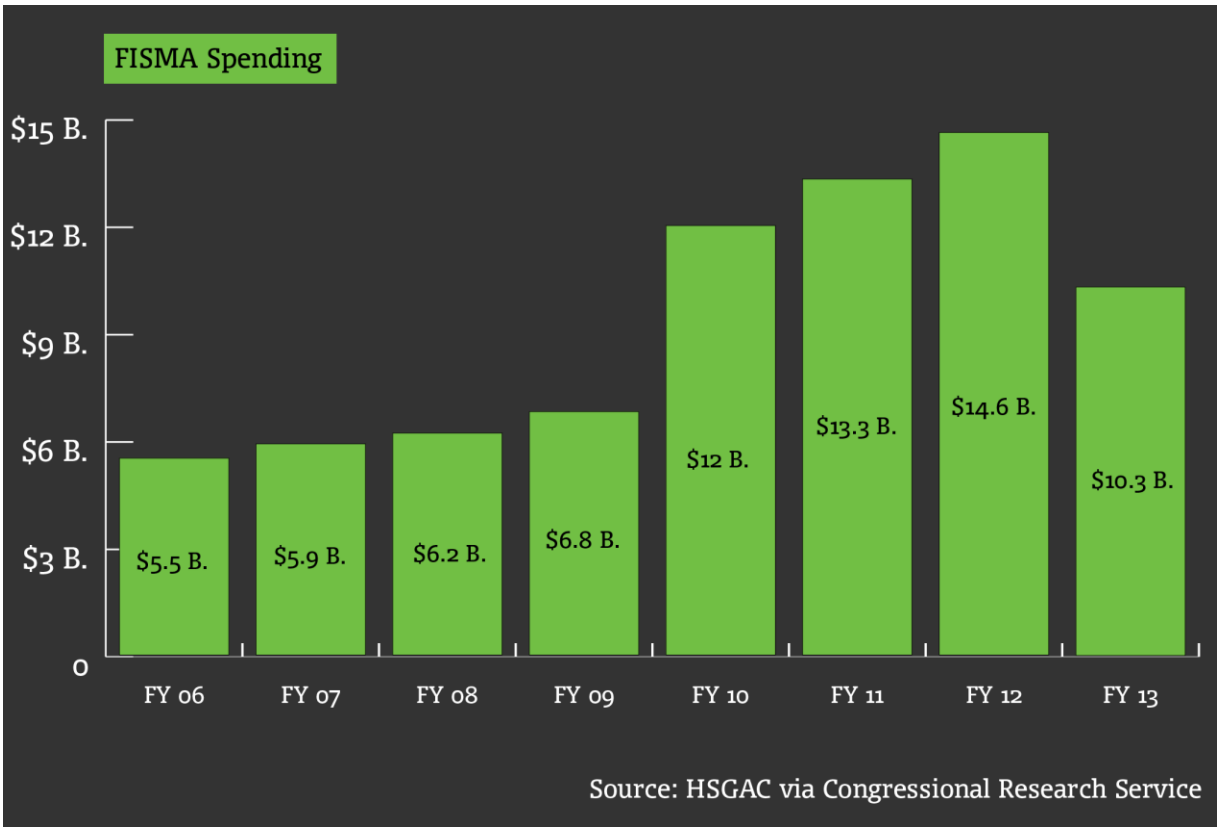
Understanding the Federal Government's "IT Insecurity" Crisis

A February 5, 2015 Report From the International Association of Information Technology Asset Managers

U.S. taxpayers have paid $59 billion for data protection since Fiscal Year 2010, including $10.3 billion in the most recent year under the Federal Information Security Management Act (FISMA). This week, the Obama Administration proposed a $14 billion cybersecurity budget for 2016.



Graphic by: NextGov.

Nonetheless, Information Technology (IT) security and IT Asset Management (ITAM) woes in federal agencies have been major staples of headlines in recent months, including problems

and mishaps at the Internal Revenue Service, the White House, State Department, and the Veteran's Administration.

The number of reported cyber incidents affecting Federal Government agencies has increased nearly a quarter in recent years, with agencies reporting more than 60,000 cyber incidents reported to authorities in Fiscal Year 2013 alone.

Figure 4: Cyber Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies in FY 2013

Incident Category	Number of Incidents	Percentage of Total Incidents
Non-Cyber (Personally Identifiable Information spillage or mishandling for hardcopy or printed material)	15,057	24.8%
Policy Violations (mishandling of data in storage or transit)	11,847	19.5%
Malicious Code (malware)	9,883	16.3%
Equipment (lost or stolen equipment)	9,587	15.8%
Other (low frequency incidents, such as unconfirmed third-party notifications, failed attacks, or incident with unknown causes)	5,885	9.7%
Social Engineering (fraudulent websites or attempts to entice users to provide sensitive information)	3,580	5.9%
Suspicious Network Activity	3,167	5.2%
Improper Usage (rule of behavior violations)	969	1.6%
Unauthorized Access (unprivileged users gain control of system or resource)	653	1.1%
Phishing (subset of Social Engineering, attempt to entice users to provide sensitive information)	71	0.1%
Denial of Service (successful Denial of Service attacks)	54	0.1%
Total	60,753	100.0%

Source: The OMB's FY 2013 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002[5] dated May 2014. Percentages do not total 100 percent due to rounding.

If anything, the situation worsened in 2014 with several high profile cases coming to light:

1. DoD/ U.S. Central Command – social media hack
2. United States Postal Service – China-linked attack on personnel info
3. White House – Russian hack on unclassified networks
4. DoD/ U.S. Transportation Command – Chinese hacker penetration
5. National Oceanic and Atmospheric Administration – Chinese hackers
6. Nuclear Regulatory Commission – IG Report- NRC hacked three times in three years
7. U.S. Investigation Services (USIS) – Primary US security clearance contractor
8. U.S. State Department – Hack on unclassified email network

But while awareness of the problem has spread, the ability to deal with such threats has improved very little. Federal IT chiefs often cite inadequate funding as the biggest inhibitor to progress, but a thorough investigation of the overall federal government IT sector reveals that cost savings and IT security would be increased by a comprehensive ITAM program at the national government level in the U.S.

It is important to understand that in addition to breaches, there is a huge potential for cutting wasteful spending through ITAM that would save taxpayers substantial sums of money. It has been estimated that the Department of Homeland Security alone saved $181 million in software licensing in one recent year, and that more than $1 billion could be saved in information technology and telecommunications per year across the federal government if best practices were applied.

The reality is that the crisis in federal IT management is as much an opportunity as it is a risk, particularly when it comes to saving taxpayers money. The overall spending pattern of the federal government on IT suggests that enormous progress could be achieved through better and tighter ITAM practices. One major reason: Better control of inventory, software licensing, upgrades, and so on, will actually reduce the risk of more federal government IT failures. Conversely, spending greater and greater sums without proper ITAM controls in place is a prescription for more breaches, risks posed by unauthorized devices, increases in lost and stolen hard drives, and major vulnerabilities created by outdated and/or "unpatched" software.

The following chart shows two roughly comparable findings that private industry in the United States pays an average of $4,600-$4,900 per employee on IT – less than $5,000 a head:

Annual IT Cost per Employee
Private Industry

	High Cost	Low Cost	Average Cost per Employee
IAITAM Study	$6,233.00	$3,500.00	$4,867.00
Gartner Study	$5867.00	$3413.00	$4,640.00

Contrast this average of less than $5,000 in private industry with the IT spending pattern of the federal government:

Sector/Agency	Budget	# of Employees	Average Cost per Employee
Federal Government	$73,700,000,000.00	2,050,000.00	$36,162.00

This suggests that the federal government spends an astonishing <u>six times more per employee on IT than does private industry</u>. As if these overall figures were not eye-popping enough, the variations by federal agency are even more extreme, including **more than *$168,000 per U.S. Department of Education employee* and *more than $109,000 per U.S. State Department employee*!** It is not comforting to see that the most reasonable (in relative terms) level of spending is at the technology-challenged Veteran's Administration at nearly $11,700 per employee, a level still well over twice what private industry pays in the U.S.

	Employment						
	United States	U.S. Territories	Foreign Countries	Unspecified	Location - All Employees	2015 IT Budget	cost per employee
AG-DEPARTMENT OF AGRICULTURE	85,396	664	163	121	86,344	$ 2,600,000,000	$ 30,112
DD-DEPARTMENT OF DEFENSE	96,170	1,348	11,886	4	109,408		
NV-DEPARTMENT OF THE NAVY	186,134	1,239	3,829	0	191,202		
AR-DEPARTMENT OF THE ARMY	242,447	1,393	10,713	0	254,553		
AF-DEPARTMENT OF THE AIR FORCE	161,451	385	3,072	252	165,160		
TOTAL DOD	**686,202**	**165,816**	**33,865**	**29,756**	**720,323**	$ 30,300,000,000	$ 42,064
CM-DEPARTMENT OF COMMERCE	44,945	128	211	50	45,334	$ 2,000,000,000	$ 44,117
DJ-DEPARTMENT OF JUSTICE	112,162	520	88	14	112,784	$ 2,500,000,000	$ 22,166
DL-DEPARTMENT OF LABOR	15,876	42	1	0	15,919	$ 611,500,000	$ 38,413
DN-DEPARTMENT OF ENERGY	15,057	0	21	0	15,078	$ 1,500,000,000	$ 99,483
ED-DEPARTMENT OF EDUCATION	4,136	6	0	0	4,142	$ 697,000,000	$ 168,276
HE-DEPARTMENT OF HEALTH AND HUMAN SERVICES	85,406	223	261	18	85,908	$ 8,600,000,000	$ 100,107
HS-DEPARTMENT OF HOMELAND SECURITY	187,032	2,696	1,049	176	190,953	$ 5,800,000,000	$ 30,374
HU-DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT	8,359	56	0	1	8,416	$ 218,000,000	$ 25,903
IN-DEPARTMENT OF THE INTERIOR	63,772	323	7	6	64,108	$ 989,000,000	$ 15,427
ST-DEPARTMENT OF STATE	12,783	15	25	4	12,827	$ 1,400,000,000	$ 109,145
TD-DEPARTMENT OF TRANSPORTATION	53,842	275	40	144	54,301	$ 3,300,000,000	$ 60,772
TR-DEPARTMENT OF THE TREASURY	106,937	671	51	299	107,958	$ 4,000,000,000	$ 37,051
VA-DEPARTMENT OF VETERANS AFFAIRS	338,107	3,960	19	3	342,089	$ 4,000,000,000	$ 11,693

https://itdashboard.gov/treemap
http://www.fedscope.opm.gov/ibmcognos/cgi-bin/cognosisapi.dll

If this level of federal spending on IT was to be reduced to just three times the average for private industry, the savings would add up to well over $30 billion, of which only a tiny fraction would be needed to put in place needed ITAM controls on overall federal IT and IT Security.

What drives the enormous bloat and inefficiencies at the federal level?

IAITAM's review of federal agencies found that while the hacks and breaches get all the attention, the waste of taxpayer dollars is every bit as troubling. Consider these findings:

DEPARTMENT OF ENERGY

THEME: Waste

- DOE is not managing its hardware acquisitions. An Inspector General (IG) investigation found that in 2012 DOE spent nearly $2 million more than necessary on IT equipment acquisitions at just eight sites investigated. The IG investigation found that IT acquisition standards that were in place were disregarded 75% of the time at these sites. At one of the eight sites monitored, standards were not followed 100% of the time. This contributed to huge and wasteful variations in the price paid per device across the sites. The IG found that at one site the DOE paid 42 different prices ranging from approximately $900 to over $2,000 for one desktop model in FY 2012. In total, those price fluctuations alone could have cost the DOE more than a quarter of a million dollars across the sites reviewed.
- September 2014 IG Audit found that over a three-year period, DOE paid approximately $600,000 more than necessary on software licenses. The IG audit found at least 52 instances where price paid for common products varied widely – up to 46%, and $2,700 per license.

SECURITIES AND EXCHANGE COMMISSION

THEME: Mismanagement

From an October 2014 IG Audit: 17% of the laptops reviewed had incorrect location; 22% had incorrect user information; and 5% – 24 of 488 laptops – were totally unaccounted for. Based on this sample, the IG concluded that more than 200 SEC laptops were missing on an agency-wide basis.

INTERNAL REVENUE SERVICE

THEMES: Waste and Mismanagement

A February 2014 IG Report found inadequate software management cost taxpayers $11.6 million in unused software in a single contract.

Figure 1: Nondeployed Software

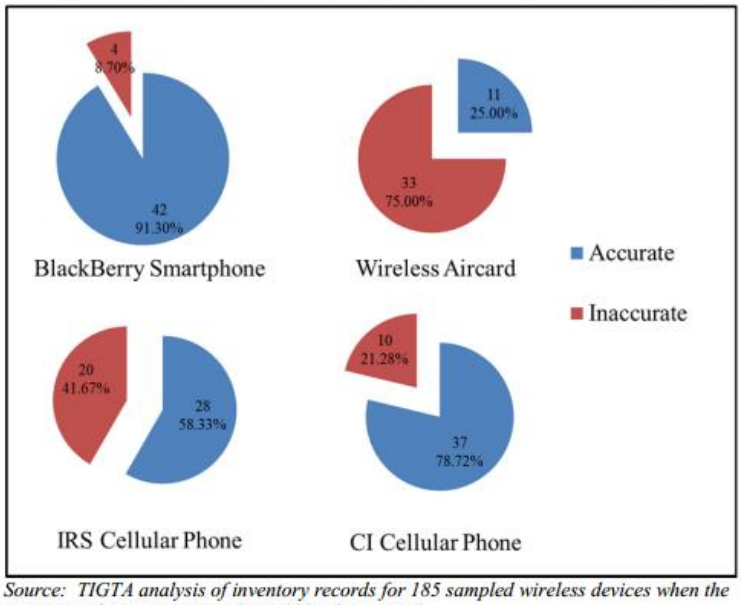
Software	Licenses Owned	Total GSA List Price	Subscription and Support Paid	Total GSA List Price Subscription and Support	Total GSA List Price Value
Product 1	516	$848,820	516	$130,032	$978,852
Product 2	516	$2,167,200	516	$361,200	$2,528,400
Product 3	516	$1,590,312	516	$136,224	$1,726,536
Product 4	156	$171,132	156	$34,476	$205,608
Product 5	156	$571,896	156	$115,440	$687,336
Product 6	362	$722,190	362	$109,324	$831,514
Product 7	362	$1,444,380	362	$219,010	$1,663,390
Product 8	50	$47,400	50	$7,200	$54,600
Product 9	362	$595,852	362	$90,500	$686,352
Product 10	362	$722,190	362	$109,324	$831,514
Product 11	362	$1,263,742	362	$191,498	$1,455,240
Total	3,720	$10,145,114	3,720	$1,504,228	**$11,649,342**

Source: TIGTA analysis of IRS and contractor records, 2012 GSA Price List, and discussions with IRS IT organization management and personnel.

An April 2014 Government Accountability Office (GAO) report found "significant deficiency" in IRS information security. The IRS had not installed appropriate patches on all databases and servers to protect against known vulnerabilities. The IRS had not sufficiently monitored database and mainframe controls. The IRS had not appropriately restricted access to its mainframe environment.

A November 2014 IG Report found that mobile device management is poor at the IRS. Nearly three out of five (57%) of mobile device inventory records were incorrect at an agency where 94% of employees are provided with a mobile device.

Figure 3: Inventory Verification Results by Device Type[24]



Source: TIGTA analysis of inventory records for 185 sampled wireless devices when the accuracy of inventory records could be determined.

The IG report found that lost and stolen wireless devices were not documented, at a whopping rate of 30% of the sample. Further, the IRS paid monthly service fees for almost 6,800 devices that were not inventoried (almost 17% of total devices, and almost $2 million per year in service fees). For more than 700 employees, the IRS paid for multiple mobile devices (between two and five) despite the prohibition against multiple devices.

U.S. DEPARTMENT OF VETERANS AFFAIRS

THEME: Recurring Unfixed Issues

In November 2014, the VA failed its annual cybersecurity audit for its 16th consecutive year. In testimony, Sondra McCauley, Deputy Assistant Inspector General for Audits and Evaluations, Office of Inspector General, U.S. Department of Veterans Affairs cited recurring issues in audit after audit. Highlights from her 2014 testimony included the following:

- IT systems were not patched or securely configured to mitigate in a timely way known and unknown information security vulnerabilities.
- VA databases included "several known critical vulnerabilities that cannot be updated with patches." Performance and security weaknesses were inherent with older versions of the system software in use.
- Several VA organizations were sharing the same local networks as other tenants of VA facilities and data centers. These networks were not under VA control, and often had "critical or high-level vulnerabilities" that weakened the overall security posture of the VA.
- Password standards, and multi-factor authentication for remote access, were not consistently implemented and enforced.
- Monitoring of access was lacking in the production environment for individuals with elevated application privileges for a major application.
- Unknown and unmonitored system interconnections continued to exist.
- VA did not effectively manage and monitor its systems hosted at a cloud service provider.
- Backup tapes were not encrypted prior to being sent to offsite storage at selected facilities and data centers.

Even after a dramatic cyber hack was detected in 2012, a GAO report from November 2014 found that the "VA has not addressed an underlying vulnerability that allowed the incident to occur."

DEPARTMENT OF EDUCATION

THEME: Recurring Unfixed Issues

A November 2014 IG Report found that "longstanding weaknesses" continue to cause the Department's information systems to be vulnerable to "serious security threats." The problems "comprised repeat or modified repeat findings from OIG reports issued in 2011 and 2013."

The repeat offenses included:

- The Department of Education was not tracking the IT assets in their inventory. The Agency "had not fully established policies and procedures to identify all devices that were attached to the network, distinguish those devices from users, and authenticate devices that were connected to the network."
- Repeated breakdowns in communication were noted when security incidents occurred. Almost 10% of sampled incidents were not reported to the United States Computer Emergency Readiness Team as required. Of those, many were deemed problematic enough to require reporting to law enforcement. Yet 94% were not communicated to appropriate law enforcement.
- System authorization and documentation: 24% of IT systems in the Department's network were operating on expired security authorizations.

U.S. DEPARTMENT OF AGRICULTURE

THEME: Recurring Unfixed Issues

A November 2014 IG Report found many longstanding weaknesses:

- Between fiscal year 2011 and 2013, IG made 55 recommendations for improving overall IT security. Less than half (21) had been addressed with corrective action at the time of the November 2014 report.
- Slow remediation: 37% of vulnerabilities found at one USDA agency were not remedied within six months.
- Software Management: USDA did not have a process for timely and secure installation of software patches, despite requirement. The IG report found that an astounding 82.5% of correctable vulnerabilities at one USDA agency were not patched when one was available.
- Documentation of incidents: When IT incidents occurred, 18% were not handled in accordance with procedures on analysis, validation, and documentation.
- Poor contractor/inventory management: IG report found 23 contractor systems were not being recorded in the Cyber Security Assessment and Management system.

DEPARTMENT OF HOMELAND SECURITY

THEME: Mismanagement

A December 2014 IG Report Found:

- FEMA and United States Citizenship and Immigration Service (USCIS) were still using the Microsoft Windows XP operating system, which remains vulnerable to attack as Microsoft stopped providing software updates to mitigate security vulnerabilities in April 2014.
- USCIS has a track record of not mitigating high-risk vulnerabilities in a timely manner. For example, the Heartbleed alert was issued to USCIS on June 27, 2014 with a mandate to get systems inoculated against it by July 7. When audited several weeks after that deadline, the IG found that USCIS workstations were still vulnerable to Heartbleed.
- IT system inventory is not supposed to fluctuate largely from month to month. If it does, it indicates a problem, such as improper capturing methodology. This remained a persistent issue at some DHS agencies.

NUCLEAR REGULATORY COMMISSION

THEME: Recurring Unfixed Issues

November 2014 IG Report: IT security program weakness.

- Continuous IT monitoring was not performed as required.
- Repeat finding: configuration management procedures are still not consistently implemented.
- Repeat finding: plan of action and milestone (POA&M) management needs improvement.

CONCLUSION/RECOMMENDATIONS

At the root of much of what ails the federal government bloat in IT spending and related woes is a lack of meaningful IT Asset Management. ITAM is the bridge that links an organization's financial, contractual, and physical IT inventory requirements with the goals and objectives of the operational IT environment.

The Federal Government's approach to ITAM should include two components:

- The first is a rigorous government-wide centralized ITAM program responsible for creating policies, procedures, processes, and metrics for all government agencies.

- The second is an agency-level ITAM team, which would include the day-to-day management of all assets within that agency as set forth and required by the centralized program.

Concurrently, legislation should be enacted to protect and manage our greatest resource (technology) at the federal level, state level, and in critical infrastructure in the private sector. This legislation should address the areas of procurement, disposal, inventory management to

the component level of IT Assets (such as hard drives), data security, and other mandated policies which would mitigate the risk to the United States and the critical infrastructure that is not owned by the government but is enabled and regulated by legislation.

A focus on ITAM at the federal level will ***decrease***:

- IT security threats by understanding what you have, how it is being used, where it is located, who is using it, and when it is being used.
- Unnecessary IT spending by eliminating unused or underused products, maintenance, storage, and potentially hundreds of other areas from procurement to disposal.
- Gross underutilization of existing IT assets by understanding what we actually have and what is actually needed.
- Software license compliance violations by not only ensuring proper licensing but also eliminating rogue purchases.
- Equipment missing and/or lost -- by having the knowledge of what you own you will be able to identify the danger in a speedy and efficient manner should the situation arise of a missing or lost piece of technology.
- Unauthorized user access by ensuring the standards are in place and backed by policy on who and when access is needed.
- Data lost by tracking the components of assets containing information.
- Unauthorized software programs installed and purchased outside of normal procurement process by ensuring a policy and standard is in place to eliminate rogue acquisition and installations.
- Project mismanagement by establishing a set of standards by which all projects must follow.
- Contract inconsistencies by establishing a set of standards by which all contracts and negotiations must follow.

A focus on ITAM at the federal level will ***increase***:

- Infrastructure security by providing the knowledge and understanding of what you have, how it is being used, where it is located, who is using it, and when it is being used within your environment.
- IT accountability by providing measurements to understand what is owned and how it is used.
- IT asset value by ensuring assets are used to their full potential and overspending is mitigated.
- IT compliance by ensuring the procedures are in place to adhere to legislation and requirements.
- Usable, reliable, real-time information for proactive IT business decision-making by enacting a reporting structure that monitors performance of assets.
- Effectiveness in process adoption and automated management by defining procedures and processes that are repeatable and measurable.
- ITAM awareness and ownership by establishing a communication and education key process area which promotes ITAM awareness.

- Visibility of the IT asset environment to support IT Service Management through the association between the service and the asset.
- Software patch management accuracy by providing the knowledge and understanding of what you have and where it lies in the lifecycle process.

ABOUT IAITAM

The International Association of Information Technology Asset Managers, Inc. is the professional association for individuals and organizations involved in any aspect of IT Asset Management, Software Asset Management (SAM), Hardware Asset Management, Mobile Asset Management, IT Asset Disposition and the lifecycle processes supporting IT Asset Management in organizations and industry across the globe. IAITAM certifications are the only IT Asset Management certifications that are accredited and unconditionally recognized worldwide. For more information, visit www.iaitam.org, or the IAITAM mobile app on Google Play or the iTunes App Store.