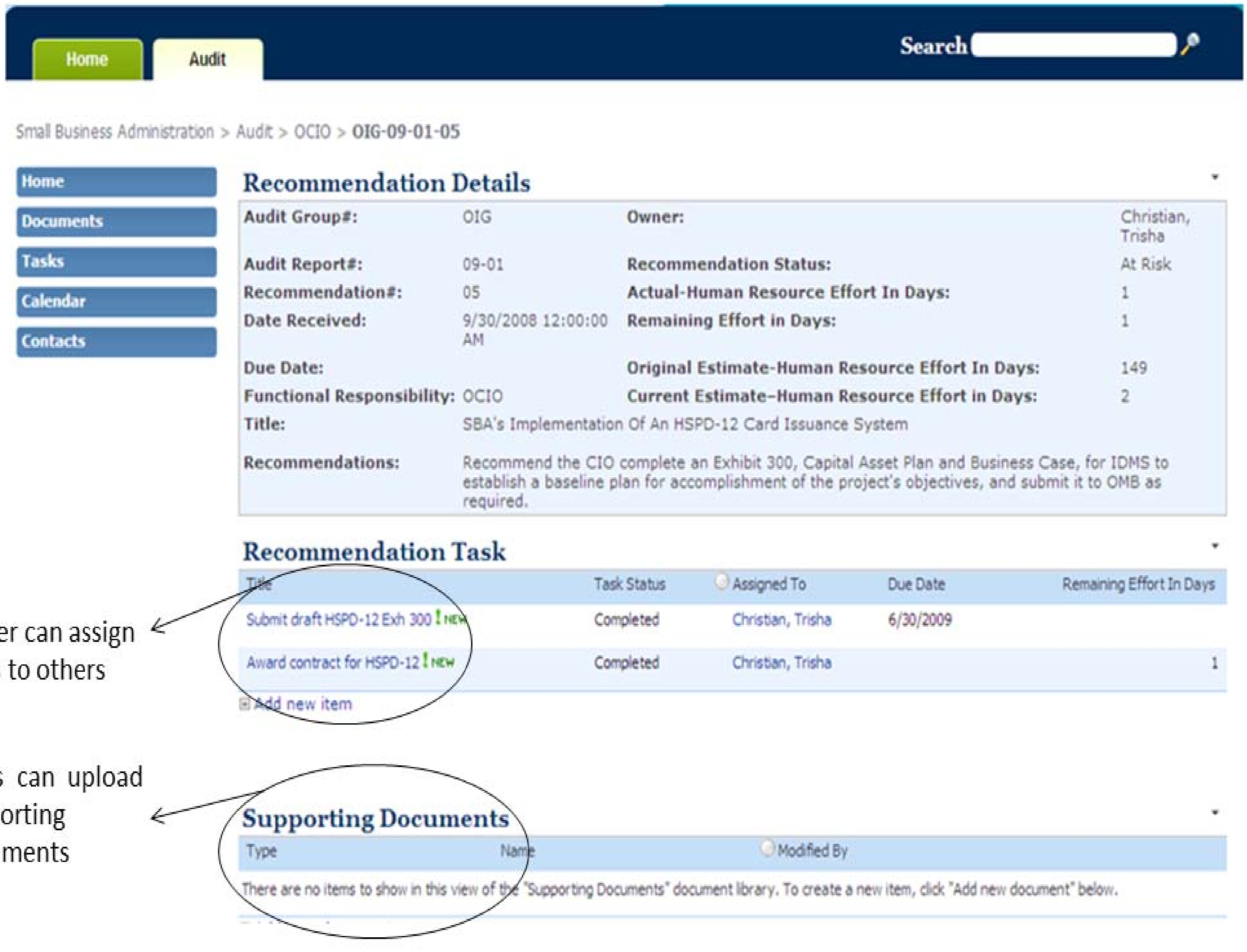
Audit Tracking and Accountability Tools



Recommendations

Title	Risk Category	Audit Report Number	Recommendation Number	Owner	Recommendation Status	Expected Completion Date	Recommendation Due Date	Functional Responsibility	Details
SBA's Implementation Of An HSPD-12 Card Issuance System	Technology Systems	09-01	05	Matthews, Ethel M.	Closed	9/17/2009	6/30/2009	OCIO	Details
Selected SBA General Support Operating Systems	Technology Systems	04-41	13	McCauley, David L.	Closed	10/30/2009	11/20/2009	OCIO	Details
SBA's Information System Controls for FY 2004	Technology Systems	05-12	21	McCauley, David L.	Closed	12/15/2009	4/15/2006	OCIO	Details
Vulnerability Technology Security Assessment	Technology Systems	07-16	7	Farmer, Darryl A.	Closed	9/16/2009		OCIO	Details
Planning for the Loan Management and Accounting System Modernization and Development Effort	Technology Systems	08-13	2	Whalen, Ronald D.	Closed	2/12/2010	4/24/2009	OCIO	Details
Planning for the Loan Management and Accounting System Modernization and Development Effort	Technology Systems	08-13	3	Francis, Chet C.	Closed	12/15/2009	4/30/2009	OCIO	Details
Audit of SBA's 2008 Financial Statements	Technology Systems	09-03	1	Gottlieb, Lawrence A.	At Risk	10/20/2009	7/30/2009	OCIO	Details
Audit of SBA's 2008 Financial Statements	Technology Systems	09-03	02	Gottlieb, Lawrence A.	At Risk	11/10/2009	6/30/2009	OCIO	Details
Audit of SBA's 2008 Financial Statements	Technology Systems	09-03	03	Gottlieb, Lawrence A.	At Risk	11/10/2009	5/1/2010	OCIO	Details
Audit of SBA's 2008 Financial Statements	Technology Systems	09-03	04	McCauley, David L.	Closed	9/23/2009	5/22/2009	OCIO	Details
Audit of SBA's 2008 Financial Statements	Technology Systems	09-03	09	Christy, Paul T.	Closed	12/1/2009	12/1/2009	OCIO	Details
Audit of SBA's 2008 Financial	Technology Systems	09-03	11	Christy, Paul T.	Closed	8/28/2009	8/21/2009	OCIO	Details

Audit Tracking and Accountability Tools



Small Business Administration > Audit > OCIO > OIG-09-01-05

Recommendation Details

Audit Group#:	OIG	Owner:	Christian, Trisha
Audit Report#:	09-01	Recommendation Status:	At Risk
Recommendation#:	05	Actual-Human Resource Effort In Days:	1
Date Received:	9/30/2008 12:00:00 AM	Remaining Effort in Days:	1
Due Date:		Original Estimate-Human Resource Effort In Days:	149
Functional Responsibility:	OCIO	Current Estimate-Human Resource Effort in Days:	2
Title:	SBA's Implementation Of An HSPD-12 Card Issuance System		
Recommendations:	Recommend the CIO complete an Exhibit 300, Capital Asset Plan and Business Case, for IDMS to establish a baseline plan for accomplishment of the project's objectives, and submit it to OMB as required.		

Recommendation Task

Title	Task Status	Assigned To	Due Date	Remaining Effort In Days
Submit draft HSPD-12 Exh 300 ! NEW	Completed	Christian, Trisha	6/30/2009	
Award contract for HSPD-12 ! NEW	Completed	Christian, Trisha		1

Add new item

Supporting Documents

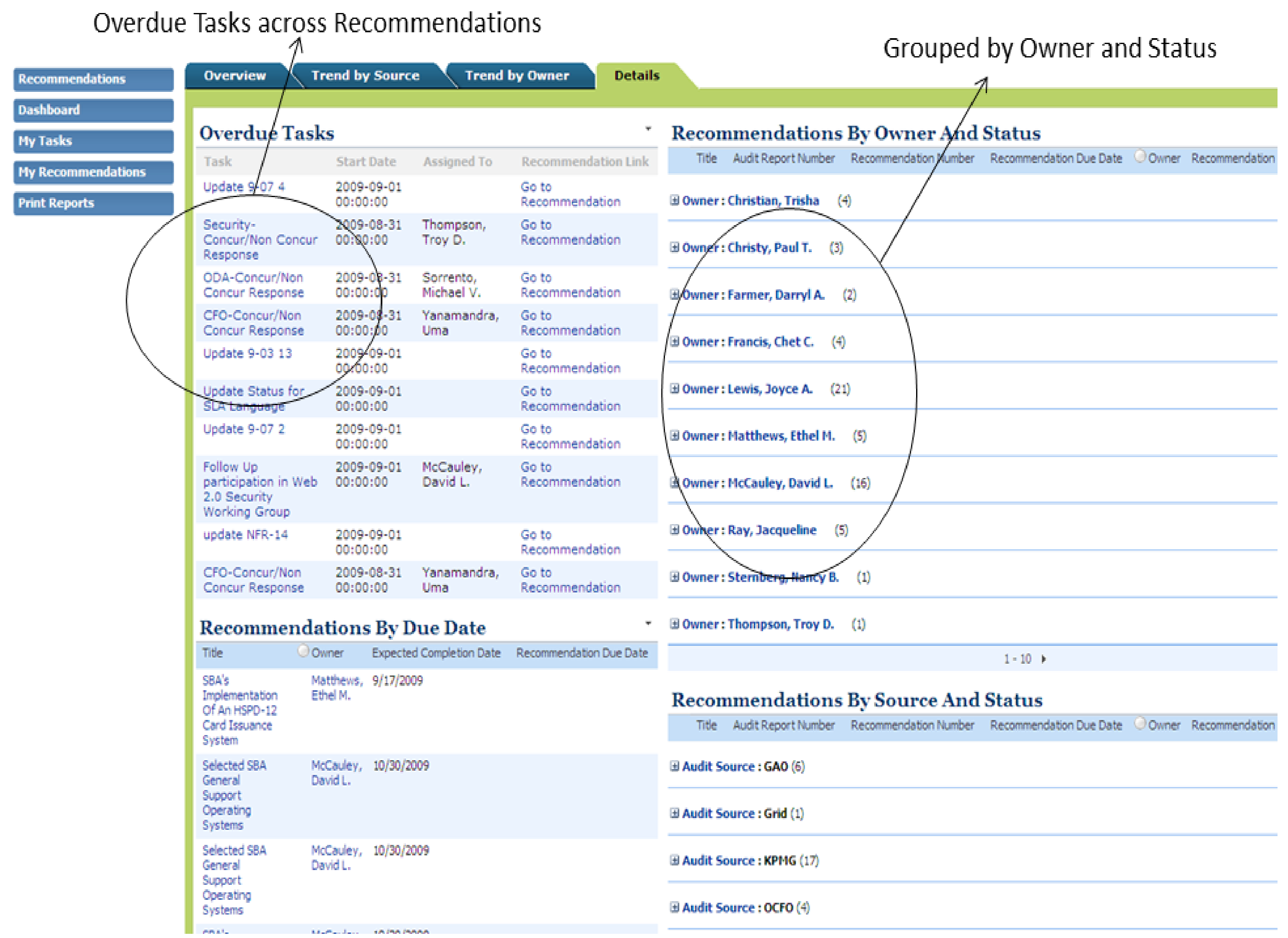
Type	Name	Modified By

There are no items to show in this view of the "Supporting Documents" document library. To create a new item, click "Add new document" below.

Owner can assign Tasks to others

Users can upload Supporting Documents

Audit Tracking and Accountability Tools



Overdue Tasks across Recommendations

Grouped by Owner and Status

Overdue Tasks

Task	Start Date	Assigned To	Recommendation Link
Update 9-07 4	2009-09-01 00:00:00		Go to Recommendation
Security-Concur/Non Concur Response	2009-08-31 00:00:00	Thompson, Troy D.	Go to Recommendation
ODA-Concur/Non Concur Response	2009-08-31 00:00:00	Sorrento, Michael V.	Go to Recommendation
CFO-Concur/Non Concur Response	2009-08-31 00:00:00	Yanamandra, Uma	Go to Recommendation
Update 9-03 13	2009-09-01 00:00:00		Go to Recommendation
Update Status for SLA Language	2009-09-01 00:00:00		Go to Recommendation
Update 9-07 2	2009-09-01 00:00:00		Go to Recommendation
Follow Up participation in Web 2.0 Security Working Group	2009-09-01 00:00:00	McCauley, David L.	Go to Recommendation
update NFR-14	2009-09-01 00:00:00		Go to Recommendation
CFO-Concur/Non Concur Response	2009-08-31 00:00:00	Yanamandra, Uma	Go to Recommendation

Recommendations By Due Date

Title	○ Owner	Expected Completion Date	Recommendation Due Date
SBA's Implementation Of An HSPD-12 Card Issuance System	Matthews, Ethel M.	9/17/2009	
Selected SBA General Support Operating Systems	McCauley, David L.	10/30/2009	
Selected SBA General Support Operating Systems	McCauley, David L.	10/30/2009	

Recommendations By Owner And Status

Title	Audit Report Number	Recommendation Number	Recommendation Due Date	○ Owner	Recommendation

⊞ Owner : Christian, Trisha (4)

⊞ Owner : Christy, Paul T. (3)

⊞ Owner : Farmer, Darryl A. (2)

⊞ Owner : Francis, Chet C. (4)

⊞ Owner : Lewis, Joyce A. (21)

⊞ Owner : Matthews, Ethel M. (5)

⊞ Owner : McCauley, David L. (16)

⊞ Owner : Ray, Jacqueline (5)

⊞ Owner : Sternberg, Nancy B. (1)

⊞ Owner : Thompson, Troy D. (1)

1 - 10 ▸

Recommendations By Source And Status

Title	Audit Report Number	Recommendation Number	Recommendation Due Date	○ Owner	Recommendation

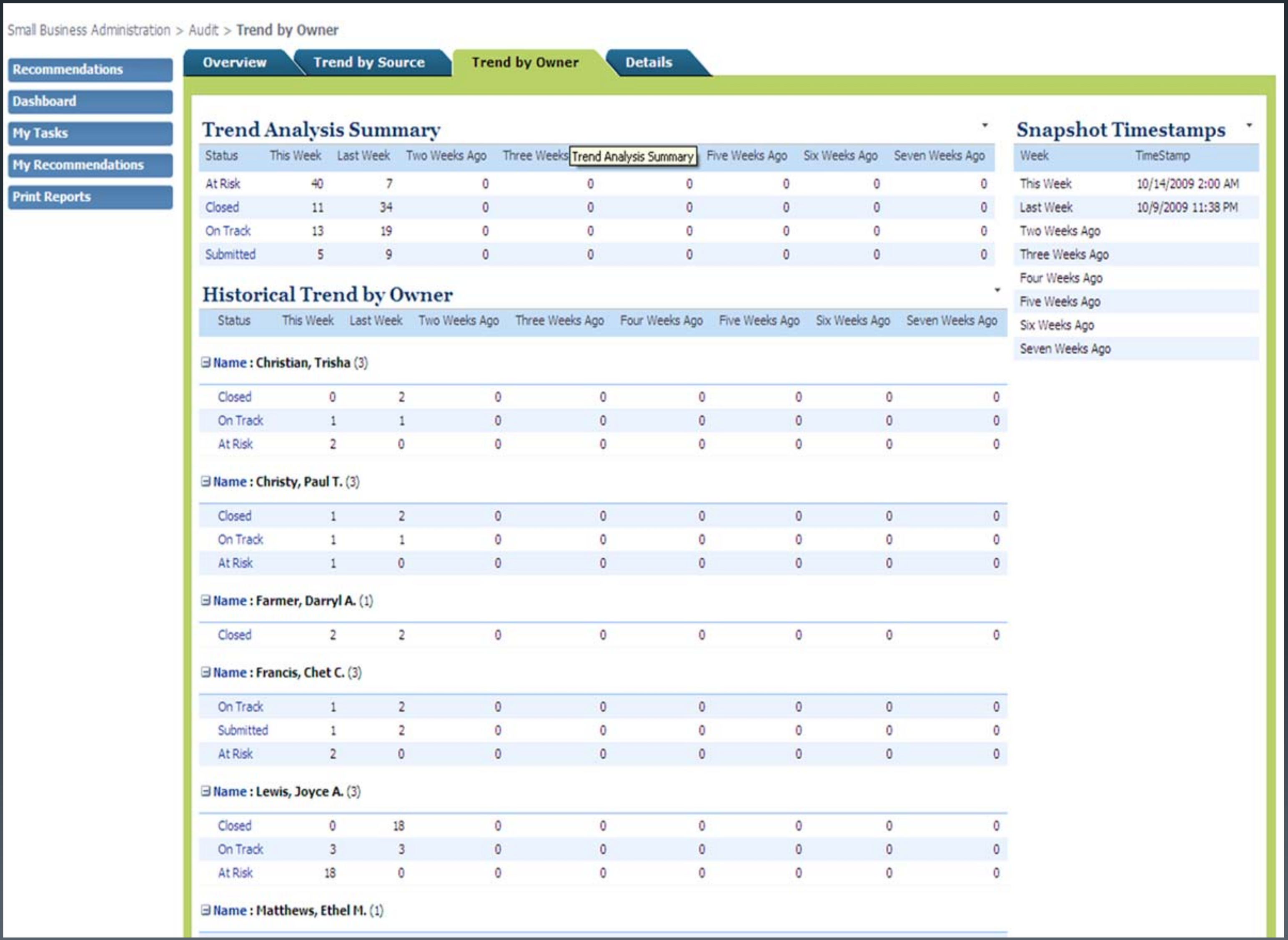
⊞ Audit Source : GAO (6)

⊞ Audit Source : Grid (1)

⊞ Audit Source : KPMG (17)

⊞ Audit Source : OCFO (4)

Audit Tracking and Accountability Tools



Trend Analysis Summary

Status	This Week	Last Week	Two Weeks Ago	Three Weeks	Trend Analysis Summary	Five Weeks Ago	Six Weeks Ago	Seven Weeks Ago
At Risk	40	7	0	0	0	0	0	0
Closed	11	34	0	0	0	0	0	0
On Track	13	19	0	0	0	0	0	0
Submitted	5	9	0	0	0	0	0	0

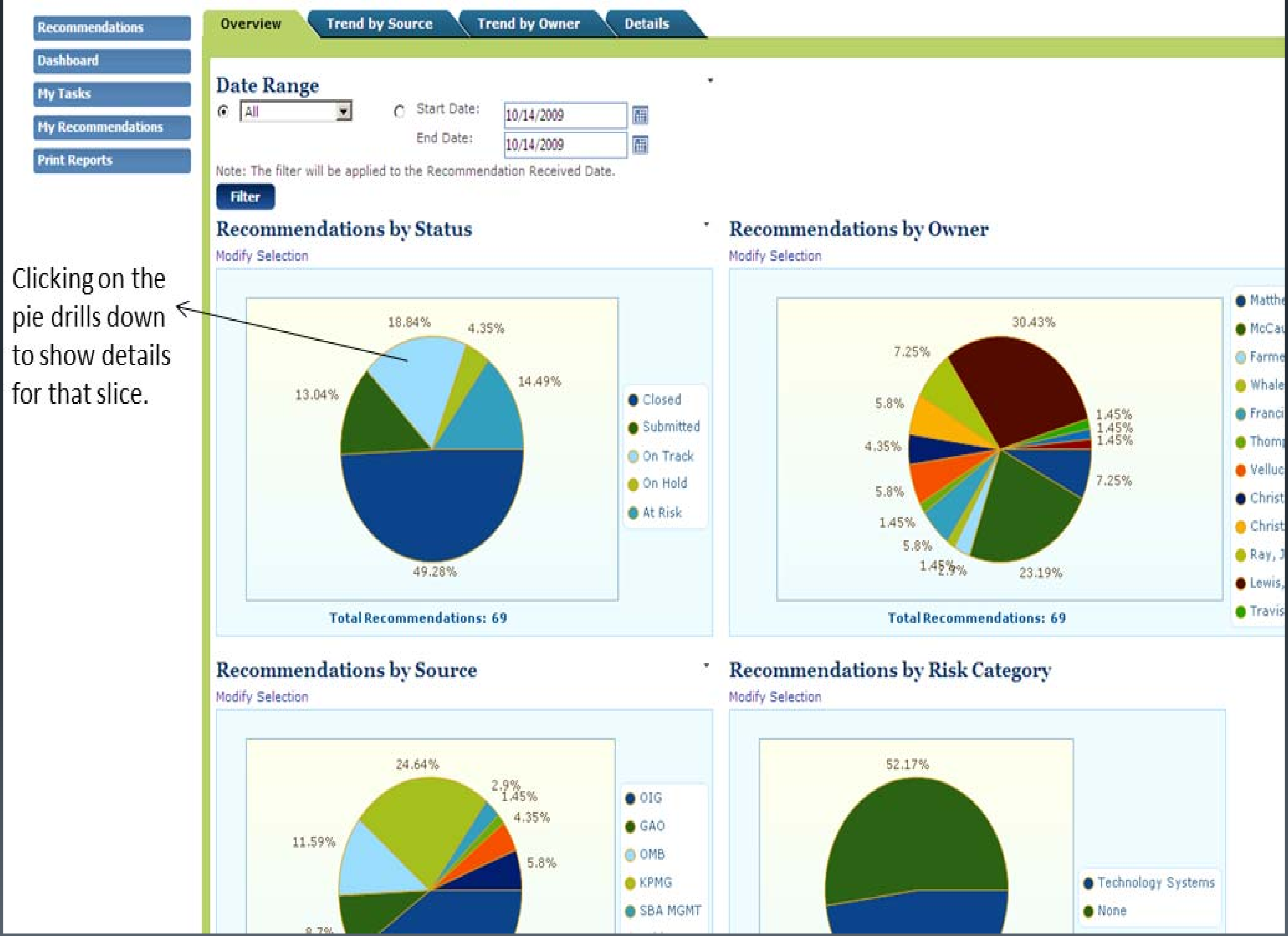
Snapshot Timestamps

Week	TimeStamp
This Week	10/14/2009 2:00 AM
Last Week	10/9/2009 11:38 PM
Two Weeks Ago	
Three Weeks Ago	
Four Weeks Ago	
Five Weeks Ago	
Six Weeks Ago	
Seven Weeks Ago	

Historical Trend by Owner

Status	This Week	Last Week	Two Weeks Ago	Three Weeks Ago	Four Weeks Ago	Five Weeks Ago	Six Weeks Ago	Seven Weeks Ago
⊟ **Name : Christian, Trisha** (3)								
Closed	0	2	0	0	0	0	0	0
On Track	1	1	0	0	0	0	0	0
At Risk	2	0	0	0	0	0	0	0
⊟ **Name : Christy, Paul T.** (3)								
Closed	1	2	0	0	0	0	0	0
On Track	1	1	0	0	0	0	0	0
At Risk	1	0	0	0	0	0	0	0
⊟ **Name : Farmer, Darryl A.** (1)								
Closed	2	2	0	0	0	0	0	0
⊟ **Name : Francis, Chet C.** (3)								
On Track	1	2	0	0	0	0	0	0
Submitted	1	2	0	0	0	0	0	0
At Risk	2	0	0	0	0	0	0	0
⊟ **Name : Lewis, Joyce A.** (3)								
Closed	0	18	0	0	0	0	0	0
On Track	3	3	0	0	0	0	0	0
At Risk	18	0	0	0	0	0	0	0
⊟ **Name : Matthews, Ethel M.** (1)								

Audit Tracking and Accountability Tools



Date Range

● All ○ Start Date: 10/14/2009

End Date: 10/14/2009

Note: The filter will be applied to the Recommendation Received Date.

Recommendations by Status

Total Recommendations: 69

Recommendations by Owner

Total Recommendations: 69

Recommendations by Source

Recommendations by Risk Category

Clicking on the pie drills down to show details for that slice.

What is needed?

- Continued support of the Chairman and Managing Director for the FCC Cyber Security Program

- Prioritization and Funding of ITC Cyber Security Unfunded Requirements to Right-size Cyber Security and to Implement Necessary Tools and Architecture to Better Protect the FCC Against Sophisticated Cyber Security Attacks

- ***Turn the FCC Cyber Security Operations into a Center of Excellence in the Federal Space***

Conclusion

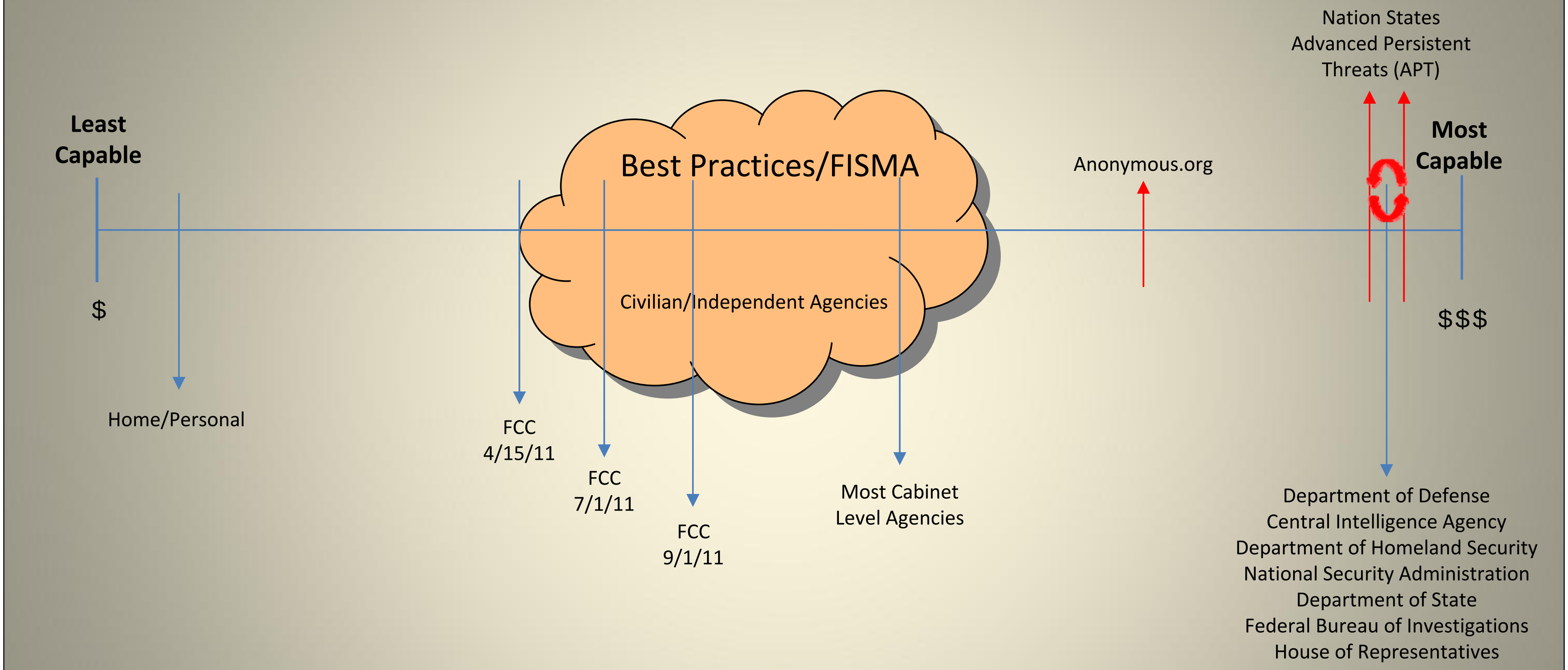
Cyber attacks have reached unprecedented levels of sophistication. The FCC’s Cyber Security program must keep pace with the adversary’s technological advances or face egregious harm to its network and reputation. To keep pace, the FCC must develop a comprehensive, risk-based approach to protect and support our missions.

Implementing an agile, effective, and cost-efficient approach to cyber security requires the FCC to develop improved and systematic processes, and to leverage technologies to streamline implementation and improve effectiveness of security controls.

In this cost-constrained environment, the Agency’s leadership needs to balance and prioritize security activities, based on risk and mission, and translate its strategies into effective tactical actions.

The cost, reputational damage, and Congressional oversight after a major FCC breech will be much more expensive versus the investment needed to prevent as many breeches as possible.   The FCC by it’s nature, must be a leader in cyber security!

Cyber Security Continuum 2011



Least Capable

$

Home/Personal

Best Practices/FISMA

Civilian/Independent Agencies

FCC
4/15/11

FCC
7/1/11

FCC
9/1/11

Most Cabinet
Level Agencies

Anonymous.org

Nation States
Advanced Persistent
Threats (APT)

Most Capable

$$$

Department of Defense
Central Intelligence Agency
Department of Homeland Security
National Security Administration
Department of State
Federal Bureau of Investigations
House of Representatives

Protection Capabilities →

Attack Capabilities →