FEDERAL AGENCIES' RELIANCE ON OUTDATED AND UNSUPPORTED INFORMATION TECHNOLOGY: A TICKING TIME BOMB

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

MAY 25, 2016

Serial No. 114–120

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE
23–644 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
JIM JORDAN, Ohio
TIM WALBERG, Michigan
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
CYNTHIA M. LUMMIS, Wyoming
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
MICK MULVANEY, South Carolina
KEN BUCK, Colorado
MARK WALKER, North Carolina
ROD BLUM, Iowa
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma
EARL L. "BUDDY" CARTER, Georgia
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY J. PALMER, Alabama

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MATT CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California
BONNIE WATSON COLEMAN, New Jersey
STACEY E. PLASKETT, Virgin Islands
MARK DESAULNIER, California
BRENDAN F. BOYLE, Pennsylvania
PETER WELCH, Vermont
MICHELLE LUJAN GRISHAM, New Mexico

JENNIFER HEMINGWAY, *Staff Director*
DAVID RAPALLO, *Minority Staff Director*
TROY STOCK, *Staff Director, Subcommittee on Transportation and Public Assets*
JULIE DUNNE, *Counsel*
WILLIE MARX, *Clerk*

CONTENTS

WITNESSES

APPENDIX

FEDERAL AGENCIES' RELIANCE ON OUTDATED AND UNSUPPORTED INFORMATION TECHNOLOGY: A TICKING TIME BOMB

Wednesday, May 25, 2016

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
WASHINGTON, D.C.

The committee met, pursuant to call, at 9:02 a.m., in Room 2154, Rayburn House Office Building, Hon. Jason Chaffetz [chairman of the committee] presiding.

Present: Representatives Chaffetz, Mica, Farenthold, Meadows, Mulvaney, Hurd, Cummings, Lynch, Connolly, Kelly, and Lieu.

Chairman CHAFFETZ. The Committee on Oversight and Government Reform will come to order. I appreciate those in attendance today. We are having a hearing about Federal agencies' reliance on outdated and unsupported information technology, a ticking time bomb.

The Federal Government is spending more than $80 billion—$80 billion—annually on IT, and it largely doesn't work. With the majority of the spending focused on maintaining and operating legacy systems, this is obviously a major concern for the United States Congress and the operation of the Federal Government.

Such spending on legacy IT results in higher costs and security vulnerabilities where old software and operating systems are no longer supported by vendors. The Federal Government is years and, in some cases, decades behind the private sector. We cannot have Federal agencies buying spare parts on eBay for IT systems, such as the case at the Department of Labor.

The Federal Government also cannot rely on 930 million lines of code using more than 70 legacy programming languages. This is the best estimate that we have on the numbers, based on the surveys that we did with the various agencies.

That includes over 155 million lines of COBOL and 135 million lines of Fortran, coding language that was first used in the 1960s. In fact, 50 years ago—50 years ago—Dartmouth described Fortran as "old-fashioned." So 50 years ago, they thought it was old-fashioned, and it is still in use today.

This does not even include the Departments of Defense or Labor, because they could not tell us how many lines of code, so you can imagine at DOD how many millions upon millions of lines of code that are still out there in those agencies.

Some agencies still use Windows 3.1, which came on the market in the early 1990s, or Windows XP, which came on the market in the early 2000s.

I read a document recently from the Department of Justice, and it was a WordPerfect document. I love WordPerfect. They are from Utah, and they still sell that product and update it. They had an update in the last 60 days. But my guess is if they tried to send you a WordPerfect document, you might have a difficult time opening it.

The Federal CIO Tony Scott is one of our witnesses today. He has stated the need to update IT legacy systems is a crisis bigger than Y2K.

I will note, personally, I am so pleased that Mr. Scott has joined the Federal Government. He has quite a background and reputation. He is the kind of talent that I think our Federal Government needs. To have somebody of his caliber helping to tackle these issues, answering the call to service for our Nation, is really an important step forward, and I applaud the Obama administration for encouraging him and getting him to participate here. I think he is part of the solution and not part of the problem.

Let me give you some examples of our deep concern here.

The Department of Defense Strategic Automated Command and Control System is 50 years old and runs on a 1970s IBM Series 1 computer that uses an 8-inch floppy disk.

This is an 8-inch floppy disk. It takes 3.2 million of these to equal one flash drive. So you can go get a flash drive down at Best Buy or you can get 3.2 million of these to get the same amount of data stored. And this is still what the Department of Defense is using.

I want to show a couple pictures here. These are from the brochure. This is what the Department of Defense in many ways is still using, nice 1970s, first-class brochures there. Those styles, that is styling. That is literally the kind of technology that we are using and up against.

DOD is only now, by the end of fiscal year 2017, finally scheduled to update parts of this system. It is good, but it is decades overdue.

The system reminds me, do you remember the movie WarGames, the WOPR, the War Operations Plan Response, from the 1983 movie? It is still like that, unfortunately.

The IRS Individual Master Files, sometimes called the IMF, which is the authoritative data source for individual taxpayer information, is also more than 50 years old. It is written in low-level computer code that is difficult to write and maintain.

The IRS has general plans to modernize and has made some progress, but provided no specific date on which the IMF will be turned off and the new system turned on. I hope that changes here today. Goals must have deadlines. Otherwise, they are just dreams, and we need specifics.

The really scary part about all this is that DOD and the IRS are not alone among the Federal agencies relying on legacy IT systems and unsupported software and operating systems.

So how do we fix this situation? How do we protect the Nation against the vulnerabilities that are inevitably there with such outdated technology?

We are going to hear a lot today about a proposal to establish a $3 billion IT modernization fund to help agencies move off of these legacy systems. There are three issues that I would like to mention proactively about this proposal. I think it is a serious proposal based on a lot of good work done in the private sector.

First, the GAO reported last week, at a joint IT–Government Operations Subcommittees hearing, there are millions of dollars' worth of savings still on the table from data center consolidation. To date, agencies have closed more than 3,000 of 10,500 data centers and achieved $2.8 billion in cost savings. Most of these savings are attributed to just four agencies, the Department of Commerce, the Department of Defense, the Department of Homeland Security, and Treasury. So there is much available in terms of savings still on the table.

I think I am much more inclined to allow CIOs who are achieving savings and have the foresight and plan to move forward to use those savings to upgrade legacy systems rather than simply writing a blank check for all CIOs, regardless of how well they are currently managing their resources.

Second, the committee wants to see progress on its FITARA implementation scorecard before giving CIOs additional resources. Under FITARA, CIOs now have a proper seat at the table.

To the men and women in the CIO positions, they must be qualified, motivated, and empowered to make decisions within their agencies, and they must be held accountable. The pattern of Fs moving to Ds, and Ds moving to Cs, and so forth, will go a long way to convincing the committee that CIOs will appropriately utilize additional resources allocated to modernizing legacy systems.

Third, I note that Mr. Milholland appears today under a subpoena. IRS Commissioner John Koskinen declined to allow Mr. Milholland to testify voluntarily and stated to the committee, and I quote, this comes from the letter, "Spending time preparing for a hearing would take Mr. Milholland away from his important role in leading IT development and operation, and would be disruptive to the IRS."

That is wholly and totally unacceptable. This is part of the solution, not part of the problem, and the accountability before Congress is part of this issue.

Preparing for, testifying at a hearing on IT issues in front of this committee does not take away from the important role. It is a key part of your important role.

The committee hopes IRS attitude and position is not widespread across the Federal Government. It is a change in attitude from the IRS Commissioner.

The IRS Commissioner insisted that he personally be here to testify, but we want to have the people who are actually responsible day-to-day and spend 100 percent of their day working on this issue. It is very frustrating.

Taxpayers deserve a government that leverages technology to serve them, rather than one that deploys unsecured, decades-old technology that places their sensitive and personal information at risk. We have a long way to go to get from COBOL to the cloud, but I am committed to helping us get there.

I know other members of the committee are working on this as well. I want to duly note Ranking Member Cummings, Chairman Hurd, Ranking Member Kelly, Chairman Meadows, and Ranking

Member Connolly among those who are spending a significant amount of time trying to help tackle and solve the problem. I appreciate their insight and their participation.

This is not a partisan issue. We all need to come together on this, on both sides of the aisle. It is the right thing to do, and it is a vital part of the infrastructure that we need in order to have a fully functional government.

So we will have a good hearing today. I appreciate the witnesses being here.

I will now recognize the ranking member, Mr. Cummings, for his comments.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

There has been an increasing number of sophisticated cyberattacks against Federal agencies like the Office of Personnel Management as well as private sector companies like Anthem, Primera, and Sony Pictures. These devastating cyberattacks highlight the challenges faced by public agencies and the private sector in keeping their systems secure from determined, sophisticated cyber spies.

They also highlight the need for strong congressional action to help agencies strengthen their security and modernize their information technology systems.

The problem, however, is that Republicans in Congress have spent the last several years making massive cuts to Federal agency budgets, making it harder for these agencies to upgrade their information systems, let alone maintain the systems they have.

The Internal Revenue Service is a prime example. Republicans slashed the IRS budget by almost 17 percent over the past 5 years, cutting it from $12.2 billion in 2010 to $11.2 billion in 2016. They cannot pretend that budget cuts of this magnitude have no effect.

Obviously, these massive cuts reduce the amount of funding the IRS could devote to system upgrades. These cuts also impair the ability of the IRS to hire and retain staff needed to modernize and replace outdated information systems.

As a result of these massive cuts, the IRS IT staff has dropped from 7,385 employees in 2011 to 6,730 employees today.

I completely agree that Federal agencies desperately need to upgrade their information technology systems. But if we want to talk about a ticking time bomb, let's talk about it. The ticking time bomb here is that Republicans keep slashing agency budgets year after year, and pretending that these actions have no negative repercussions.

Just yesterday, Republicans on the House Appropriations Committee released their fiscal year 2017 budget. It would slash another $236 million from the IRS budget.

We cannot expect Federal agencies to modernize, replace, and strengthen their information systems against determined, sophisticated cyber attackers without giving them the resources and tools they need to do so.

This is why I am proud to cosponsor the Information Technology Modernization Act that was recently proposed by the Obama administration and introduced in the House by my colleague from the State of Maryland, Congressman Steny Hoyer. Our fellow committee members Representatives Connolly, Lieu, Kelly, and Duckworth are also cosponsoring this bill.

The bill would improve cybersecurity by establishing a dedicated $3.1 billion information technology modernization fund to help agencies replace their outdated information systems with more modern, adaptive, and secure systems. The bill would take some of the best practices from the private sector by establishing a revolving loan fund that would be dedicated for the purpose of funding wholesale upgrades and replacing outdated information technology infrastructure. The fund would be self-sustaining because agencies that receive money for modernization projects would be required to repay it over time.

By doing this, the bill would ensure that the fund can continue to support modernization projects into the future.

The bill also would create an independent review board with experts in acquisition and cybersecurity to oversee the fund and review proposals from agencies to upgrade their systems. The board would provide technical support to agencies in implementing modernization plans, and it would provide regular monitoring to ensure that every project that receives funding would be subject to centralized oversight and expertise.

As the Government Accountability Office's newly released report on Federal agency IT systems found, Federal agencies spend almost 75 percent of their budgets on maintaining current computer systems—75 percent—which leaves little for funding the development of more modern but costly technologies that are more secure.

We hope to have the support of our chairman for this landmark legislation. And the chairman is absolutely right, this is not something that should be done on a partisan basis. This is, indeed, a bipartisan problem that must have bipartisan solutions.

So I want to thank you, Mr. Chairman, for calling this important hearing, and I look forward to the testimony of our witnesses today. And with that, I yield back.

Chairman CHAFFETZ. I thank the gentleman.

I would like to ask unanimous consent to enter into the record two documents. The first is a spreadsheet demonstrating that, since President Obama took office until now, there is $6 billion in annual funding increases since the President took office. Despite the comments earlier, there are billions of dollars on an annual basis more being spent on IT.

I would also ask unanimous consent to enter into the record the GAO summary of major information technology acquisition failures. The total about $8 billion, things that have been started and scuttled, everything from NOAA to the Department of Defense to Veterans Affairs to Homeland Security. I ask unanimous consent to enter that into the record as well.

Without objection, so ordered.

Chairman CHAFFETZ. I want to hold the record open for 5 legislative days for any members who would like to submit a written statement.

It is now time to recognize our witnesses.

I am pleased to welcome Mr. Dave Powner, director of IT management issues at the Government Accountability Office. I appreciate your expertise. You have testified before, and we are glad to have you here.

Mr. Terry Milholland, chief technology officer at the Internal Revenue Service at the Department of the Treasury, thanks for being with us again.

Mr. Terry Halvorsen, chief information officer at the Department of Defense. Again, we welcome you, Mr. Halvorsen, and your presence again before this committee.

Ms. Beth Killoran—did I pronounce it properly?

Ms. KILLORAN. Killoran.

Chairman CHAFFETZ. Killoran. I believe this is your first time testifying in front of Congress, and we welcome you here today.

She is the acting Deputy Assistant Secretary for information technology and chief information officer at the Department of Health and Human Services.

Thank you for being here.

And the Honorable Tony Scott, the Federal chief information officer at the Office of Management and Budget.

Welcome and thank you all for being here.

Pursuant to committee rules, witnesses are to be sworn before they testify.

If you will please rise and raise your right hand?

Do you solemnly swear or affirm that the testimony you are about to give will be the truth, the whole truth, and nothing but the truth?

Thank you. Let the record reflect that all witnesses answered in the affirmative.

We would appreciate you limiting your verbal comments to 5 minutes. Your entire written statement will be entered into the record. We will give you a little latitude, but if it gets to be too long, we will cut you off, so we can ask some pertinent questions.

But, again, we appreciate you being here.

Mr. Powner, you are now recognized for 5 minutes.

WITNESS STATEMENTS

STATEMENT OF DAVE POWNER

Mr. POWNER. Chairman Chaffetz, Ranking Member Cummings, members of the committee, thank you for holding this hearing that highlights a significant issue for our Nation. We have too many old legacy systems that are not serving citizens well, cost too much to maintain, are at risk of failing, and pose significant security vulnerabilities.

This morning, I will summarize some of these systems and why we got into the situation, the dire security situation these systems pose, and what needs to occur to fix this issue.

I would like to start by highlighting the fact that the Federal Government spends roughly 75 percent of its IT dollars on operations and maintenance and only 25 percent on modernizing or new development. So last year, roughly $60 billion was spent on legacy, and $20 billion went to new development. Some of this legacy goes toward duplicative systems and inefficient data centers. In your committee hearing last week, you administered FITARA implementation grades that directly address this, could move savings from the legacy bucket to development, and greatly help the situation.

At that hearing, Commerce CIO Steve Cooper illustrated this best when he discussed significant savings resulting from consolidating data centers and how these funds can be moved toward new modernization efforts.

Within that $60 billion spent are many old legacy systems, some of which have components over 50 years old. Our report being released today highlights numerous systems that are still being run with outdated languages, like Assembly, COBOL, and Fortran; have old parts that are obsolete and difficult to find; and contain hardware and software that is no longer supported by vendors.

A key point here is that many of these systems are tied to mission-critical functions, not just administrative or financial management systems, not to downplay the importance of those systems. But our report highlights these aging systems that process our tax returns, coordinate operational functions for nuclear forces, determine Social Security eligibility and amounts. In addition, these aging systems maintain information on hazardous materials important to the Department of Transportation. They also serve as a key communications hub for our Nation's weather warnings.

A couple key reasons why we have this situation is CIO tenure and poor governance over IT spending. The average CIO tenure is roughly only 2 years, and most CIOs are not tackling these large modernization efforts that typically involve massive application and data conversions.

Also, agency IT governance over legacy spending is typically either lacking or poor at best. Not only are these old systems difficult and expensive to maintain because agencies have to rehire retired programmers or pay a premium to vendors for such services, but they also pose significant security risks.

Having all this unsupported hardware and software is a recipe for security breaches. In fact, during our review, we asked for and took pictures of these older systems, and four agencies told us that they could not provide us with these pictures because that alone created significant security concerns.

This is a difficult yet fixable problem. To address this situation, agencies need to first identify and prioritize their old legacy systems in need of replacement. Tony Scott's draft guidance does just this, and this committee's inquiries also help agencies to complete this first step.

Next, agencies need to develop replacement plans with clear milestones for their replacement efforts. Our report highlights far too many instances where these plans are not in place.

Finally, these plans need to be implemented effectively by tackling these efforts incrementally and having aggressive governance that monitors progress that should include clear transparency on the IT dashboard.

Again, your FITARA implementation grades that stress incremental development and accurate CIO ratings could be extremely helpful in fixing the government's aging legacy system problem.

Mr. Chairman, thank you for your leadership on this important issue, and I look forward to your questions.

[Prepared statement of Mr. Powner follows:]

United States Government Accountability Office

GAO

Testimony
Before the Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 9:00 a.m. ET
Wednesday, May 25, 2016

INFORMATION TECHNOLOGY

Federal Agencies Need to Address Aging Legacy Systems

David A. Powner, Director, Information Technology Management Issues

GAO Highlights

Highlights of GAO-16-696T, a testimony before the Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

The President's fiscal year 2017 budget request for IT was more than $89 billion, with much of this amount reportedly for operating and maintaining existing (legacy) IT systems. Given the magnitude of these investments, it is important that agencies effectively manage their IT O&M investments.

GAO was asked to summarize its report being released today that (1) assesses federal agencies' IT O&M spending, (2) evaluates the oversight of at-risk legacy investments, and (3) assesses the age and obsolescence of federal IT.

In preparing the report on which this testimony is based, GAO reviewed 26 agencies' IT O&M spending plans for fiscal years 2010 through 2017 and OMB data. GAO further reviewed the 12 agencies that reported the highest planned IT spending for fiscal year 2015 to provide specifics on agency spending and individual investments.

What GAO Recommends

In the report being released today, GAO is making multiple recommendations, one of which is for OMB to finalize draft guidance to identify and prioritize legacy IT needing to be modernized or replaced. In the report, GAO is also recommending that selected agencies address obsolete legacy IT O&M investments. Nine agencies agreed with GAO's recommendations, two partially agreed, and two stated they had no comment. The two agencies that partially agreed, the Departments of Defense and Energy, outlined plans that were consistent with the intent of GAO's recommendations.

View GAO-16-696T. For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

May 2016

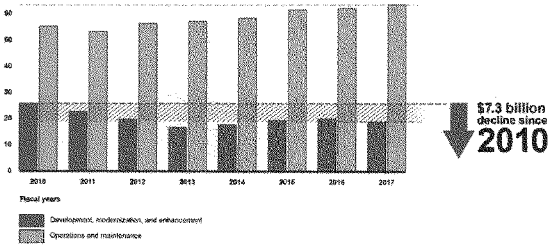
INFORMATION TECHNOLOGY

Federal Agencies Need to Address Aging Legacy Systems

What GAO Found

The federal government spent more than 75 percent of the total amount budgeted for information technology (IT) for fiscal year 2015 on operations and maintenance (O&M) investments. Specifically, 5,233 of the government's approximately 7,000 IT investments are spending all of their funds on O&M activities. Such spending has increased over the past 7 fiscal years, which has resulted in a $7.3 billion decline from fiscal years 2010 to 2017 in development, modernization, and enhancement activities.

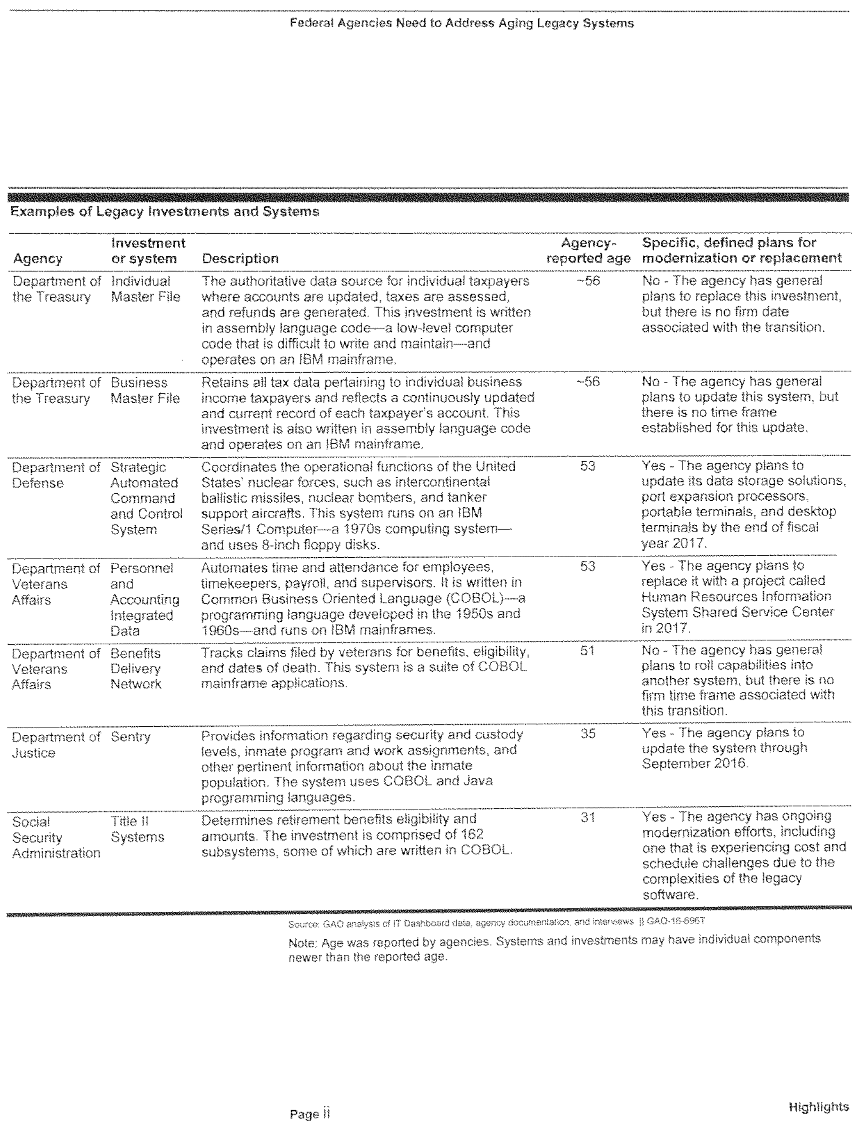
Total Federal IT Spending by Type (in billions)



Source: GAO analysis of agency data. | GAO-16-696T

Many IT O&M investments in GAO's review were identified as moderate to high risk by agency CIOs and agencies did not consistently perform required analysis of these at-risk investments. Until agencies fully review their at-risk investments, the government's oversight of such investments will be limited and its spending could be wasteful.

Federal legacy IT investments are becoming increasingly obsolete: many use outdated software languages and hardware parts that are unsupported. Agencies reported using several systems that have components that are, in some cases, at least 50 years old. For example, the Department of Defense uses 8-inch floppy disks in a legacy system that coordinates the operational functions of the nation's nuclear forces. In addition, the Department of the Treasury uses assembly language code—a computer language initially used in the 1950s and typically tied to the hardware for which it was developed. OMB recently began an initiative to modernize, retire, and replace the federal government's legacy IT systems. As part of this, OMB drafted guidance requiring agencies to identify, prioritize, and plan to modernize legacy systems. However, until this policy is finalized and fully executed, the government runs the risk of maintaining systems that have outlived their effectiveness. The following table provides examples of legacy systems across the federal government that agencies report are 30 years or older and use obsolete software or hardware, and identifies those that do not have specific plans with time frames to modernize or replace these investments.



Examples of Legacy Investments and Systems

Agency	Investment or system	Description	Agency-reported age	Specific, defined plans for modernization or replacement
Department of the Treasury	Individual Master File	The authoritative data source for individual taxpayers where accounts are updated, taxes are assessed, and refunds are generated. This investment is written in assembly language code—a low-level computer code that is difficult to write and maintain—and operates on an IBM mainframe.	~56	No - The agency has general plans to replace this investment, but there is no firm date associated with the transition.
Department of the Treasury	Business Master File	Retains all tax data pertaining to individual business income taxpayers and reflects a continuously updated and current record of each taxpayer's account. This investment is also written in assembly language code and operates on an IBM mainframe.	~56	No - The agency has general plans to update this system, but there is no time frame established for this update.
Department of Defense	Strategic Automated Command and Control System	Coordinates the operational functions of the United States' nuclear forces, such as intercontinental ballistic missiles, nuclear bombers, and tanker support aircrafts. This system runs on an IBM Series/1 Computer—a 1970s computing system—and uses 8-inch floppy disks.	53	Yes - The agency plans to update its data storage solutions, port expansion processors, portable terminals, and desktop terminals by the end of fiscal year 2017.
Department of Veterans Affairs	Personnel and Accounting Integrated Data	Automates time and attendance for employees, timekeepers, payroll, and supervisors. It is written in Common Business Oriented Language (COBOL)—a programming language developed in the 1950s and 1960s—and runs on IBM mainframes.	53	Yes - The agency plans to replace it with a project called Human Resources Information System Shared Service Center in 2017.
Department of Veterans Affairs	Benefits Delivery Network	Tracks claims filed by veterans for benefits, eligibility, and dates of death. This system is a suite of COBOL mainframe applications.	51	No - The agency has general plans to roll capabilities into another system, but there is no firm time frame associated with this transition.
Department of Justice	Sentry	Provides information regarding security and custody levels, inmate program and work assignments, and other pertinent information about the inmate population. The system uses COBOL and Java programming languages.	35	Yes - The agency plans to update the system through September 2016.
Social Security Administration	Title II Systems	Determines retirement benefits eligibility and amounts. The investment is comprised of 162 subsystems, some of which are written in COBOL.	31	Yes - The agency has ongoing modernization efforts, including one that is experiencing cost and schedule challenges due to the complexities of the legacy software.

Source: GAO analysis of IT Dashboard data, agency documentation, and interviews. || GAO-16-696T

Note: Age was reported by agencies. Systems and investments may have individual components newer than the reported age.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee

Thank you for the opportunity to participate in today's hearing on the federal government's legacy information technology (IT) systems. The President's fiscal year 2017 budget request for IT was more than $89 billion, with over 70 percent reportedly for operating and maintaining existing IT systems. Given the size and magnitude of these investments, it is important that agencies effectively manage the operations and maintenance (O&M) of existing investments.

As requested, this statement summarizes our report being released today that (1) assesses federal agencies' IT O&M spending, (2) evaluates the oversight of at-risk legacy investments, and (3) assesses the age and obsolescence of federal IT.[1]

In that report, our review of O&M spending included the Office of Management and Budget (OMB) and the 26 agencies that report to OMB's IT Dashboard.[2] For specific information on individual systems or investments, we focused on the 12 agencies that reported the highest planned IT spending for fiscal year 2015, given that these agencies make up over 90 percent of reported federal IT spending.[3]

[1] GAO, *Information Technology: Federal Agencies Need to Address Aging Legacy Systems*, GAO-16-468 (Washington, D.C.: May 25, 2016).

[2] In June 2009, OMB established the IT Dashboard, a public website that provides detailed information on major IT investments at 26 federal agencies. Agencies are to report, via the Dashboard, the performance of their IT investments. Currently, the Dashboard publicly displays information on the cost, schedule, and performance of over 700 major federal IT investments at 26 federal agencies. The 26 agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; U.S. Army Corps of Engineers, Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Archives and Records Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

[3] These agencies are the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Homeland Security, Justice, State, Transportation, the Treasury, Veterans Affairs, and the Social Security Administration.

To assess federal agencies' IT O&M spending, we reviewed data reported to OMB as part of the budget process for fiscal years 2010 through 2017. We analyzed that data to determine whether spending had changed over those years and compared OMB's associated performance measure to federal best practices.[4]

We evaluated the extent to which the 12 selected federal agencies are performing oversight on their existing legacy investments by reviewing agency IT Dashboard data to identify investments in O&M that had been designated as being moderate to high risk. We also reviewed agency documentation such as TechStat[5] documentation and operational analyses, as available.

To assess the age and obsolescence of federal IT, we reviewed agency documentation, such as operational analyses and enterprise architecture documents, and interviewed agency officials. We also requested that the 12 agencies provide a list of their three oldest systems. We compared OMB and agencies' current practices with federal guidance to determine whether OMB and agencies are adequately managing the age and obsolescence of federal IT.

To assess the reliability of the OMB budget data and IT Dashboard data, we reviewed related documentation, such as OMB guidance on budget preparation, capital planning, and IT Dashboard submissions. In addition, we corroborated with each agency that the data downloaded were accurate and reflected the data it had reported to OMB. We determined that the data were reliable for the purposes of our reporting objectives.

The work upon which this testimony is based was conducted in accordance with generally accepted government auditing standards.

[4] Department of the Navy, Office of the Chief Information Officer, *Guide for Developing and Using Information Technology (IT) Performance Measurements* (Washington, D.C.: October 2001); and General Services Administration, Office of Governmentwide Policy, *Performance-Based Management: Eight Steps To Develop and Use Information Technology Performance Measures Effectively* (Washington, D.C.: 1996).

[5] In January 2010, the Federal CIO began leading TechStat sessions—face-to-face meetings to terminate or turn around IT investments that are failing or are not producing results. These meetings involve OMB and agency leadership and are intended to increase accountability and improve performance. OMB also empowered agency CIOs to begin to hold their own TechStat sessions within their respective agencies by June 2012.

Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. A more detailed description of the scope and methodology of our work is provided in our report being issued today.

Background

Over the last three decades, Congress has enacted several laws to assist agencies and the federal government in managing IT investments. For example, to assist agencies in managing their investments, Congress enacted the Clinger-Cohen Act of 1996.[6] More recently, in December 2014, Congress enacted IT acquisition reform legislation (commonly referred to as the Federal Information Technology Acquisition Reform Act or FITARA)[7] that, among other things, requires OMB to develop standardized performance metrics, including cost savings, and to submit quarterly reports to Congress on cost savings.

In carrying out its responsibilities, OMB uses several data collection mechanisms to oversee federal IT spending during the annual budget formulation process. Specifically, OMB requires federal departments and agencies to provide information related to their Major Business Cases (previously known as exhibit 300) and IT Portfolio Summary (previously known as exhibit 53).[8]

OMB directs agencies to break down IT investment costs into two categories: (1) O&M and (2) development, modernization, and enhancement (DME). O&M (also known as steady-state) costs refer to the expenses required to operate and maintain an IT asset in a production environment. DME costs refers to those projects and activities that lead to new IT assets/systems, or change or modify existing IT assets to substantively improve capability or performance.

[6] 40 U.S.C. § 11101, et seq.

[7] Pub. L. No. 113-291, div. A, title VIII, subtitle D ,128 Stat. 3292, 3438-50 (Dec. 19, 2014).

[8] OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget* (June 30, 2015).

In addition, OMB has developed guidance that calls for agencies to develop an operational analysis policy for examining the ongoing performance of existing legacy IT investments to measure, among other things, whether the investment is continuing to meet business and customer needs.[9]

Nevertheless, federal IT investments have too frequently failed or incurred cost overruns and schedule slippages while contributing little to mission-related outcomes. The federal government has spent billions of dollars on failed and poorly performing IT investments which often suffered from ineffective management, such as project planning, requirements definition, and program oversight and governance.[10]

Accordingly, in February 2015, we introduced a new government-wide high-risk area, *Improving the Management of IT Acquisitions and Operations.*[11] This area highlights several critical IT initiatives underway, including reviews of troubled projects, an emphasis on incremental development, a key transparency website, data center consolidation, and the O&M of legacy systems.

To make progress in this area, we identified actions that OMB and the agencies need to take. These include implementing the recently-enacted statutory requirements promoting IT acquisition reform, as well as implementing our previous recommendations. In the last 6 years, we made approximately 800 recommendations to OMB and multiple agencies to improve effective and efficient investment in IT. As of October 2015, about 32 percent of these recommendations had been implemented.

[9] OMB, *Preparation, Submission, and Execution of the Budget*, Circular No. A-11 (June 30, 2015); OMB Memorandum M-10-27 (June 2010), requires agencies to establish a policy for performing operational analyses on steady-state investments as a part of managing and monitoring investment baselines. Parts of this guidance do not apply to the Department of Defense.

[10] GAO, *Information Technology: OMB and Agencies Need to More Effectively Implement Major Initiatives to Save Billions of Dollars*, GAO-13-796T (Washington, D.C.: July 25, 2013).

[11] GAO, *High-Risk Series: An Update,* GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

GAO Has Reported on the Need to Improve Oversight of Legacy IT

We have previously reported on legacy IT and the need for the federal government to improve its oversight of such investments. For example, in October 2012,[12] we reported on agencies' operational analyses policies and practices. In particular, we reported that although OMB guidance called for each agency to develop an operational analysis policy and perform such analyses annually, the extent to which the selected federal agencies we reviewed carried out these tasks varied significantly. The Departments of Defense (Defense), the Treasury (Treasury), and Veterans Affairs (VA) had not developed a policy or conducted operational analyses.

As such, we recommended that the agencies develop operational analysis policies, annually perform operational analyses on all investments, and ensure the assessments include all key factors. Further, we recommended that OMB revise its guidance to include directing agencies to post the results of such analyses on the IT Dashboard. OMB and the five selected agencies agreed with our recommendations and have efforts planned and underway to address them. In particular, OMB issued guidance in August 2012 directing agencies to report operational analysis results along with their fiscal year 2014 budget submission documentation (e.g., exhibit 300) to OMB. Thus far, operational analyses have not yet been posted on the IT Dashboard.

We further reported in November 2013 that agencies were not conducting proper analyses. Specifically, we reported[13] on IT O&M investments and the use of operational analyses at selected agencies and determined that of the top 10 investments with the largest spending in O&M, only a Department of Homeland Security (DHS) investment underwent an operational analysis. DHS's analysis addressed most, but not all, of the factors that OMB called for (e.g., comparing current cost and schedule against original estimates). The remaining agencies did not assess their investments, which accounted for $7.4 billion in reported O&M spending. Consequently, we recommended that seven agencies perform

[12] GAO, *Information Technology: Agencies Need to Strengthen Oversight of Billions of Dollars in Operations and Maintenance Investments,* GAO-13-87 (Washington, D.C.: Oct. 16, 2012).

[13] GAO, *Information Technology: Agencies Need to Strengthen Oversight of Multibillion Dollar Investments in Operations and Maintenance,* GAO-14-66 (Washington, D.C.: Nov. 6, 2013).

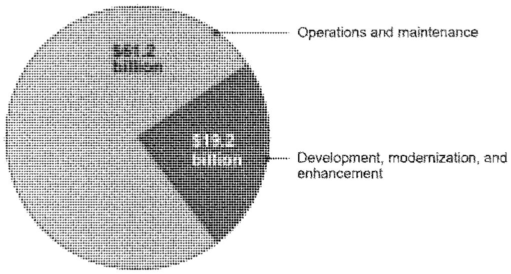
operational analyses on their IT O&M investments and that DHS ensure that its analysis was complete and addressed all OMB factors. Three of the agencies agreed with our recommendations; two partially agreed; and two agencies had no comments.

Government-wide Spending on IT Operations and Maintenance Is Increasing

As discussed in our report, federal agencies reported spending the majority of their fiscal year 2015 IT funds on operating and maintaining a large number of legacy (i.e., steady-state) investments. Of the more than $80 billion reportedly spent on federal IT in fiscal year 2015, 26 federal agencies[14] spent about $61 billion on O&M, more than three-quarters of the total amount spent. Specifically, data from the IT Dashboard shows that, in 2015, 5,233 of the government's nearly 7,000 IT investments were spending all of their funds on O&M activities. This is a little more than three times the amount spent on DME activities (see figure 1).

[14] This $80 billion represents what 26 agencies reported to OMB on planned IT spending. However, this $80 billion figure is understated. This figure does not include spending for Defense classified IT systems; and 58 independent executive branch agencies, including the Central Intelligence Agency. Additionally, not all executive branch IT investments are included in this estimate because agencies have differed on what they considered an IT investment. For example, some have considered research and development systems as IT investments, while others have not.

Figure 1: Fiscal Year 2015 Federal Spending on IT Operations and Maintenance and Development, Modernization, and Enhancement



Source: GAO analysis of Office of Management and Budget's Information Technology Dashboard | GAO-16-696T

According to agency data reported to OMB's IT Dashboard, the 10 IT investments spending the most on O&M for fiscal year 2015 total $12.5 billion, 20 percent of the total O&M spending, and range from $4.4 billion on Department of Health and Human Services' (HHS) Centers for Medicare and Medicaid Services' Medicaid Management Information System[15] to $666.1 million on HHS's Centers for Medicare and Medicaid Services IT Infrastructure investment (see table 1).

[15] The 50 states, the District of Columbia, and the 5 U.S. territories each administer a state-based Medicaid program. Every state must implement a claims processing and information retrieval system to support the administration of the program. This investment represents the federal share of state Medicaid systems' cost. In technical comments on a draft of our report, HHS stated that it does not manage any of these IT assets or control how this money is spent.

Table 1: Ten Largest Expenditures on Operations and Maintenance Investments in Fiscal Year 2015, in millions

Agency	Investment	Fiscal year 2015 funds in millions
Department of Health and Human Services	Centers for Medicare and Medicaid Services' Medicare Management Information System[a]	$4,381.0
Department of Defense	Defense Information Systems Network	$1,252.2
Department of Veterans Affairs	Medical IT Support	$1,234.9
Department of Defense	Next Generation Enterprise Network Increment 1	$1,057.7
Social Security Administration	Infrastructure Operations and Maintenance	$864.0
Department of Veterans Affairs	Enterprise IT Support	$809.5
Department of Defense	Network Enterprise Technology Command	$767.5
Department of Defense	Network Enterprise Center Staff Operations Costs	$752.8
Department of Defense	Non-Defense Information Systems Network Telecomm	$688.8
Department of Health and Human Services	Centers for Medicare and Medicaid Services IT Infrastructure – Ongoing	$666.1
Total		**$12,474.5 million**

Source: GAO analysis of agency budgetary data. | GAO-16-696T

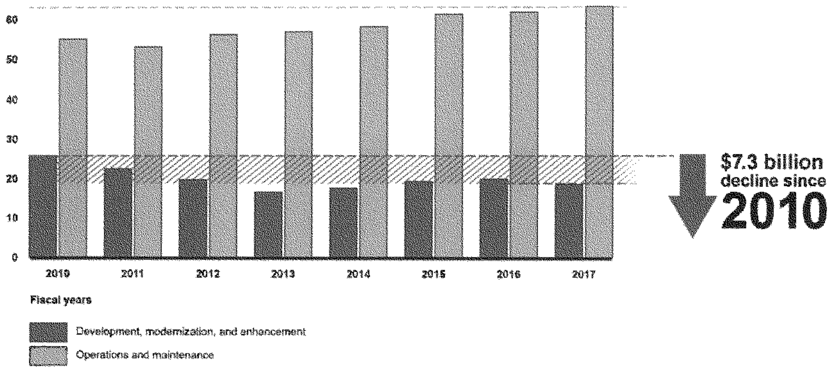
Note:

[a] This investment represents the federal share of state Medicaid systems' cost. In technical comments on a draft of our report, the Department of Health and Human Services stated that it does not manage any of these IT assets or control how this money is spent.

Spending on O&M Has Increased over 7 Years

Over the past 7 fiscal years, O&M spending has increased, while the amount invested in developing new systems has decreased by about $7.3 billion since fiscal year 2010. (See figure 2.)

Figure 2: Summary of IT Spending by Fiscal Year from 2010 through 2017 (Dollars in Billions)



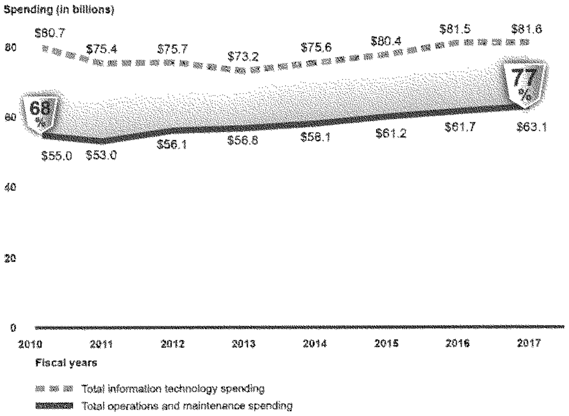
$7.3 billion decline since 2010

Source: GAO analysis of agency data. | GAO-16-696T

Note: According to DOD officials, the department's fiscal year 2010 IT expenditures reported to the IT Dashboard includes both classified and unclassified spending, whereas its fiscal year 2011 to 2017 expenditures only include unclassified spending.

Further, agencies have increased the amount of O&M spending relative to their overall IT spending by 9 percent since 2010. Specifically, in fiscal year 2010, O&M spending was 68 percent of the federal IT budget, while in fiscal year 2017, agencies plan to spend 77 percent of their IT funds on O&M. (See figure 3.)

Figure 3: Percentage of IT Spending on Operations and Maintenance from Fiscal Year 2010 to Fiscal Year 2017



Source: GAO analysis of agency data. | GAO-16-696T

Further, 15 of the 26 agencies have increased their spending on O&M from fiscal year 2010 to fiscal year 2015, with 10 of these agencies having over a $100 million increase. The spending changes per agency range from an approximately $4 billion increase (HHS) to a decrease of $600 million (National Aeronautics and Space Administration).

OMB staff in the Office of E-Government and Information Technology have recognized the upward trend of IT O&M spending and identified several contributing factors, including (1) the support of O&M activities requires maintaining legacy hardware, which costs more over time, and (2) costs are increased in maintaining applications and systems that use older programming languages, since programmers knowledgeable in these older languages are becoming increasingly rare and thus more expensive. Further, OMB officials stated that in several situations where agencies are not sure whether to report costs as O&M or DME, agencies default to reporting as O&M. According to OMB, agencies tend to categorize investments as O&M because they attract less oversight, require reduced documentation, and have a lower risk of losing funding.

Many O&M Investments Were at Risk and Lacked Proper Oversight

According to OMB guidance,[16] the O&M phase is often the longest phase of an investment and can consume more than 80 percent of the total lifecycle costs. As such, agencies must actively manage their investment during this phase. To help them do so, OMB requires that CIOs submit ratings that reflect the level of risk facing an investment.

In addition, in instances where investments experience problems, agencies can perform a TechStat, a face-to-face meeting to terminate or turn around IT investments that are failing or not producing results.[17] In addition, OMB directs agencies to monitor O&M investments through operational analyses, which should be performed annually and assess costs, schedules, whether the investment is still meeting customer and business needs, and investment performance.

Several O&M investments were rated as moderate to high risk in fiscal year 2015.[18] Specifically, CIOs from the 12 selected agencies reported that 23 of their 187 major IT O&M investments were moderate to high risk as of August 2015. They requested $922.9 million in fiscal year 2016 for these investments. Of the 23 investments, agencies had plans to replace or modernize 19 investments. However, the plans for 12 of those were general or tentative in that the agencies did not provide specificity on time frames, activities to be performed, or functions to be replaced or enhanced. Further, agencies did not plan to modernize or replace 4 of the investments (see table 2). The lack of specific plans to modernize or replace these investments could result in wasteful spending on moderate and high-risk investments.

[16] OMB, *Preparation, Submission, and Execution of the Budget,* Circular No. A-11 (2015).

[17] OMB, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Washington, D.C.: Dec. 9, 2010).

[18] Agencies submit ratings on major investments from their CIO, which, according to OMB's instructions, should reflect the level of risk facing an investment relative to that investment's ability to accomplish its goals. To do so, each agency CIO is to assess his or her IT investments against a set of six pre-established evaluation factors identified by OMB and then assign a rating of 1 (high risk and red) to 5 (low risk and green) based on the CIO's best judgement of the level of risk facing the investment.

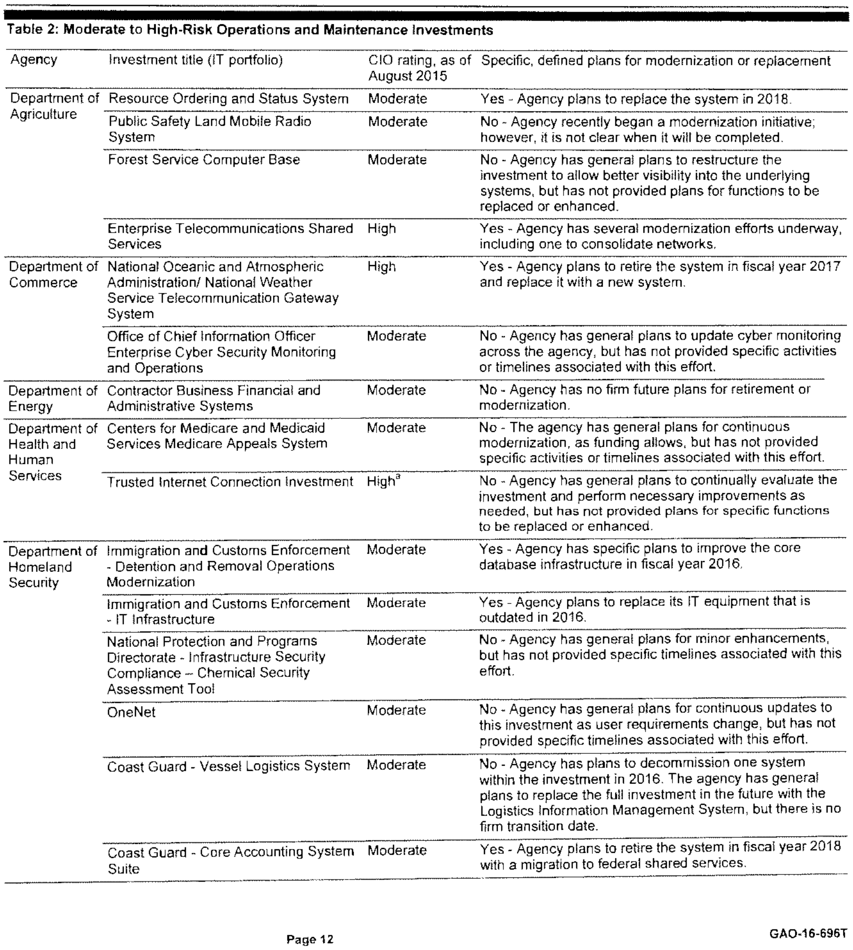


Table 2: Moderate to High-Risk Operations and Maintenance Investments

Agency	Investment title (IT portfolio)	CIO rating, as of August 2015	Specific, defined plans for modernization or replacement
Department of Agriculture	Resource Ordering and Status System	Moderate	Yes - Agency plans to replace the system in 2018.
	Public Safety Land Mobile Radio System	Moderate	No - Agency recently began a modernization initiative; however, it is not clear when it will be completed.
	Forest Service Computer Base	Moderate	No - Agency has general plans to restructure the investment to allow better visibility into the underlying systems, but has not provided plans for functions to be replaced or enhanced.
	Enterprise Telecommunications Shared Services	High	Yes - Agency has several modernization efforts underway, including one to consolidate networks.
Department of Commerce	National Oceanic and Atmospheric Administration/ National Weather Service Telecommunication Gateway System	High	Yes - Agency plans to retire the system in fiscal year 2017 and replace it with a new system.
	Office of Chief Information Officer Enterprise Cyber Security Monitoring and Operations	Moderate	No - Agency has general plans to update cyber monitoring across the agency, but has not provided specific activities or timelines associated with this effort.
Department of Energy	Contractor Business Financial and Administrative Systems	Moderate	No - Agency has no firm future plans for retirement or modernization.
Department of Health and Human Services	Centers for Medicare and Medicaid Services Medicare Appeals System	Moderate	No - The agency has general plans for continuous modernization, as funding allows, but has not provided specific activities or timelines associated with this effort.
	Trusted Internet Connection Investment	High[a]	No - Agency has general plans to continually evaluate the investment and perform necessary improvements as needed, but has not provided plans for specific functions to be replaced or enhanced.
Department of Homeland Security	Immigration and Customs Enforcement - Detention and Removal Operations Modernization	Moderate	Yes - Agency has specific plans to improve the core database infrastructure in fiscal year 2016.
	Immigration and Customs Enforcement - IT Infrastructure	Moderate	Yes - Agency plans to replace its IT equipment that is outdated in 2016.
	National Protection and Programs Directorate - Infrastructure Security Compliance – Chemical Security Assessment Tool	Moderate	No - Agency has general plans for minor enhancements, but has not provided specific timelines associated with this effort.
	OneNet	Moderate	No - Agency has general plans for continuous updates to this investment as user requirements change, but has not provided specific timelines associated with this effort.
	Coast Guard - Vessel Logistics System	Moderate	No - Agency has plans to decommission one system within the investment in 2016. The agency has general plans to replace the full investment in the future with the Logistics Information Management System, but there is no firm transition date.
	Coast Guard - Core Accounting System Suite	Moderate	Yes - Agency plans to retire the system in fiscal year 2018 with a migration to federal shared services.

	Coast Guard - Standard Workstation Infrastructure Recapitalization and Sustainment	Moderate	No - Agency has general plans, including a migration to Windows 10, but did not provide dates on when this would happen.
	Customs and Border Protection - Tactical Communications Modernization	Moderate	Yes - Agency plans to decommission obsolete equipment by the end of fiscal year 2017.
	Customs and Border Protection - Integrated Fixed Towers	High[a]	No - Agency has no plans for retirement or modernization at this time because the investment only reached initial operating capability in October 2015. It plans to reach final operating capability in fiscal year 2020.
	National Protection and Programs Directorate – Federal Protective Service Tac Com Equipment and Support	Moderate	No - Agency has general plans to update the program, but no firm date associated with the effort.
	Customs and Border Protection - Tethered Aerostat Radar System	Moderate	No - Agency has no plans for replacement or modernization of the investment, but is currently undergoing an analysis of alternatives to determine whether they should modemize or replace the system.
	Customs and Border Protection – TRIRIGA	Moderate	No - Agency has no plans for replacement or modernization of the investment.
Department of the Treasury	Departmental Offices IT Infrastructure Mainframes and Servers Services and Support	Moderate	No - Agency has general plans to update this investment, but has not provided specific activities or timelines associated with this effort.
	Departmental Offices IT Infrastructure End User Systems and Support	Moderate	No - Agency has general plans to update this investment, but has not provided specific activities or timelines associated with this effort.

Source: GAO analysis of IT Dashboard data, agency documentation, and interviews. | GAO-16-969T

Note:

[a]According to agency officials, this investment has since been lowered to moderate risk.

While agencies generally conducted the required operational analyses, they did not consistently perform TechStat reviews on all of the at-risk investments. Although not required, agencies had performed TechStats on only five of the 23 at-risk investments. In addition, operational analyses were not conducted for four of these investments (see table 3).

Table 3: At-Risk Investments and Required Analyses and Oversight Activities

Agency	Investment	TechStat performed	Operational analysis performed
Department of Agriculture	Resource Ordering and Status System	X	X
	Public Safety Land Mobile Radio System		X
	Forest Service Computer Base		X
	Enterprise Telecommunications Shared Services		X
Department of Commerce	National Oceanic and Atmospheric Administration / National Weather Service Telecommunication Gateway System	X	X

	Office of Chief Information Officer Enterprise Cyber Security Monitoring and Operations		
Department of Energy	Contractor Business Financial and Administrative Systems	X	X
Department of Health and Human Services	Centers for Medicare and Medicaid Services Medicare Appeals System	X	X
	Trusted Internet Connection Investment		X
Department of Homeland Security	Immigration and Customs Enforcement - Detention and Removal Operations Modernization		X
	Immigration and Customs Enforcement - IT Infrastructure		X
	National Protection and Programs Directorate - Infrastructure Security Compliance – Chemical Security Assessment Tool		X
	OneNet		X
	Coast Guard - Vessel Logistics System		X
	Coast Guard - Core Accounting System Suite		X
	Coast Guard - Standard Workstation Infrastructure Recapitalization and Sustainment		X
	Customs and Border Protection - Tactical Communications Modernization		X
	Customs and Border Protection - Integrated Fixed Towers		
	National Protection and Programs Directorate – Federal Protective Service Tac Com Equipment and Support	X	X
	Customs and Border Protection - Tethered Aerostat Radar System		X
	Customs and Border Protection – TRIRIGA		X
Department of the Treasury	Departmental Offices IT Infrastructure Mainframes and Servers Services and Support		
	Departmental Offices IT Infrastructure End User Systems and Support		

Source: GAO analysis of agency documentation. | GAO-16-696T

Agencies provided several reasons for not conducting TechStats and required assessments. For example, according to agency officials, several of the investments' risk levels were reduced to low or moderately low risk in the months since the IT Dashboard had been publicly updated.[19] Regarding assessments, one official stated that, in place of operational analyses, the responsible bureau reviews the status of the previous month's activities for the development, integration, modification, and procurement to report issues to management. However, this monthly process does not include all of the key elements of an operational analysis. Until agencies ensure that their O&M investments are fully

[19] The public portion of the IT Dashboard is not updated during the formulation of President's Budget.

reviewed, the government's oversight of old and vulnerable investments will be impaired and the associated spending could be wasteful.

IT Investments Are Becoming Obsolete and Agencies Are Not Required to Identify Investments That Need Attention

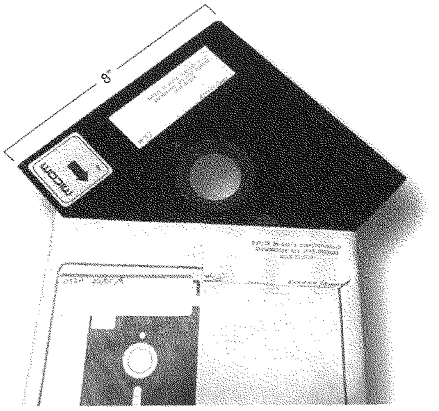
Legacy IT investments across the federal government are becoming increasingly obsolete. Specifically, many use outdated languages and old parts. Numerous old investments are using obsolete programming languages. Several agencies, such as the Department of Agriculture (USDA), DHS, HHS, Justice, Treasury, and VA, reported using Common Business Oriented Language (COBOL)—a programming language developed in the late 1950s and early 1960s—to program their legacy systems. It is widely known that agencies need to move to more modern, maintainable languages, as appropriate and feasible. For example, the Gartner Group, a leading IT research and advisory company, has reported that organizations using COBOL should consider replacing the language and in 2010 noted that there should be a shift in focus to using more modern languages for new products.[20]

In addition, some legacy systems may use parts that are obsolete and more difficult to find. For instance, Defense is still using 8-inch floppy disks in a legacy system that coordinates the operational functions of the United States' nuclear forces.[21] (See figure 4.)

[20] Gartner, *IT Market Clock for Application Development*, August 2010.

[21] Introduced in the 1970s, the 8-inch floppy disk is a disk-based storage medium that holds 80 kilobytes of data. In comparison, a single modern flash drive can contain data from the equivalent of more than 3.2 million floppy disks.

Figure 4: Example of an 8-Inch Floppy Disk



Source: GAO | GAO-16-696T

Further, in some cases, the vendors no longer provide support for hardware or software, creating security vulnerabilities and additional costs. For example, each of the 12 selected agencies reported using unsupported operating systems and components in their fiscal year 2014 reports pursuant to the Federal Information Security Management Act of 2002. Commerce, Defense, Treasury, HHS, and VA reported using 1980s and 1990s Microsoft operating systems that stopped being supported by the vendor more than a decade ago.

Lastly, legacy systems may become increasingly more expensive as agencies have to deal with the previously mentioned issues and may pay a premium to hire staff or contractors with the knowledge to maintain outdated systems. For example, one agency (SSA) reported re-hiring retired employees to maintain its COBOL systems.

Selected agencies reported that they continue to maintain old investments in O&M. For example, Treasury reported systems that were about 56 years old.

Table 4 shows the 10 oldest investments and/or systems, as reported by selected agencies.[22] Agencies reported having plans to modernize or replace each of these investments and systems. However, the plans for five of those were general or tentative in that the agencies did not provide specific time frames, activities to be performed, or functions to be replaced or enhanced.

Table 4: Ten Oldest IT Investments or Systems as Reported by 12 Selected Agencies

Agency	Investment or system	Description	Agency-reported age	Specific, defined plans for modernization or replacement
Department of the Treasury	Individual Master File	This investment is the authoritative data source for individual taxpayer accounts where accounts are updated, taxes are assessed, and refunds are generated during the tax filing period. It is written in assembly language code—a low-level computer code, initially used in the 1950s, that is difficult to write and maintain and is typically tied to the hardware for which it was developed.	~56	No - A new investment will eventually replace this investment, but there is no firm date associated with the transition.
Department of the Treasury	Business Master File	This investment retains all tax data pertaining to individual business income taxpayers and reflects a continuously updated and current record of each taxpayer's account. It is also written in assembly language code and operates on an IBM mainframe.	~56	No - The agency has general plans to update this system, but there is no date associated with this update.
Department of Defense	Strategic Automated Command and Control System	This system coordinates the operational functions of the United States' nuclear forces, such as intercontinental ballistic missiles, nuclear bombers, and tanker support aircrafts. It runs on an IBM Series/1 Computer—a 1970s computing system—and uses 8-inch floppy disks.	53	Yes - The agency is planning to update data storage solutions, port expansion processors, portable terminals, and desktop terminals, which are all scheduled to be completed by the end of fiscal year 2017.

[22] Not all agencies track systems and their associated ages in the same manner—some track individual systems and others track by investment. An investment may be made up of several systems and infrastructure. In some cases, agencies were unsure of the actual age of the system or investment and had to approximate the initiation date.

Department of Veterans Affairs	Personnel and Accounting Integrated Data	This system automates time and attendance for employees, timekeepers, payroll, and supervisors. It is written in COBOL—a programming language developed in the 1950s and 1960s—and runs on IBM mainframes.	53	Yes - The agency plans to replace it with a project called Human Resources Information System Shared Service Center in 2017.
Department of Defense	Compass	This system is a command and control system that is used for deliberate and crisis action planning, strategic mobility analysis, and mobilization and deployment movement execution. It runs on a Windows 2008 server and is programed in Java—a programming language first released in 1995. It also uses a 2009 Oracle 11g database.	52	Yes - The system is currently using an Oracle 11g database, but the agency plans to migrate it a 2012 SQL server by the end of the year.
Department of Veterans Affairs	Benefits Delivery Network	This system tracks claims filed by veterans for benefits, eligibility, and dates of death. It is a suite of COBOL mainframe applications.	51	No - The agency has general plans to roll capabilities into another system, but there is no firm date associated with this transition.
Department of Transportation	Hazardous Materials Information System at the Pipeline and Hazardous Materials Safety Administration	This system allows the agency to maintain comprehensive information on hazardous materials incidents. The software applications and processes used by the system, such as Classic Active Server Pages and Microsoft.NET, have become outdated and costly to maintain. In addition, the system uses an application that is no longer supported by the manufacturer, which can cause security risks, among other issues.	~46	Yes - All legacy components within this system are scheduled to be replaced by 2018.
Department of Commerce	National Oceanic and Atmospheric Administration/ National Weather Service Dissemination Systems	This investment includes three information dissemination systems used to provide the U.S. public and emergency managers warnings of severe weather events. It runs a variety of operating systems and software, including Windows Server 2003, which is no longer supported by the vendor, and uses a variety of programming languages including FORTRAN—a high-level programming language developed in the 1950s for scientific and engineering applications.	46	No - The agency has general plans to continuously update system components.
Department of Commerce	National Oceanic and Atmospheric Administration/ National Weather Service / National Data Buoy Center Ocean Observing System of Systems	This investment supports systems that include meteorological, oceanographic, tsunami, and climate observing platforms. It runs on both Windows and Linux operating systems, including Windows Server 2003, which is no longer supported by the vendor. In addition, it uses a version of Oracle that is also no longer fully supported by the vendor. This investment also uses a variety of programming languages, including FORTRAN.	46	No - The agency has general plans for continuous incremental upgrades to this investment.

Department of Homeland Security	Immigration and Customs Enforcement - Hiring Tracking Systems	This system is used by the agency to track current and prior hiring actions and maintains information about individuals who are selected for vacant positions. It runs on a 2008 IBM z10 mainframe using COBOL, among other languages. The web component runs on a Windows 2012 server using Java.	39	Yes - The agency plans to replace the existing mainframe with a service-oriented architecture to allow for integration with new systems beginning in fiscal year 2016, contingent upon receiving funding.

Source: GAO analysis of agency data. | GAO-16-696T

Note: Systems and investments may have selected components newer than the reported age.

Separately, in our related report, we profiled one system or investment from each of the 12 selected agencies. The selected systems and investments range from 11 to approximately 56 years old, and serve a variety of purposes. Of the 12 investments or systems, agencies had plans to replace or modernize 11 of these. However, the plans for 3 of those were general or tentative in that the agencies did not provide specificity on time frames, activities to be performed, or functions to be replaced or enhanced. Further, there were no plans to replace or modernize 1 investment.

Table 5: Summary of Investments and Systems Profiled in Related Report

Agency	Investment or system	Description	Agency-reported age	Specific, defined plans for modernization or replacement
Department of Commerce	National Weather Service Telecommunication Gateway	This investment is the nation's hub for the collection and distribution of weather data and products. The agency replaced its hardware and software with Power7 IBM servers and Unix operating systems; however, the investment still lacks full backup capability for 26 percent of its functions.	31	Yes - The agency plans to retire the system in fiscal year 2017 and replace it with a new system.
Department of Defense	Strategic Automated Command and Control System	This system coordinates the operational functions of the nation's nuclear forces. This system is running on an IBM Series/1 Computer—a 1970s computing system—and uses 8-inch floppy disks.	53	Yes - The agency is planning to update data storage solutions, port expansion processors, portable terminals, and desktop terminals by the end of fiscal year 2017. A full system replacement is scheduled to be completed in fiscal year 2020.

Department of Homeland Security	Core Accounting System Suite	This investment is the primary financial management system for the Coast Guard and other Department of Homeland Security agencies. The system relies on outdated and heavily customized Oracle Federal Financials software that was first available in 2004 and the extended vendor support for the software ended in November 2013. As a result it has become expensive to support. Further, it relies on Windows 2003 servers and any changes would require recoding of many functions within its suite. In some cases, Coast Guard is unable to upgrade the system to the newest version of software because it is dependent on older versions of supporting software.	18	Yes - The agency plans to transition to federal shared services in fiscal year 2018.
Department of Transportation	Hazardous Material Information System	This system maintains and provides access to comprehensive information on hazardous materials incidents, among other things. The software applications and processes used by the system, such as Classic Active Server Pages and Microsoft.NET, have become outdated and costly to maintain. In addition, the system uses an application that is no longer supported by the manufacturer, which can cause security risks, among other issues.	~46	Yes - The agency is developing a new system to replace legacy modules and plans to retire the legacy modules by the end of fiscal year 2018.
Department of Energy	Contractor Business Financial and Administrative Systems	This investment is the business and administrative systems for a management and operating contractor, liquid waste contractor, and the site security contractor to manage human resources, financial reporting, supply chain, and project management. It runs on Windows and Unix servers and uses Oracle's PeopleSoft applications. The investment has gone through several updates, with the last including the retirement of 16 associated legacy applications in 2011.	12	No - The agency does not have future plans for retirement or modernization.
Department of Health and Human Services	Medicare Appeals System	This system facilitates the maintenance and transfer of case-specific data with regard to Medicare appeals through multiple levels of the appeal process. The system runs on a Solaris 10 operating system and uses commercial-off-the-shelf systems for case management and reporting.	11	No - The agency has general plans to continuously update the system.
Department of Justice	Sentry	This system provides information regarding security and custody levels, inmate program and work assignments, and other pertinent information about the inmate population. When the system was first deployed, it was comprised of approximately 700 program routines written in COBOL and ran on a mainframe platform. Over the years, the agency has updated the system to allow for web accessibility.	35	Yes – The agency plans to update the user interface and integrate system data through September 2016.
Social Security Administration	Title II Systems	These systems determine retirement benefits eligibility and amounts. The investment is comprised of 162 subsystems and some are still written in COBOL.	31	Yes - The agency has ongoing modernization efforts, including one that is experiencing cost and schedule challenges due to the complexities of the legacy software.

Department of State	Diversity Visa Information System	This system is an electronic case management system to track and validate application information submitted by foreign nationals under the Diversity Visa immigration program. The interface software, PowerBuilder, is no longer supported by the vendor.	~26	No - The agency plans to replace the investment at an unknown date and has general plans to upgrade unsupported software to a new version, which is also not supported.
Department of the Treasury	Individual Master File	This investment is the authoritative data source for individual taxpayer accounts where accounts are updated, taxes are assessed, and refunds are generated during the tax filing period. This investment is written in assembly language code—a low-level computer code that is difficult to write and maintain—and operates on an IBM mainframe.	~56	No - The agency plans to replace the investment at an unknown date.
Department of Agriculture	Resource Ordering and Status System	This investment mobilizes and deploys a multitude of resources, including qualified individuals, teams, aircraft, equipment, and supplies to fight wildland fires and respond to all hazard incidents. One of the applications the system uses is no longer supported by the vendor, creating vulnerability issues.	18	Yes - The agency plans to replace the system in 2018.
Department of Veterans Affairs	Personnel and Accounting Integrated Data	This system automates time and attendance for employees, timekeepers, payroll, and supervisors. This system is written in COBOL—a programming language developed in the 1950s and 1960s—and runs on IBM mainframes.	53	Yes - The agency plans to replace most of the system's functionality in 2017.

Source: GAO analysis of agency documentation and interviews. | GAO-16-696T

Note: Systems and investments may have components newer than the reported age.

We have previously provided guidance that organizations should periodically identify, evaluate, and prioritize their investments, including those that are in O&M; at, near, or exceeding their planned life cycles; and/or are based on technology that is now obsolete, to determine whether the investment should be kept as-is, modernized, replaced, or retired.[23] This critical process allows the agency to identify and address high-cost or low-value investments in need of update, replacement, or retirement.

Agencies are, in part, maintaining obsolete investments because they are not required to identify, evaluate, and prioritize their O&M investments to determine whether they should be kept as-is, modernized, replaced, or

[23] GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, Version 1.1, GAO-04-394G (Washington, D.C.: March 2004).

retired. According to OMB staff from the Office of E-Government and Information Technology, OMB has created draft guidance that will require agencies to identify and prioritize legacy information systems that are in need of replacement or modernization. Specifically, the guidance is intended to develop criteria through which agencies can identify the highest priority legacy systems, evaluate and prioritize their portfolio of existing IT systems, and develop modernization plans that will guide agencies' efforts to streamline and improve their IT systems. The draft guidance includes time frames for the efforts regarding developing criteria, identifying and prioritizing systems, and planning for modernization. However, OMB did not commit to a firm time frame for when the policy would be issued. Until this policy is finalized and carried out, the federal government runs the risk of continuing to maintain investments that have outlived their effectiveness and are consuming resources that outweigh their benefits.

Regarding upgrading obsolete investments, in April 2016, the IT Modernization Act[24] was introduced into the U.S. House of Representatives. If enacted, it would establish a revolving fund of $3 billion that could be used to retire, replace, or upgrade legacy IT systems to transition to new, more secure, efficient, modern IT systems. It also would establish processes to evaluate proposals for modernization submitted by agencies and monitor progress and performance in executing approved projects.

Implementation of Our Recommendations Should Allow Federal Agencies to Better Manage Legacy Systems and Investments

Our report that is being released today contains 2 recommendations to OMB and 14 to selected federal agencies. Among other things, we recommend that the Director of OMB commit to a firm date by which its draft guidance on legacy systems will be issued, and subsequently direct agencies to identify legacy systems and/or investments needing to be modernized or replaced and that the selected agency heads direct their respective agency CIOs to identify and plan to modernize or replace legacy systems as needed and consistent with OMB's draft guidance. If agencies implement our recommendations, they will be positioned to better manage legacy systems and investments.

[24] *Information Technology Modernization Act*, H.R. 4897, 114th Cong. (2016).

In commenting on a draft of the report, eight agencies (USDA, Commerce, HHS, DHS, State, Transportation, VA, and SSA) and OMB agreed with our recommendations. Defense and Energy partially agreed with our recommendation. Defense stated that it planned to continue to identify, prioritize, and manage legacy systems, based on existing department policies and processes, and consistent to the extent practicable with OMB's draft guidance. Energy stated that while the department continues to take steps to modernize its legacy investments and systems, it could not agree fully with our recommendation because OMB's guidance is in draft and the department has not had an opportunity to review it. Defense and Energy's comments are consistent with the intent of our recommendation. Upon finalization of OMB's guidance, we encourage both agencies to implement OMB's guidance. In addition, Justice and the Treasury stated that they had no comment on their recommendations.

In summary, O&M spending has steadily increased over the past 7 years and as a result, key agencies are devoting a smaller amount of IT spending to DME activities. Further, legacy federal IT investments are becoming obsolete and several aging investments are using unsupported components, many of which did not have specific plans for modernization or replacement. This O&M spending has steadily increased and as a result, key agencies are devoting a smaller amount of IT spending to DME activities. To its credit, OMB has developed a draft initiative that calls for agencies to analyze and review O&M investments. However, it has not finalized its policy. Until it does so, the federal government runs the risk of continuing to maintain investments that have outlived their effectiveness and are consuming resources that outweigh their benefits.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

GAO Contact and Staff Acknowledgments

If you have any questions on matters discussed in this testimony, please contact David A. Powner at (202) 512-9286 or at pownerd@gao.gov. Other key contributors include Gary Mountjoy (assistant director), Kevin Walsh (assistant director), Scott Borre, Rebecca Eyler, Tina Torabi, and Jessica Waselkow.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates.
Listen to our Podcasts and read The Watchblog.
Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper.

Chairman CHAFFETZ. Thank you. I appreciate it.

Mr. Milholland, you are now recognized for 5 minutes.

STATEMENT OF TERRY MILHOLLAND

Mr. MILHOLLAND. Chairman Chaffetz, Ranking Member Cummings, and members of the committee, thank you for the opportunity to testify here today.

The IRS recognizes the need to continue work to modernize our information technology. We make every effort to stay current and efficient in our data centers and our processing platforms while remaining vigilant about the security of our systems and the taxpayer data entrusted to us.

We operate a number of legacy systems vital to our tax administration mission. Our goal is to retire all of these legacy systems as quickly as possible. We consider them to be legacy because their programming languages and data structures were generally designed and built decades ago when computer infrastructure was extremely expensive and technology capabilities were limited.

Over time, the underlying hardware and operating infrastructures of the legacy systems have been modernized. Together with the movement to electronic filing technology, and despite the restrictions of the programming language and data structures, this modernization has made it possible for the IRS to deliver smooth filing seasons year after year.

To give the committee an idea of what our submission systems can handle, over this last filing season, we received 4.4 million tax returns on our peak day. At that peak, our systems accepted more than 800,000 filings in a single hour, which equates to more than 225 filings per second.

But the main challenge posed by our legacy systems is that their data structures stored on computer tapes make it very difficult to use that data in our downstream service and compliance systems to better serve taxpayers.

So we have been working for many years within the constraints of our budget to transition our legacy systems' programming languages and data structures so that we can make that data more available for more modern, Web-based applications and data analytics that we use in other key mission functions, like enforcement and compliance.

Our most visible effort in this regard has been the development of a centralized relational database for all individual taxpayer accounts called the Customer Account Data Engine, CADE2. When fully implemented, it will replace the legacy Individual Master File, or IMF, which historically has been the primary data source for individual taxpayer accounts.

We think that will happen in three major steps, or what we call transition states. The first step of this transition state in implementing CADE2 was the launch in January 2002 of that relational database. Up to this point, we had been performing core account processing on a weekly basis. Launching this phase of CADE2 meant that the IRS can now process updates to accounts on a daily basis. This has fundamentally changed the way the IRS provides information and services to taxpayers, and has delivered significant and lasting benefits to our tax system.

For example, taxpayers can now receive their refunds faster, and IRS customer service representatives have much more up-to-date customer account information.

This, however, is a complex, multistep process, not a single switch to be thrown. It is not an easily accomplished action because connections for these legacy systems are intertwined throughout the IRS for both system and data repositories.

There is a lot more work to be done on CADE2, but the steps we have taken so far have improved our ability to interact with taxpayers efficiently and effectively.

I also want to mention that GAO has acknowledged the importance of the IRS work in this area. In 2013, GAO removed our business system modernization program from its high-risk list, singling out delivery of the initial phase of CADE2 as the main reason for determining that business system modernization was no longer high risk.

I also should point out that all new development work over the past 7 years has been using state-of-the-art programming languages and database technologies so that the problems of older legacy systems will not be repeated.

In working to transition our legacy systems to more modern ones, we have a number of challenges. None is more critical than the budget situation. IRS funding was cut each year for 5 years from 2011 to 2015, and our budget is currently about $900 million below what it was in 2010. Making progress at a faster pace on transitioning our legacy systems will require significant, sustained, additional resources in the IT area.

Another way Congress can help is by reauthorizing streamlined critical pay authority. The loss of this authority has made it very difficult and time-consuming to recruit and retain employees with expertise in highly technical areas in IT, such as legacy system modernization, cybersecurity, architecture, engineering, and operations.

Chairman Chaffetz, Ranking Member Cummings, and members of the committee, this concludes my statement, and I am happy to take your questions.

[Prepared statement of Mr. Milholland follows:]

WRITTEN TESTIMONY OF
TERENCE MILHOLLAND
CHIEF TECHNOLOGY OFFICER
INTERNAL REVENUE SERVICE
BEFORE THE
HOUSE OVERSIGHT AND GOVERNMENT REFORM COMMITTEE
ON IRS LEGACY INFORMATION TECHNOLOGY SYSTEMS
MAY 25, 2016

INTRODUCTION

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, thank you for the opportunity to appear before you today to discuss the IRS's ongoing efforts to modernize our information technology (IT) systems.

Information technology continues to transform the landscape of how the IRS interacts with its constituencies. The current pace of technological change exceeds the ability of a large, well-established organization such as the IRS to embrace all of these transformative technologies. The IRS, however, has found that effective enterprise IT management consists of thoughtful planning engineering and delivery, coupled with active and adaptive IT investment management. We continue to work to stay current and efficient in our data centers and core processing platforms, while remaining vigilant about the security of our systems.

Against that backdrop, the IRS continues to operate a number of legacy IT systems, although it is not our preference to do so, and our ultimate goal is to retire all of them as quickly as possible. We consider them to be "legacy" because their programming language and data structures generally were built decades ago when computer infrastructure, such as computer memory and storage media, was tape-based, and computational machinery was extremely expensive. These factors limited system capabilities. Thus, system designers had to be very creative in how they built and sustained IRS applications to operate in the early days of computers. At the time these systems were originally developed, they were constructed around a system that was dependent on the filing of paper returns. In effect, we automated the processing of paper returns. This makes it much more difficult than it should be in today's environment to efficiently access the information in the return.

Since our systems were initially developed over 50 years ago, we have upgraded the underlying hardware and operating systems of these legacy systems, while the application programming language and data structures have essentially remained static, although they are well-written and robust. This allows the IRS to handle annual legislative mandates and run the filing season each year. The situation is analogous to operating a 1960's automobile with the original chassis, suspension and drive train, but with a more modern engine, satellite radio and a GPS navigation system. It runs better than the original model but not nearly as efficiently as a system bought today.

Our ability to effectively manage enterprise IT despite our legacy systems, and within our limited resources, is evidenced by the fact that the IRS continues to deliver smooth filing seasons, amid steady growth both in the number of returns filed and the percentage of electronically filed returns over the past decade. Return processing goes smoothly even in years where passage of tax legislation late in a given year requires the IRS to move quickly to update our systems to accommodate tax changes enacted by Congress. To give the Committee an idea of what our systems are capable of handling, in the filing season that just concluded, our systems received 4.4 million tax returns on one of our busiest days. At the peak, our systems accepted more than 800,000 filings in a single hour, which equates to more than 225 filings each second.

TRANSITIONING THE IMF TO CADE2

The main challenge posed by our legacy systems is that their data structures do not allow us to easily use the data in our downstream service and compliance systems to best serve taxpayers. For that reason, we have been working diligently for many years, within the constraints of our budget, to make this data more available, so that we can update and modernize numerous key functions.

In addition to the challenge with data structures, another challenge we face involves the need to change the core programming language of our processing systems from a decades-old Assembly language code (ALC) used in the 1950s and 1960s to a more modernized programming language, such as JAVA. The IRS faces a significant shortage of programmers who understand very old programming languages and can maintain mission-critical applications required to deliver each filing season. Therefore, we are working to ensure that we are no longer dependent on these old languages to maintain legacy systems and can use the flexibilities provided by more modern languages. In fact, our IT engineering function has recently developed an in-house code translation methodology using automated tools to translate the programming language used in our legacy tax processing applications into the JAVA language. This is a technological breakthrough for which the IRS is applying for a U.S. patent.

Our most critical effort with regard to legacy systems to date has been the development of a centralized relational database for all individual taxpayer accounts, called the Customer Account Data Engine, or CADE2. When fully implemented, CADE2 will replace the legacy Individual Master File (IMF), which historically has been the primary data source for individual taxpayer accounts. In fact, IMF has the distinction of being the oldest system highlighted in the Government Accountability Office's (GAO) report on legacy IT systems The IRS envisions that CADE2 will replace the IMF in three major steps, or transition states.

The IRS took the first step in implementing CADE2 with the launch of Transition State 1 in January 2012. Up to this point, the IRS had been performing core account processing on a weekly basis. The launch of CADE2 meant the IRS successfully migrated to daily processing and posting of individual taxpayer accounts. This has fundamentally changed the way the IRS provides information and services to taxpayers, and has delivered significant and lasting benefits to our tax system. With Transition State 1, CADE2 allowed taxpayers to receive faster refunds and gave IRS assistors quicker updates to account information. Today, when a taxpayer calls us, the account information available to the customer service representative is no more than 24 hours old.

Implementation of Transition State 2 of CADE2 will result in a major reengineering of the IMF. This step will: apply modern programing languages; establish CADE2 as the authoritative data source for legal and financial purposes; and implement functionality to address the IRS's Financial Material Weakness over unpaid tax assessments for individual taxpayer accounts. The IRS plans to implement Transition State 2 over the next several years, with the final release planned for deployment in the 2020 filing season. Upon completion of Transition State 2, the IRS will begin the third and final step toward replacing the IMF, which will complete the reengineering of the IMF architecture.

It is important to note that the modernization effort I have just described is a complex, multistep process – not a single, easily accomplished action. The steps we have undertaken thus far have already provided important improvements to our ability to interact with taxpayers efficiently and effectively.

Another important component of effective IT includes building key management capabilities. The IRS IT organization has implemented world-class IT processes for applications development and operations. These processes, known as CMMI and ITIL, are recognized throughout the IT industry for their efficiency and effectiveness. The IRS is the only government agency to be at maturity Level 3 for CMMI and ITIL across the entire IT organization. This is a significant accomplishment and means that IRS IT is recognized as maintaining a high level of competency in managing IT development and operations.

In regard to the transition of the IMF to CADE2, I would also note that the GAO has acknowledged the importance of the IRS's accomplishments in this area. In 2013, the GAO removed the agency's Business Systems Modernization program (BSM) from its high-risk list. The BSM program had been on the list since 1995. In its 2013 report, the GAO mentioned the advances made by the IRS over many years in addressing weaknesses in IT and financial management capabilities, and it singled out the successful delivery of the initial phase of CADE2 as the main reason for its determination that the BSM program was no longer high risk.

That same year, the Excellence.gov Awards Program sponsored by the American Council for Technology and the Industry Advisory Council recognized CADE2 for Excellence in Enterprise Efficiencies. This awards program honors government programs and projects that use information technology in innovative ways to enhance government operations, provide a more open and transparent government, and deliver important citizen resources.

LOOKING TO THE FUTURE

CADE2 is one component within our broader efforts to upgrade our legacy systems. Going forward, the IRS is prioritizing the transition of mission-critical legacy systems to more modern technology in accordance with our Future State and the IRS Technology Roadmap efforts. Both are the result of an enterprise-wide effort to determine how the IRS can best use the latest technology to improve taxpayer service and enforcement efforts.

Our Future State encompasses programs across the IRS and will transform the IRS to create efficiencies in IRS service efforts and internal operations and to improve the taxpayer experience. In developing this strategy, the IRS is considering evolving taxpayer expectations, the increasing risk and complexity of current processes and supporting technology, available funding, and increased occurrences of identity theft and fraud.

An important example of this effort in the compliance area has been the development and phase-in of the Return Review Program (RRP). The RRP is an integrated and unified system that enhances IRS capabilities to detect and potentially prevent criminal and civil tax non-compliance. During the 2016 filing season, RRP overtook the legacy Electronic Fraud Detection System (EFDS) as the primary system for detecting anomalies in tax returns. RRP selected more than 600,000 potentially fraudulent returns for which refunds were claimed totaling more than $4 billion. Continued investment in RRP will allow the IRS to retire EFDS and address more sophisticated instances of identity theft more quickly.

The IRS intends to further improve compliance programs through investment in an Enterprise Case Management (ECM) system, which is intended to modernize, upgrade, and consolidate more than 60 aging IRS case management systems. This common case management environment will yield efficiencies by implementing standard case management functions, providing the ability to transfer cases between IRS organizations and creating centralized case data accessibility and usability.

Another initiative that will help the IRS move toward the Future State is the Event Driven Architecture (EDA) framework, which will process returns in near-real time. This will also enable robust online self-service tools, including immediately notifying taxpayers of errors on a return as soon as it is filed, and allowing taxpayers to self-correct return errors by logging into an online account.

NEED FOR ADEQUATE RESOURCES AND IT EXPERTISE

The IRS budget situation is the most critical challenge facing IT modernization. IRS funding was cut each year from 2010 to 2015. These cuts have taken a toll on taxpayer service, enforcement programs, and IT projects. Although Congress provided $290 million in additional funding for the agency for Fiscal Year (FY) 2016, which we appreciate, the IRS budget remains about $900 million below what it was in 2010, not accounting for inflation. We therefore remain under severe financial constraints. To illustrate the problem in the IT area, in FY 2015 alone, we were forced to delay critical IT investments of more than $200 million, including investments needed to continue replacing legacy systems.

A related challenge involves the fact that the IRS, during this same period, has begun to implement a number of significant legislative requirements, nearly all of which came with no additional funding. Satisfying these requirements has involved significant IT investments, requiring resources that would otherwise have gone to IT projects such as our legacy systems transition work.

These requirements include those stemming from: the Affordable Care Act (ACA); the Foreign Account Tax Compliance Act (FATCA); the Achieving a Better Life Experience (ABLE) Act, which includes a new certification requirement for professional employer organizations; and reauthorization of the Health Coverage Tax Credit (HCTC), among others. Two other legislative mandates that require additional resources were approved by Congress in December: a private debt-collection program and a registration requirement for newly created 501(c)(4) organizations.

While we have made and will continue to make progress in modernizing our IT systems within the constraints of our budget, making progress at a faster pace will require providing the IRS with significant additional resources. For example, the President's FY 2017 Budget proposes $53.5 million to leverage new technologies to advance the IRS mission for projects such as CADE2 and Modernized e-File; $48.5 million to improve taxpayer service, including the online taxpayer experience; and $90 million to help advance our efforts against identity theft and reduce improper payments. All of these initiatives include the resources for the technology improvements needed in these areas.

In addition to adequate funding, the IRS also needs to be able to attract individuals from the private sector with highly specialized IT skills and expertise, particularly for our leadership positions in IT. In the past, the IRS has successfully recruited such individuals using streamlined critical pay authority that was enacted in 1998. In fact, the Treasury Inspector General for Tax Administration (TIGTA) in a 2014 report found that the IRS had appropriately used this authority, by adequately justifying the positions, demonstrating the need to recruit or retain exceptionally well-qualified individuals, and adhering to pay limitations. This authority expired at the end of FY 2013 and has not yet been renewed.

The loss of streamlined critical pay authority has created major challenges to our ability to retain employees with the necessary high-caliber expertise in IT and other specialized areas. In fact, out of the many expert leaders and IT executives hired under streamlined critical pay authority, there are only nine IT experts remaining at the IRS, and we anticipate there will be no staff left under this authority by this time next year. The President's FY 2017 Budget proposes reinstating this authority, and I urge the Congress to approve this proposal.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, this concludes my statement, and I would be happy to take your questions.

Chairman CHAFFETZ. Thank you.

Mr. Halvorsen, you are now recognized for 5 minutes.

STATEMENT OF TERRY HALVORSEN

Mr. HALVORSEN. Good morning, Mr. Chairman, Ranking Member, and distinguished members of the committee. Thank you for this opportunity to testify before you on the Department of Defense legacy information technology spending plans for modernization and the implications of IT acquisition reform and security.

As the department CIO, I am the principal adviser to the Secretary of Defense for information management, IT, cybersecurity, communications, positioning, navigation and timing, spectrum management, and senior leadership and Nuclear Command and Control and Communications matters. My written testimony provides more detailed information on these matters, but I want to highlight some of the department's activities in this area.

All of the services have modernization plans that align with DOD and service priorities. The DOD and the services have recognized some critical areas to which funds have been added for modernization. NC3, PNT, the Joint Regional Security Stacks are some examples. All of the services are committed to moving to Windows 10, and we are working on moving toward a common private cloud supported by various hybrid and public clouds.

The department and services are committed to modernization as it relates to improved cybersecurity. For example, within the services, the Army is moving forward with upgrading its camp, post, station, and base communications IT infrastructure. The Air Force is implementing Communications Squadron Next. The Navy is moving forward with shipboard modernization with programs such as CANES. And the USMC has focused its efforts to modernize IT at the edge by creating a seamless Marine Corps enterprise network.

I believe we are correctly balancing between mission priorities, legacy systems, and modernization within current budget constraints. Today, about 25 percent of our budget goes to modernization. That doesn't mean that we don't have challenges or that there are enough resources.

OPTEMPO also has a major impact on IT equipment and modernization. DOD has been busy, and we continue to have high demand for our services.

Our priority for investments are C2 systems and direct combat support systems. We aren't modernizing business systems as fast as we would like, but we have prioritized DOD resources to ensure overall mission success.

The DOD is "Fortune Zero." It is the largest IT operation in the world.

I think it is important to note that DOD is not out of balance with large enterprise IT in the private sector. We are not out of balance in investment, use of cloud, percentage using older languages. I think we should note that COBOL runs 70 percent to 80 percent of all business transactions in the world.

IT modernization competes for dollars with other DOD modernization efforts, like aviation platforms, ship weapons, combat vehicles, et cetera. Again, I think we've got the priorities right, given the budget constraints. The budget, however, is constrained, and that affects all modernization efforts, to include IT.

While I am the CIO, DOD must look at the entirety of the department's modernization efforts, not just IT, and prioritize accordingly.

Thank you for the time. I look forward to your questions today.

[Prepared statement of Mr. Halvorsen follows:]

STATEMENT BY

TERRY HALVORSEN
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE OVERSIGHT AND GOVERNMENT REFORM COMMITTEE

ON

FEDERAL AGENCIES' RELIANCE ON OUTDATED AND UNSUPPORTED INFORMATION TECHNOLOGY: A TICKING TIME BOMB

May 25, 2016

**NOT FOR PUBLICATION UNTIL
RELEASED BY THE HOUSE
OVERSIGHT AND GOVERNMENT
REFORM COMMITTEE**

Introduction
Good morning Mr. Chairman, Ranking Member, and distinguished Members of the Committee. Thank you for this opportunity to testify before the Committee today on the Department's legacy information technology (IT) spending, plans for modernization, and implications for IT acquisition reform and security. I am Terry Halvorsen, the Department of Defense (DoD) Chief Information Officer (CIO). As the senior civilian advisor to the Secretary of Defense for IT, I am responsible for all matters relating to the DoD information enterprise, including cybersecurity and IT modernization for the Department.

DoD has a long history of leaning forward on using and in some cases developing emerging and new technologies. We are one of the largest procurers of technology in the world. Our IT portfolio today has a mixture of inhouse-development, recently deployed, and older systems, and systems that are a mixture of all three.

GAO's report places great emphasis on Development, Modernization, and Enhancement, or DME, a construct used in budgetary and management reporting to categorize IT resources according to the life-cycle activities taking place in an IT investment. It is a longstanding and useful categorization, similar to how funds are categorized in the DoD budget. DME is one indicator of how well the Department is injecting new technology and systems into its inventory. DME is an indicator, not a goal. There are limitations to how well this and other budgetary constructs can be used to assess the technological currency of systems and portfolios.

Aging systems have risk. So does DME. The Department's approach is to balance our capacity to plan, architect, manage, coordinate, contract, build, document, test, train, and transition new systems into the portfolio with the need to manage, operate, and protect our installed base. In the last several years, DoD has modernized, replaced, updated, upgraded, enhanced, technologically "refreshed," consolidated, and retired hundreds of systems, whether coded as DME or as more routine technology replacements under "Operations and Maintenance."

In the past few years, DoD's focus has been on foundational changes that position the Department to move forward in a more enterprise, coordinated, secure and cost effective environment. These changes include consolidating data centers; making platform, backbone, and communications improvements; implementing common security constructs under the Joint Regional Security Stacks; moving to a standard operating systems and a common platform; rationalizing applications; and continuing the move to cloud environments.

This will improve the Department's IT infrastructure and processes for broad impact, and position even more systems to come into an enterprise or shared environment, in a more secure, mission effective and cost efficient way. Optimizing the DoD IT infrastructure in this way will help us meet the diverse missions of today, and support the strategic requirements of tomorrow. Supported by JRSS and leveraging the flexibility and interoperability of cloud computing, the future DoD IT environment will empower the Department to operate in a modern security environment that is highly connected and driven by data. We are working closely with our mission partners to make smart choices in how IT enables execution of the mission in the face of a persistent cyber threat.

DoD is striving to facilitate system improvements while lowering operating risks by increasing use of enterprise solutions, transforming the DoD IT to a more agile, innovative, and mobile thin client, cloud-based environment at less cost to the taxpayers. DoD's move to the enterprise and shared services model will reduce duplication, close performance gaps, and promote better security among government, industry, and mission partners. Enterprise solutions also provide current technologies to implement standardization, common design principles, responsive scalability, and repeatable architectures to foster more agile and useful planning, decision-making, and IT management.

The Department has some old systems and some cases of obsolete technology. We are making progress reducing obsolescence. Highlighting the oldest systems in our inventory does not represent the DoD technology portfolio as a whole. Some systems with older languages and older technologies exist like those that still use COBOL – the programming language DoD helped pioneer decades ago. Where it makes sense to re-code or upgrade those systems, we need to do that — with a priority on those systems with the greatest potential for cybersecurity vulnerabilities. It is critical that we focus on investing in system replacements, modernization, or upgrades when there is a clear and compelling operational need or business case to do so. Not everything old needs to be replaced.

Moving forward, the Department's IT strategies and policies will continue to evolve, including those related to the quality and quantity of evaluations to measure the ongoing effectiveness and technological profiles of the installed baseline of IT systems. As the DoD CIO, my goal is to ensure these strategies and policies are implemented by the DoD Components, who are ultimately responsible for funding, implementing, operating and modernizing the Department's IT systems, and to ensure that DoD IT investments continue to support mission critical and mission support operations of the Department.

To address obsolete IT investments in need of modernization or replacement, the GAO recommends that the Department identify and plan to modernize or replace legacy systems as needed and consistent with OMB's draft guidance, including timeframes, activities to be performed, and functions to be replaced or enhanced. The Department is already doing this using the principles described above, which leverage existing DoD policies and processes,

Conclusion

DoD recognizes the importance of modernization and the security implications that come with operating legacy systems. We have more work to do and are not where we want to be today. We are, however, making the right investments in our legacy systems and balancing modernization against the sustainment and improvement of systems that are critical to warfare mission and business mission success. The Department is actively pursuing modernization while operating within the confines of a constrained budget environment. We look forward to receiving final guidance from the Office of Management and Budget, as well as working with Congress on these matters. Thank you for the opportunity to testify today and I look forward to your questions.

Chairman CHAFFETZ. Thank you.

Ms. Killoran? Did I get it better that time?

Ms. KILLORAN. Yes, thank you. Good morning.

Chairman CHAFFETZ. You are now recognized for 5 minutes. Thank you.

STATEMENT OF BETH KILLORAN

Ms. KILLORAN. Good morning, Chairman Chaffetz, and Ranking Member Cummings, and members of the committee. Thank you for giving me the opportunity to discuss our legacy Federal IT technology at HHS.

As the chief information officer acting for the Department of Health and Human Services, my testimony today will describe how we have been able to decrease some of our end-of-life systems through both a risk mitigation approach as well as our plans moving forward.

HHS is the U.S. Government's principal agency for protecting the health of all Americans and providing essential human services, especially for those who are least able to help themselves. Information technology is critical to enabling HHS to achieve its mission by fostering advances in medicine, public health, and social services. HHS currently spends approximately $5 billion annually on our internal IT and over $7 billion in IT grants that are primarily given to States and local agencies to facilitate our programs.

In managing our IT programs, one of the key risks associated with operational systems is our ability to secure them. Last year, HHS did make measurable progress in our increase of Federal Information Security Modernization Act score, or FISMA. But our work there isn't done.

HHS is currently working to implement the next phase of Einstein, and we are working to improve our trusted Internet connection and deploy different tools under DHS's continuous diagnostics and mitigation program.

All of this work will not only strengthen our systems, but will build on HHS Cyber Sprint success that we had and strengthen our overall cyber infrastructure resiliency.

When our agency decides to replace a legacy system, cloud offerings can help our agency reduce time to develop those products and services. Cloud solutions have helped already HHS reduce program risk and development time.

Our most successful cloud implementation to date is our HHS financial systems upgrade of our core backbone, which occurred last year. This ambitious program modernized our IT infrastructure by using cloud capabilities to improve our systems over all. and through a shared technology, we were able to add cutting-edge technology in a shorter period of time.

Given the importance of our IT mission, I worked diligently over the last year to also improve our IT portfolio review process. Through this, I have launched a number of initiatives in collaboration with our operating divisions to address the most common systematic issues, improve transparency, and enhance governance. Our HHS Federal information technology reform act implementation plan helps support that path moving forward.

One initiative that I have done is to enhance our program evaluation model to make sure that we are looking at enterprise risk overall, and implemented changes to how we look at and score our programs for the IT Federal dashboard last October. This new model incorporates new risks, operational performance objectives, and factors both from scoring and risk factors that OMB has established in GAO.

This data is used to closely monitor our IT programs and risks, and identify those that are at risk. And if something is at high risk for a certain period of time, we do conduct TechStats, of which we actually conducted 10 within the last year, including both the programs cited in the recent GAO report.

We will continue to work on mitigating risks as we look at our legacy systems and work to improve.

By working one-on-one with our program managers, we can increase the probability of success. We have found that investing in those individuals is critical to our success. We have trained 300 people over the last year, and we have an HHS human capital pilot to increase our cybersecurity work force and competencies over the next year.

HHS does spend significantly more on operations, 71 percent, than on our development at 29 percent. HHS recognizes the need for greater development spending, but challenges exist.

Some of our challenges include lack of authority, uncertain grantee systems, the ability to make sure that we are accomplishing Federal mandates, the interdependencies of our systems, and funding by smaller organizations.

As we move forward with some of these capabilities, we will make sure that we look at our inventory and make sure that our FITARA plan establishes how we will evaluate those and look at our modernization moving forward.

One way that we know that we can address a funding challenge is by Congress passing the IT modernization fund. This model can help agencies with upgrading their systems, and the business case we have is our nonrecurring expense fund. This is provided to use unobligated balances to allow us to make changes to our critical systems, and we have succeeded in enhancing our DME significantly from 2012 and 2013 to current standards.

Simply put, doing nothing is not doing nothing. As systems age, the risk to security, reliability, and availability have to be addressed. To reduce exploitation and system vulnerabilities' associated risk, we need to look at those systems and make sure that we are looking at business and security risks to make our priorities.

Thank you for your time, and I will yield to any questions you might have.

[Prepared statement of Ms. Killoran follows:]

TESTIMONY OF
Beth Anne B. Killoran
Acting Chief Information Officer
U.S. Department of Health and Human Services
Before the
House Committee on Oversight and Government Reform
May 25, 2016

Good morning Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, thank you for giving me the opportunity to discuss federal information technology (IT). As the Acting Chief Information Officer (CIO) at the Department of Health and Human Services (HHS), my testimony will describe how HHS has been able to decrease the use of our end-of-life systems through a risk mitigation approach as well as discuss plans we have for remaining systems.

Leveraging IT to Support Mission Outcomes

HHS is the U.S. government's principal agency for protecting the health and well-being of all Americans and providing essential human services, especially for those who are least able to help themselves. IT is critical to enabling HHS to achieve its mission by fostering advances in medicine, public health, and social services. HHS spends approximately $5 billion annually to develop and maintain our IT. HHS has an annual operating budget of over $1 trillion, is responsible for almost a quarter of all federal outlays, and administers more grant dollars than all other federal agencies combined, including $7.3 billion in IT grants to state and local agencies for the procurement of IT to facilitate HHS programs.

In managing our IT programs, one of the key risks associated with operational systems is the ability to secure them. On this front, HHS has made measurable progress in improving cybersecurity. We are constantly making improvements resulting in our Federal Information Security Modernization Act (FISMA) score being the highest it has been in four years. Last year, our score improved by 23 percentage points from 35 percent in fiscal year (FY) 2014 to 58 percent in FY 2015.

Our work isn't done. HHS is continuing to strengthen our cybersecurity efforts. We are currently deploying the next phase of Einstein tools, defining the next generation of the Trusted Internet Connection, and deploying security monitoring tools consistent with the Department of Homeland Security's Continuous Diagnostics and Mitigation program. All of this work will not only strengthen our posture, but will build on HHS's Cyber Sprint by strengthening HHS's cyber infrastructure resiliency.

Finally, HHS has established the CyberCARE campaign to ensure HHS users are educated regarding cyber threats. The program won an annual award from the Federal Information Security System Educator's Association (FISSEA) and has been selected as a finalist in the Community Awareness category by U.S. Government Information Security Leadership Awards (GISLA). Each of these efforts illustrate that operational systems can provide continued mission support and functionality, if we continue to ensure they are secure and provide mission value.

Strategies and Capabilities to Modernize

When it is time to replace a legacy system, cloud capabilities reduce time necessary for modernizing or enhancing IT systems. By sponsoring cloud technologies through the federal standardized cloud products security assessment, authorization, and continuous monitoring process (FedRAMP), HHS works to offer and leverage cloud solutions. Cloud solutions have helped HHS reduce IT capital expenditures, reduce program risk, and reduce implementation time. Our most successful cloud implementation to date is development and modernization of the Department's financial systems. This ambitious program serves as a model on how to modernize IT infrastructure. As one of the largest federal financial systems upgrade to date, this program provides new capabilities across HHS through a shared delivery model utilizing a cutting-edge technology. In addition, HHS has successfully utilized cloud solutions to establish a new E-mail-as-a-Service (EaaS) platform, provide solutions to assist HHS in addressing urgent initiatives such as the Ebola response, and enhance communications through cloud technologies and business analytics. In each of these examples, cloud computing offerings have enabled HHS to reduce time to develop new products and services and increase collaborative capabilities.

Improving Our Program Management

Given the importance of IT, I have worked over the last year in my roles within the HHS CIO organization to improve our review process of our IT portfolios by conducting in-depth reviews of our own large IT programs. In collaboration with Operating Divisions to develop and implement a number of initiatives to address the most common systemic issues, we have improved transparency and enhanced governance.

Part of our FITARA change impacts how the HHS Office of the Chief Information Officer has evaluated the Department's major IT investments. Early CIO evaluations examined project management practices and operational performance placing an emphasis on timely reporting. I determined that we needed to enhance our evaluation model to adequately assess potential risks and dependencies. Implemented in October 2015, the revised risk model incorporates new risk factors, operational performance metrics, and is scored based on OMB's 5-point risk scale.

In addition, HHS closely monitors IT investment risks and quickly identifies mitigation strategies for reducing risk. If a major system is identified as "High Risk" for three consecutive months, then either the HHS or Operating Division Chief Information Officer requires that a TechStat is conducted. A TechStat is a face-to-face, evidence-based review of an IT program, undertaken with agency leadership, powered by the IT Dashboard. HHS has a robust TechStat program that is valuable for both developmental and operational programs. In FY 2015, HHS performed eight TechStat reviews of IT investments in the HHS IT Portfolio to reduce the risk associated with these investments.

TechStats have been performed on both of the programs cited in the GAO legacy systems. In June 2013, a TechStat was conducted on the first program identified by GAO, the Medicare Appeals System (MAS). The MAS supports a tracking system for Medicare appeals across all Medicare programs (fee-for-service, Medicare Advantage, and Part D). The TechStat review identified additional project management best practices that should be implemented to track schedule and cost changes. Based on the review, the Centers for Medicare & Medicaid Services implemented those recommendations resulting in the program now consistently receiving the lowest risk rating.

The Trusted Internet Connection (TIC) went into operations and maintenance in 2015 after we completed installation on our final three locations. The final phase ensures that all HHS traffic is routed through centralized access points, increasing visibility of network traffic and reducing vectors for compromise and attack. To strengthen the program as it continues to make changes, a TechStat was performed for the Trusted Internet Connection (TIC) in February 2016. That TechStat identified program practices regarding performance metrics and reporting that needed to be added to monitor progress. Since the TechStat review, my team has implemented several initiatives to collect, analyze, and report performance metrics, resulting in reducing the program risk level. In addition, the TIC has performed a number of modernization activities this year and more will continue over the next 12-18 months.

Developing Our Staff

As we continue to enhance our risk management practices this year, we will continue to focus on preventing investments from trending as high-risk by working with project managers to solve potential problems before they become issues. We work on a one-on-one basis with project managers in order to ensure that program health is optimized and appropriately represented. Through our outreach efforts, we have found that investing in our most important resource, our people, is critical to ensuring the health of our IT portfolio.

We are committed to providing training for our IT program and project managers. To improve the probability of program success, our training program aligns with the Office of Federal Procurement Policy's October 2009 guidelines and standards. HHS provides three levels of training (entry, mid, and senior level) for IT program and project managers to receive certification as a Federal Acquisition Certification program professional. HHS has trained close to 300 IT program and project managers since November 2015. This was accomplished through a combination of classroom and virtual project managers collaboration network where practicing can collaborate, discuss best practices, share innovative ideas and learn from each other. In addition, HHS has sponsored an agency Annual IT Project Manager Summit for the last three years where the entire HHS IT community comes together to strategize, share insights on improvement strategies that are working well, not only at HHS but the federal government, and to participate in training.

Beyond development, HHS is working to attract new IT staff to critically important positions for our long-term success. Over the past two years, we developed the HHS IT Human Capital Strategy pilot for Cybersecurity, an approach that outlines IT career paths and enables us to establish a professional continuum that defines competencies employees need to advance their career. We are currently working to expand this program to other IT professions. Partnering with the Office of the Chief Human Capital Office, we are working to identify new methods for recruiting critical IT positions through direct hire, internships, Schedule A, and targeted recruiting through universities and professional organizations by marketing our Department's mission to draw professionals to a career at HHS.

Making the Case for Change

Like other federal agencies, HHS spends significantly more on operations and maintenance than on DME. HHS recognizes the need for greater development spending, and modernizing or replacing unsupported technology, but challenges to this practice exist. Some of our specific challenges include lack of clear authority to require grantees to replace or modernize their systems, DME funding used for new mandates, and interdependencies of systems or software that prohibits changes. To make the case for funding, agencies must first identify which IT investments qualify as legacy, and then prioritize programs. For example, HHS would not consider an IT system that entered operations and maintenance last year, such as the TIC nor would a decade old system with underlying technology still supported by the manufacturer (MAS) be considered legacy. Once a program has been identified as needing replacement, agencies will need adequate funding to make legacy system changes.

One way to address the Government funding challenge is by Congress passing the Administration's proposed $3.1 billion IT Modernization Fund (H.R. 4897). The IT Modernization Fund would serve as a mechanism for agencies to upgrade legacy IT to more modern, cloud-based systems. To ensure agencies are modernizing the most critical systems, the legislation would establish a board of experts to help prioritize high-risk federal systems for replacement. The board would also look for multiple legacy systems that could be replaced with a few common platforms.

Congress established the Nonrecurring Expense Fund (NEF) at HHS, which permits HHS to procure capital acquisitions including IT and facilities infrastructure necessary for operation of the Department. These funds provide vital support to HHS. This funding has supported a number of critical IT system modernizations. For example, in FY 2014, HHS allocated NEF funds to invest in an electronic case processing system for the Office of Medicare Hearings and Appeals, modernization of the Resource and Patient Management System in the Indian Health Service, and the Centers for Disease Control and Prevention performed IT infrastructure enhancements to public health programs. Since the NEF was established, HHS has used this resource to provide support to critical Department-wide cybersecurity efforts, including activities to address emerging issues, which were then able to be urgently addressed. The NEF helps HHS meet both long-term IT procurement needs and address the needs of a rapidly changing cybersecurity environment, but could additionally benefit from ITMF. Without these types of funds, HHS would struggle to make necessary modernizations to keep our IT systems current and secure.

The NEF also enabled the successful financial systems modernization effort I mentioned at the outset of my comments today. The NEF is an important funding source for large-scale projects to modernize systems, improve the underlying infrastructure, and leverage new technology. These are the types of projects that can drive transformational change, improve mission delivery, effectiveness, and efficiency. More importantly, these are the types of projects that address the risks associated with operating on outdated and unsupported platforms.

Simply put, the cost of doing nothing is not nothing. As systems age, the risks to security, reliability, and availability are very real – increasingly so these days, as attempts to exploit system vulnerabilities become more sophisticated. HHS's financial systems and other IT systems have benefitted from NEF funds. Given the scale of HHS's operations and the scope of its programs, the implications of a system breach or failure represent risks that are difficult to quantify.

Understandably, HHS's front-line programs receive much visibility– these are important programs, after all they touch and improve the lives and well-being of countless Americans. It is imperative to recognize, however, that these programs cease to operate effectively and efficiently without a secure and reliable IT infrastructure supporting them. The NEF and the ability to use those funds effectively, addressing the Department's most pressing business needs, supports the sustainability of HHS's IT environment and HHS's mission. I thank you for your continued support and authorization of these essential dollars.

Conclusion
HHS recognizes that IT investment planning and management is a dynamic and fluid process that occurs at multiple levels. IT investments must be selected with involvement of key stakeholders and with the understanding of mission risk. Once selected, IT investments must be continually monitored and evaluated to ensure that each approved IT investment effectively and efficiently supports the agency mission.

The federal government, through adoption of the IT Modernization Fund, has the ability to make meaningful changes to IT legacy systems and measurably improve the mission and business effectiveness of the federal government. My comments today have highlighted this impact at HHS – from developing a strategic approach to comprehensively modernizing HHS's IT portfolio, to managing these large, complex initiatives and being effective stewards of the funds entrusted to the Department, to enabling improved mission delivery supported by a secure, reliable, and high-performing IT environment. It is a track record I hope to build on, working with you and your Congressional colleagues on future endeavors. Thank you for the opportunity to speak with you today and I look forward to answering your questions.

First, a board of experts, acting independently of any one agency and utilizing an objective, rules-based methodology, will identify the highest-priority projects across the Government, ensuring that the Federal Government's most pressing and highest-risk systems are targeted for replacement. In addition, the board will identify opportunities to attain economies of scale in IT infrastructure by replacing multiple legacy systems with a smaller number of common platforms, facilitating a Government-wide transition to common platforms and re-engineered business practices.

Second, the ITMF will require agencies to pay back the fund over time. Doing so will ensure that the ITMF is self-sustaining and can continue to support modernization projects well beyond the initial infusion of capital. We estimate that the $3.1 billion in one-time seed funding could address at least $12 billion in modernization projects over the first 10 years and will continue to remain available into the future.

Third, experts in IT acquisition and development will provide integrated modernization expertise to agencies that need it to implement their modernization plans. Further, we will maintain a public dashboard listing every ITMF-funded project, including a description of the project, key milestones, and financial expenditure data. As a result, every project that receives funding will benefit from centralized oversight and expertise, increasing the probability of success.

Fourth, the ITMF will have the ability to provide funding in smaller increments tied to real-world delivery of working products versus one annual appropriation. This approach ensures that agencies employ agile development techniques and that funds support successful projects.

Finally, by requiring agencies to apply and compete for incremental funding, the ITMF will provide strong incentives for agency leadership to develop and implement comprehensive, high-quality, and cost-effective modernization plans.

Conclusion

Ultimately, retiring or modernizing vulnerable and inefficient legacy IT systems will not only make us more secure, it will also save money. As a means of addressing these pressing challenges, the ITMF is a crucial step in changing the way the Federal Government manages its IT portfolio. In short, the ITMF will enhance agencies' ability to protect sensitive data, reduce costs, and deliver world-class services to the public.

I thank the Committee for holding this hearing, and for your commitment to addressing the challenges associated with legacy IT. We look forward to working with Congress on this critical initiative. I am pleased to answer any questions you may have.

Chairman CHAFFETZ. Thank you.

Mr. Scott, you are now recognized for 5 minutes.

STATEMENT OF TONY SCOTT

Mr. SCOTT. Thank you, Chairman Chaffetz, Ranking Member Cummings, members of the committee. I appreciate the invitation to appear before you today.

As has been noted, Federal agencies spend nearly three-quarters of their IT budgets maintaining legacy systems. They are particularly vulnerable to malicious cyber activity, and they are often unable to utilize current cybersecurity best practices, such as data encryption, multifactor authentication, and other techniques.

But in addition to posing security vulnerabilities, these systems are often very inefficient and subject to rising costs over time, and the inability to meet mission requirements. To address these challenges, the administration has proposed the creation of an information technology modernization fund to facilitate the transition of Federal systems to more secure, cost-effective, and more modern infrastructure, such as cloud platforms.

The ITMF would address these challenges associated with legacy IT by better aligning with the following private sector best practices.

First, a board of experts acting independently of any one agency will review agency proposals and select the highest priority projects across the government, ensuring that the Federal Government's most pressing and highest risk systems are targeted for replacement.

Second, the ITMF will require agencies to pay back the funds as projects complete. Doing so will ensure that projects receive significant buy-in and attention from agency leadership, and that, over time, the ITMF is self-sustaining and continues to support future modernization projects. We estimate that the $3.1 billion in one-time seed funding could address at least $12 billion in modernization projects over the first 10 years and would continue to remain available in the future.

Third, experts in IT acquisition and development will provide expertise to agencies in implementing their modernization plans. To increase the probability of success, every project that receives funding will have access to centralized expertise, including a public-facing dashboard that tracks key milestones and financial expenditure data.

Fourth, the ITMF will have the ability to provide funding in smaller increments tied to real-world delivery of working products. This agile approach ensures that agencies employ modern development techniques and that these funds support successful projects.

Finally, by requiring agencies to apply and compete for incremental funding, the ITMF will provide strong incentives for agency leadership to develop and implement comprehensive, high-quality, and cost-effective modernization plans.

Retiring or modernizing vulnerable and inefficient legacy IT systems will not only make the government more secure, it will also save us money. As a means of acting on this necessary next step, we look forward to working with Congress on enacting the ITMF, which will enhance agencies' ability to protect sensitive data, reduce costs, and deliver world-class digital services to the American people.

I thank the committee for holding this hearing, and I would be pleased to answer any questions that you might have.

[Prepared statement of Mr. Scott follows:]

Embargoed until Delivered

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503
www.whitehouse.gov/omb

TESTIMONY OF TONY SCOTT
UNITED STATES CHIEF INFORMATION OFFICER
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

May 25, 2016

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, I appreciate the invitation to appear before you today to speak about the challenges posed by antiquated technologies and the opportunities to improve cybersecurity and achieve cost-savings presented by transitioning to more secure, efficient, and modern IT systems.

Challenges Associated with Legacy IT

Currently, civilian agencies spend nearly three-quarters of their IT budgets maintaining "legacy" IT systems. These systems often pose significant security risks, such as the inability to utilize current security best practices, including data encryption and multi-factor authentication, which make them particularly vulnerable to malicious cyber activity. These systems may also pose operational risks, such as rising costs and inability to meet mission requirements. Absent timely action, the cost to operate and maintain legacy systems, as well as security vulnerabilities and other risks, will continue to grow.

What the Administration Has Done

To address these challenges, the Administration has proposed the creation of an Information Technology Modernization Fund (ITMF) to facilitate the transition to more secure, efficient, and modern IT systems and infrastructure, such as cloud platforms, while also establishing a self-sustaining mechanism so that Federal agencies may benefit from these resources into the future.

How the ITMF Would Improve Outcomes

The ITMF would address the challenges associated with legacy IT in a number of unique ways. The ITMF process will better align with practices from the private sector, where significant IT investments are often presented to a corporate capital committee for approval, and require a viable business case that demonstrates sound architecture and measurable outcomes, such as lower life-cycle costs and improved performance.

Chairman CHAFFETZ. Thank you. Thank you all.

I will now recognize myself for 5 minutes, but I will yield my time to the chairman of the Subcommittee on IT, Mr. Hurd of Texas.

Mr. HURD. Thank you, Mr. Chairman. Thank you and the ranking member for the leadership on this issue.

I always say that nobody is going to hold a rally for IT procurement, but when I am back home, everybody asks about this question because they recognize that $80 billion is being spent on IT procurement and 80 percent of it is on legacy systems. It is about using American taxpayer dollars wisely. It is about making sure we have an efficient government that is providing services to our citizens. And it is making sure that we are using technology that is keeping us safe and protecting our digital infrastructure.

My first question is to Mr. Halvorsen. When did you come into the position as CIO?

Mr. HALVORSEN. I have been in this position about 2.5 years.

Mr. HURD. Are you familiar with the Expeditionary Combat Support System?

Mr. HALVORSEN. I am.

Mr. HURD. And that is a system that was canceled in 2012, after spending more than $1 billion and failing to deploy within 5 years of initially obligating funds. Is that accurate?

Mr. HALVORSEN. It is.

Mr. HURD. One of the things that we are looking at in the FITARA scorecard is incremental development. It's major development investments and are they achieving measurable goals every 6 months? DOD is listed as an F when it comes to delivering this. As of May 2016, only 41 percent of those projects are being delivered.

In asking for a modernization fund and additional funds, what is going to be done differently in the Department of Defense to ensure that, if you do have more money for investments on updating legacy IT systems, that you are going to actually hit the mark on time?

Mr. HALVORSEN. I would say a couple things.

One, we are a little out of sync with the grading criteria in that we have a 6- to 12-month, not a zero- to 6-month grade within DOD. We are moving that more forward, so we leveled that time to 6 to 12. It was higher before.

I think if you look at the things we have done recently, you will see that we are doing things in modernization. The move to Windows 10 is the single biggest move to a single operating system ever undertaken by any organization. We are getting that done. We have a 1-year time frame. We are on track to do that. We will hit 80 percent of DOD in a year.

We have done more modernization with the commercial sector. I think that is the important piece that we need to recognize here. Our modernization needs to be done much more in conjunction and partnership with the commercial sector.

Mr. HURD. So, Mr. Halvorsen, are you saying buy, not build?

Mr. HALVORSEN. I am saying buy mostly, not build.

Mr. HURD. Excellent.

My next question is for Mr. Milholland. What is Treasury's strategy to manage unsupported technologies, such as the mainframe capabilities where it states the Treasury will assume the risk of the expired support technology? We sent a letter out to every agency asking for old programming language that is being used, systems that are no longer supported by vendors. In some of these systems that are no longer supported by vendors, Treasury is saying that they are assuming the risk for that expired technology.

What is the strategy to manage these unsupported technologies?

Mr. MILHOLLAND. I am not the Treasury CIO, so I cannot answer that completely, but we are a large part of that organization.

Mr. HURD. In some of these, the response was saying that the IRS will be assuming the responsibility for managing that.

Mr. MILHOLLAND. Yes. We believe that all of the technologies we have today are, in fact, supported. For example, when we were completing the drive to get to Windows 7, we worked out a special support deed with Microsoft to cover the Windows XP environments while we were completing the job, for example.

The rest of the environments, like what you call the mainframes, which is a Systems z, is, in fact, fully supported by the supplier, IBM. It is a very modern operating system. We are running Linux on the z. In fact, our main migration path for all new development is to build these applications with Java and run it on the z, or wherever best. It could be on an Intel processor.

We are also using the dollars to stay current whether it is the BIOS, whether it is operating systems, whether it is the middleware, whether the tools you are using, or the cross product, be more no more than n or n-1 versions behind.

Mr. HURD. I copy, Mr. Milholland, and I only have 10 seconds left.

Do you have a modernization roadmap that creates a common modern platform for mission delivery?

Mr. MILHOLLAND. Absolutely. In fact, we have shared it with this committee. We call it the technology roadmap, part of delivering of what we call the future state for the IRS.

Mr. HURD. Where are you in implementation?

Mr. MILHOLLAND. We are just at the very beginning for that, for the migration to be the digital enterprise. But part of that is the modernization of all the legacy systems, which includes replacing that assembly language code with Java. That is in part driven by the CADE2 project that is underway.

Mr. HURD. Thank you, Mr. Chairman. I yield back.

Chairman CHAFFETZ. We will now recognize the gentleman from Virginia, Mr. Connolly, for 5 minutes.

Mr. CONNOLLY. Thank you, Mr. Chairman, and I thank the ranking member for his ongoing support that has allowed us to elevate this issue in this committee and actually created enormous common ground.

Thank you, Mr. Cummings, especially.

Welcome to the panel.

Mr. Scott, we are talking about legacy systems, but has there been a comprehensive audit of Federal agencies, so we actually know the full universe we are talking about?

Mr. SCOTT. There is a data collection effort underway currently where we hope to gain better insight into actually what it is. I would say that some of this is problematic in the sense that much of the data isn't automated in the sense that you can just push a button and get a digital report in the as-is environment. So we don't have a comprehensive ——

Mr. CONNOLLY. But the fact of the matter is —anecdotally, right?—we've had, maybe we still have, Federal agencies with multiple email systems ——

Mr. SCOTT. Correct.

Mr. CONNOLLY.—not all of which are compatible; multiple HR systems, not all of which are compatible; huge numbers of data centers that proliferated, and God only knows what coordination exists among the thousands of data centers we are trying to consolidate; and legacy systems. And on top of legacy systems, isn't it also true we have widely distributed software products that also need updating or patching?

Mr. SCOTT. This is correct. One of the techniques we have used to estimate the level of legacy systems is I recently went to some of our key suppliers of network storage computer equipment and asked them to provide us data in terms of what they know about the Federal Government.

One of the interesting things coming back was, in many cases, we pay for support contracts for hardware, software that they have sold the Federal Government.

I asked them to look at what is either expired or will expire in the next 3 years, to try to get some handle on what that might look like, just from their own records.

These are systems that we are paying today for support contracts on.

In just the next 3 years, we will have over $3 billion worth of hardware, software, and services that will go out of support, meaning no spare parts, no patches, no upgrades, no security.

Mr. CONNOLLY. Isn't it also true—I am running out of time, so forgive me for interrupting—that we have had to hire 3,427 IT professionals just to maintain legacy systems?

Mr. SCOTT. That sounds about right, yes.

Mr. CONNOLLY. Wow. Any idea what the estimated cost is to replace all the legacy systems in the Federal Government?

Mr. SCOTT. We don't have an accurate estimate of that. We've tried to triangulate it in a number of different ways. That's why we ended up with the $3 billion proposal. We think that is at the low end of what would be required to make a meaningful start to this.

But I think the more important concept we should all embrace is, given the rapid advance of technology, we really need to get into a continuous upgrade mode, not a "wait until it breaks" mode.

Mr. CONNOLLY. Right. And I want to deal with something, because the chairman has on several occasions cited the fact that you have $82 billion a year you spend on procurement. He cited in his opening statement the fact that this administration, over its lifespan, has increased that. That total amount represents an increase of about $6 billion.

Why isn't that sufficient? Why do you need more money? Why do you need this modernization fund, when you have such a substantial amount of money we are spending every year, and even that amount might be understated, in terms of not capturing other expenses within the Federal family?

Mr. SCOTT. I agree with the wide observation that there is an opportunity to save money. The challenge is, as was already said, a lot of that money is spent on just keeping the lights on the current old stuff.

Unfortunately, we cannot shut that off until we have a replacement in place, so you cannot actually capture the savings until after you have done something to replace it. That is why this concept is important.

Mr. CONNOLLY. Sort of dovetailing with, I think, one the chairman's points, I do think the burden is going to be on the Federal Government, the executive branch.

Okay, let's say, we authorize the modernization fund, buying the argument that we are going to have to make an initial outlay to achieve savings. There is going to have to be a codified savings and efficiency plan that shows we can make IRS, DOD, and HHS, and every other Federal agency, this much more efficient, and either keep a budget stable or, in fact, effectuate net savings because we have replaced those legacy systems.

I think the chairman has expressed that it is counterintuitive that we would actually need to add more money. I think you can sell that, the argument you just made, Mr. Scott, if you can demonstrate, “And here will be the payoff. Here is the return on that investment.”

I think we have to spend some real time with Congress in making that case.

I yield back.

Chairman CHAFFETZ. I thank the gentleman, because those last comments, I do agree with. I think that is the seminal question we have to get out and agree that is the question that we need to analyze on that particular piece of legislation.

I now recognize the gentleman from Florida, Mr. Mica, for 5 minutes.

Mr. MICA. Thank you, Mr. Chairman. And thank you for holding this, it's kind of a meat-and-potato hearing. It is not flashy like some we do.

I had the privilege to serve with a very capable ranking member, Mr. Connolly, with Government Operations. He is very knowledgeable, in fact, more knowledgeable than I was when I assumed that position and learned a lot from him.

Our objective was to look at the total amount of money we were spending at the time, which at that time was $80 billion. Now I see with your report that was released today, they are spending $89 billion.

The estimate when Mr. Connolly and I were doing our review was that about 50 percent of this money is wasted either on outdated technology, on duplicate data centers.

Would GAO or OMB, would you say that about 50 percent is not properly spent, is wasted? Is that still about where we are?

Mr. SCOTT. Yes, I think it would make sense to say, if you missed multiple generations of the opportunity to improve your computing environment, you are wasting money. It is very clear.

Mr. MICA. What do you think, GAO?

Mr. POWNER. I do not know if it is 50. I will say this, I don't know that I have a precise number, but there is a lot of money spent on inefficient operations, data centers, and there are a lot of failed acquisitions. So clearly, there are billions wasted.

Mr. MICA. Your report says Federal legacy IT investments are becoming increasingly obsolete. Many use outdated software languages and hardware parts that are unsupported. Agencies reported using systems that have components that are in some cases at least 50 years old.

This is your finding.

Mr. POWNER. Correct.

Mr. MICA. Well, we won't even go half, if we just go $40 billion in waste.

When Mr. Connolly and I started this exercise, we asked you all how many data centers there were. I think, first, we got 800 or something. Then we got 1,200. Then we got, oh my God, we were in the thousands.

I was interested to see in your report here how many thousand data centers we have.

What is that current number?

Mr. POWNER. It is about 10,500.

Mr. MICA. Ten thousand five hundred. What would you guesstimate we could reduce that to?

Mr. POWNER. Well, we have closed 3,100 to date and saved $2.8 billion. We can close another 2,000 and save $5.4 billion. I think that $5.4 billion is greatly understated because many agencies ——

Mr. MICA. So we can actually spend less and get better technology, better results, and improved systems. Is that correct?

Mr. POWNER. Yes, we need to definitely get more modern.

Mr. MICA. So the opening salvo from the other side was that Republicans are slashing the money. But actually, we have actually saved money by going to the cloud. Is that correct, sir?

Mr. POWNER. Yes, there have been savings.

Mr. MICA. And there are certain concerns about security. We do have the cyberthreat.

A great deal of the data in the Federal Government is not classified or necessarily high-security risk, is it, Mr. Powner?

Mr. POWNER. It varies. It clearly varies.

Mr. MICA. But again, your report points out there can be very substantial savings consolidating these data centers, 10,000—we have done some—and then moving to the cloud and other—now the question came from Mr. Hurd a little bit about buy or build, and the answer was build. What about buy or lease? Can somebody say we should be leasing?

The problem is that the Federal Government buys equipment, and the equipment, I will take you back here, we have it even in our offices, is outdated. Maybe Mr. Davis bought some of it, but now Mr. Chaffetz has inherited it. That is the way agencies work, the same way.

So buy or lease, anyone want to respond? Mr. Scott? Mr. Powner?

Mr. SCOTT. Well, I think our guidance as proposed would rate projects that use cloud, use these more modern techniques, the buy-by-the-drink kind of thing, versus build it yourself. That is a high-scoring criteria for those projects.

Mr. MICA. But where are you going to get equipment in an office, buy or lease?

Mr. SCOTT. You have to have a replacement strategy and often that means leasing.

Mr. POWNER. Yes, so I think, clearly, we want to build less in the Federal Government. There is less risk with that.

Mr. MICA. Thank you. I yield back.

Chairman CHAFFETZ. I thank the gentleman.

We will now recognize the ranking member of the Subcommittee in IT, Ms. Kelly of Illinois, for 5 minutes.

Ms. KELLY. Thank you, Mr. Chair.

As ranking member of the IT Subcommittee, I have been working with Chairman Hurd on the very issue of legacy systems. One of the topics consistently discussed is moving to the cloud.

The CIO.gov Web site says the government's current information technology environment is characterized by, and I quote, "low-asset utilization, a fragmented demand for resources, duplicative systems, environments that are difficult to manage, and long procurement times." It goes on to say, and I quote, "Cloud computing has a potential to play a major part in addressing these inefficiencies."

Mr. Scott, can you briefly explain what is cloud computing?

Mr. SCOTT. Generally, it is an environment that leverages the power of virtualization, of compute, of storage, of networking, as though it were one operating system that allows individual programs to scale up or scale down and get better asset utilization in aggregate than would be the case in the alternative, which is to have a bunch of individual servers.

It is often surrounded by sets of utilities and other mechanisms that allow for the provisioning and de-provisioning of computer environments very quickly, which also saves time and makes IT more efficient.

Ms. KELLY. So you started explaining what an important role it can play in helping agencies modernize their IT systems. Can you expand on that?

Mr. SCOTT. One of the benefits of the cloud is the agility factor, and then just the scale that most cloud environments exist in.

So I used to talk about the double-double rule as the primary way by which system engineers create and compute. If you are in the old days an engineer and you are configuring a server, you would figure out what it was going to take to support that application. You would double it, and then you would double it again. That was just an unwritten rule about how engineers would configure systems.

So it was no wonder that when you went into the data center, you would find things running at 15 percent or 20 percent of their capacity.

What cloud does is aggregate all of that together. Then you can run the whole plant at 70 percent, 80 percent, or 90 percent efficiency instead of 15 percent. That saves money.

Ms. KELLY. Can you tell us what, if anything, the Office of Management and Budget has been doing to encourage agencies to move toward cloud computing solutions?

Mr. SCOTT. As we have talked with agencies about their plans, we have highlighted the opportunity to do that and ask questions. We are requiring them to show us what their modernization plans are and highly favoring both cloud but also virtualization and other modern development techniques. We are encouraging the buying of services rather than developing them themselves. We are also encouraging the use of shared services.

So one of the challenges is, in the old world, every agency thought it had to do everything top to bottom by itself. As was mentioned in the case of email or shared networks or payroll systems or financial systems, there is a great opportunity to use more shared services and not have every agency do everything top to bottom on its own.

Ms. KELLY. I'm glad to hear that, because I wondered in another hearing, but didn't get a chance to ask the question, about how often do we share.

Back in July 2010, David McClure, then associate administrator of the General Services Administration, testified before this committee that cloud computing would, and I quote, "increase the overall IT security posture of the government."

Can you explain how cloud computing can improve the Federal Government's overall IT security?

Mr. SCOTT. We have a FedRAMP standard that takes all of the best practices of security and puts together a template and a process that providers can certify against that includes background checks and other things like that on the people that are actually operating the systems, and, taken altogether, is much more comprehensive than what we would typically find in a sampling of individual agencies or individual environments.

These are businesses that depend on high security for their reputation and future business models, so they often take it far more seriously and can put the resources toward it that maybe a small organization might not be able to.

Ms. KELLY. Thank you.

Thank you, Mr. Chair. I yield back.

Mr. MULVANEY. [Presiding] I thank the lady.

The gentleman from Texas, Mr. Farenthold, is now recognized for 5 minutes.

Mr. FARENTHOLD. Thank you, Mr. Chairman.

Mr. Milholland, you and I think several other members of the panel testified that one of the things holding you back from getting rid of these legacy systems and upgrading was budget concerns. I have to tell you, one of the things I consistently hear from everybody who comes into my office, whether they are advocating for education or increased medical research is, "Give me more money today, and I will give you savings tomorrow."

Now, this is, I think, part of our Federal Government budgeting mentality, that we do not think enough like the private sector. You look at what is happening in the private sector right now, when I started practicing law, we were on IBM Selectrics. We moved to a mini-computer and moved to a PC network. And we went from one assistant for every lawyer now to one assistant for every four or five lawyers through the technology.

You look at what the IRS has done. You have millions of people e-filing your taxes. You now don't need people in data centers keying that into the computer.

So the savings are coming naturally. So I have a kind of two-part question here. One, can you quantify, "If you give me X billion dollars today, I will save you Y billion dollars over the next," and we will take a lifespan of the computer, 5 to 7 years? Can that be quantified?

Second of all, isn't there a way within your budget to pay for this incrementally with the savings you are going to get?

Mr. MILHOLLAND. I will try to answer that two-part question.

With respect to the IRS and investment in IRS, people have said returns for about every dollar are $4 in revenue to the U.S. Often, a lot of that occurs because of the investment in the underlying IT infrastructure.

Where we have suffered is that the budget has been reducing, not staying flat. I have been told that we are ——

Mr. FARENTHOLD. Isn't that what we are trying to do? I am going to give you a dollar and then, over the next 10 years, I'm going to reduce your budget by $4, and we are going to be in the same place by your figures.

Mr. MILHOLLAND. But, sir, you also increased the tasks that we have. For example, far more people now are, in fact, filing income taxes.

Mr. FARENTHOLD. I would be much happier if you guys weren't having to fool with Obamacare, I will tell you that.

Mr. MILHOLLAND. Well, there are a number of unfunded mandates like that that we have had to absorb, whether it has been Obamacare, FATCA, there is HCTC, the ABLE Act ——

Mr. FARENTHOLD. I do not have much time, so let me go to Mr. Scott.

Can you talk about that on a broader scale?

Mr. SCOTT. Yes, in fact, if we can show the chart that I brought, I don't know if they can put that up.

What we did is we studied—we took a sample out of our database of projects across the Federal Government, this is across hundreds and hundreds and hundreds of investments, where there was an injection of modernization money prior to 2013. Then we looked and we compared that against projects where there was no injection, and what happened to the maintenance costs of those investments over time.

What you see is a very clear trend. Where there was no injection of money to go fix things, costs continued to rise at a rate of around 6 percent.

Mr. FARENTHOLD. This number doesn't even take in reduced personnel costs. I'm assuming that as we modernize technology, as we see in law firms or banks with ATMs instead of tellers, we ought to see an even bigger cost decrease as people are able to work more efficiently. So we ought to be able to save money and deliver better service to the hardworking American taxpayers who are our customers.

Mr. SCOTT. I think we would see, if we factored all those factors in, an even sharper drop. In cases, as shown in the chart there, where there was an investment, costs would continue to go down at a much faster rate. So they went down at least 5 percent a year on average, where there was an ——

Mr. FARENTHOLD. I would love to see an agency come in here and say, "All right, give me this much money to modernize my IT, and you can cut my budget by this much."

Mr. SCOTT. Well, this is actual data over an at least 4-year period, based on actual experience in the government, so I think it proves the case.

Mr. FARENTHOLD. All right, if I am able to get back for a second round of questions, I do want to address the DOD hackathon and the success that had.

But my time has expired, and I will yield back.

Mr. MULVANEY. I thank the gentleman.

I now recognize the gentleman from California for 5 minutes, Mr. Lieu.

Mr. LIEU. Thank you, Mr. Chairman.

Let me first say I've read the biographies of the witnesses today, and all of you could be making a lot more money in the private sector, so thank you for your public service.

I do have a question for Mr. Halvorsen. The GAO identified a 53-year-old legacy system in the Department of Defense known as the Strategic Automated Command and Control System. This system coordinates operational functions of the United States of nuclear forces, such as intercontinental ballistic missiles and nuclear bombers. Is that correct?

Mr. HALVORSEN. Not exactly.

Mr. LIEU. All right, what does the system do?

Mr. HALVORSEN. It is a tertiary—I can only go into the system a little bit. It is a tertiary system that is responsible for delivering two small, very important messages as a third backup. That is what that system does today. It is a tertiary system.

And we are actually investing in the NC3 system to change the way we deliver that whole product.

Mr. LIEU. The reason you cannot talk more is because the rest is classified?

Mr. HALVORSEN. That is correct.

Mr. LIEU. Okay. This system is still running on IBM Series 1 computer, which is in 1970s computing system, according to the GAO, and written in Assembly language code. The GAO also reports that the system currently uses 8-inch floppy disks, which are a 1970s-era storage device. Is that accurate, sir?

Mr. HALVORSEN. That is correct.

Mr. LIEU. Okay. So this system also, as I think you noted, sends and receives emergency action messages to nuclear forces. Is that correct?

Mr. HALVORSEN. A tertiary system for doing that, yes, sir.

Mr. LIEU. I got that, but it does send and receive emergency action messages to nuclear forces.

You would agree that our nuclear forces are pretty darn important?

Mr. HALVORSEN. I would.

Mr. LIEU. Okay. You had in your testimony earlier today said that the Department of Defense is not of balance with other private sector companies, and that your priorities are right. Are you aware of any other successful private sector company that uses 8-inch floppy disks?

Mr. HALVORSEN. I am not, but I am aware of other private companies that use similar technology. No one is saying that we should continue to use the 8-inch discs much longer, but I would point out a couple things. The reliability factor on that system is where I need it to be, which is five 9s, 99.999 percent. It is completely secure because it is a closed system. So while I want to fix it, all I am saying is that in the priority of things that I need to fix, that will be in probably year 3 of my next 5-year plan. It is not in the top priority of things I think either I want to fix or you would want me to fix, in terms of priority.

Mr. LIEU. Why are you fixing it at all, if it is not as important as you say it is, if it is just this classified system you cannot even really talk about for nuclear forces?

Mr. HALVORSEN. I didn't say it wasn't important. I said it was a tertiary system. And what I am fixing is the entire way that we are going to deliver that whole process.

I won't actually replace this system. The system is going to go away and be replaced by a different method of delivery.

Mr. LIEU. And it'll be done by year 3?

Mr. HALVORSEN. It will.

Mr. LIEU. Okay, thank you, sir.

So, Ms. Killoran, I have a question for you about another system the GAO identified. It is the Health and Human Services Medicare appeals system. Can you explain what that is?

Ms. KILLORAN. Yes. That system is a system that we actually have that plaintiffs can file appeals to claims that they have. It is actually a business process flow and goes through three of the five levels of appeals.

Mr. LIEU. And a fair number of Americans have Medicare appeals, and the system helps them?

Ms. KILLORAN. Yes. It allows them to get not only notifications and status, but it also sends out letters.

Mr. LIEU. And the system also helps respond to congressional inquiries, correct?

Ms. KILLORAN. Correct.

Mr. LIEU. Do you have any plans to update that legacy system?

Ms. KILLORAN. So that legacy system is 10 years old. We actually do have—the system has been updated to make sure that the software is current and the hardware is current. One of the things that we slightly disagree with on the audit is just because something has a particular age doesn't necessarily mean that it is end-of-life.

As Mr. Scott had talked about, all of the operating system, the software and the hardware for this particular system, is completely up-to-date and supported by the vendor at this time. So we don't have a plan to replace, but we are going to keep updating it and making sure that it is current.

Mr. LIEU. So your view is the system is working currently, and there is no need to upgrade it?

Ms. KILLORAN. So we have been doing continual upgrades as we have different mandates and there have been requirements for operating system changes and software to keep it current, yes.

Mr. LIEU. Thank you.

Let me conclude by thanking Ranking Member Cummings and Chairman Chaffetz for holding this hearing, and I want to thank the ranking member for his support of the IT modernization bill, which I'm a co-author of as well, and hopefully we can get that through.

With that, I yield back.

Chairman CHAFFETZ. [Presiding] I thank the gentleman.

We will now recognize the gentleman from South Carolina, Mr. Mulvaney, for 5 minutes.

Mr. MULVANEY. I thank the chairman. I'm over here in the corner.

I guess my questions are, Mr. Connolly was here, and I'm always frightened when I agree with him, but I agree with him more and more when we do these oversight hearings. I want to focus a little bit on how we got here.

I heard the ranking member talk about the draconian budget cuts. Mr. Milholland, I heard you mention draconian budget cuts. Certainly, at the IRS, I apologize, I don't have the HHS numbers or DOD, so I don't want to appear to be picking on the IRS, but they are the numbers I could get in the last 5 minutes. Certainly, your budget has been cut in the last couple years, 3 percent this year. It was up 0.8 percent the year before that. Down 5 percent the year before that. Down 2.5 percent the year before that.

But I think we would all agree that when you are still using technology and computer systems from the 1970s and 1980s, this is not a problem that started in 2012, okay?

I see that Mr. Milholland is nodding his head.

I go back to 2000, Mr. Milholland, when the Republicans were in charge, actually, and your budget went up almost 6 percent, the next year 8.5 percent, the next year almost 4 percent, then 4 percent, 4 percent after that. The Democrats take over in 2007, your budget is up 4.73 percent, 3.8 percent, 5.4 percent.

How can you really sit there and tell us this is money? I mean, you got bigger increases than everybody else in the country in 2008. I can assure you there were private industries and businesses and households that didn't see a 5.4 percent increase in their budgets during the recession.

I mean, how can you sit there with a straight face and say it is money? While that is convenient today and ties into what the ranking member was saying, haven't you been mismanaging the money since the 1970s and 1980s? Isn't that the only way you end up in this problem?

Mr. MILHOLLAND. I think there is a different way to characterize it than management. I can't speak for my predecessors at all, but decisions made back in the 1970s and continued into the 1980s and 1990s and the first decade of this century basically said, "Let's build a set of systems that automate the paper processing set of systems." So the way taxes were handled in the 1940s and 1950s and 1960s became automated in the way that computer systems were designed.

That means that when you file your taxes even electronically today, they are actually batched up electronically in a set of files that then need to be passed from system to system. There are lots and lots of interconnections that make that possible.

The program was written in Assembly language. By the way, it is written very elegantly. It is incredibly well-engineered for the time it was designed and built. The underlying infrastructure is very much state-of-the-art. That is why we can process returns so fast.

But we are constrained by those past decisions and the ability to share that data with I will just say new programs that we want to provide, so we are—I'm sorry, go ahead.

Mr. MULVANEY. Does anybody that you know, anybody on the whole panel, does anybody in the private sector do it the way the government does it? Are there any private companies out there using 8-inch floppy disks and expired languages and machines they cannot get pieces for? Is there anybody out there who does this?

Mr. MILHOLLAND. There are certainly companies that use old programming languages like Assembly language and COBOL and Fortran and others. Most are converting themselves like we are to a modern programming language, all new development beginning with Java, for example, or other modern programming languages.

They use modern development techniques, so that you start with building a data model for your enterprise rather than have it as an afterthought with security built in.

I think the current practices, we would not have done it that way, if we had the knowledge we have today.

Mr. MULVANEY. Mr. Milholland, you mentioned something about your predecessor, and someone mentioned something in the previous testimony. How long have you been in this position at the IRS?

Mr. MILHOLLAND. I have been here not quite 8 years.

Mr. MULVANEY. What is the average tenure? This may be to the OMB or GAO. What is the average tenure of a CIO at our major agencies?

Mr. POWNER. Two years.

Mr. MULVANEY. Is that a problem?

Mr. POWNER. It is a huge problem.

Mr. MULVANEY. Why?

Mr. POWNER. Well, in regards to legacy systems, what CIO wants to come in over a 2-year period and undertake one of these massive conversion efforts? They pick the low-hanging fruit and get quick wins, and they don't tackle the difficult stuff often enough.

Mr. MULVANEY. Who controls the tenure of a CIO at a major agency or department? Does Congress? Anybody?

Mr. SCOTT. It depends. Some are Senate confirmed. Most are appointed politically.

Mr. MULVANEY. Right, but if we are going to say that Mr. Halvorsen is going to be CIO at DOD, and we leave him there 2 years, whose call is that? Is it ours or somebody else's?

Mr. HALVORSEN. Depending on when the 2 years started, it would generally be the Secretary of Defense's call. But I am politically appointed, so I will change out with the administration.

Mr. MULVANEY. It is an executive decision. It was sort of a rhetorical question. Congress doesn't say that you have a 2-year term at DOD, or a 2-year term at HHS, or at any agency. It is an executive decision under both administrations.

Mr. Powner, I take it your data goes back to Republican administrations as well.

Mr. POWNER. Yes, it goes back a long way. We have done multiple studies dating back for years on this.

Mr. MULVANEY. Thank you, Mr. Chairman.

Chairman CHAFFETZ. I thank the gentleman.

We will now recognize the gentleman from Massachusetts, Mr. Lynch, for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman and the ranking member, for holding this hearing. It's very important.

I would like to ask unanimous consent to enter into the record the GAO report to congressional requesters entitled, "Federal Agencies: The Need to Address Aging Legacy Systems." We have been referring to that during our questions. I just wanted to get on the record.

Chairman CHAFFETZ. Without objection, so ordered.

Mr. LYNCH. Thank you, Mr. Chairman.

I also have another report here that was generated with a bunch of folks, including the Department of Homeland Security, Intel, EMC, a whole bunch of people. And it is entitled, "2016 Data Breach Investigations Report."

Chairman CHAFFETZ. Without objection, so ordered.

Mr. LYNCH. Thank you.

The trend that the data are indicating from these reports are that the time frame for breaches and infiltration is going down, so it is measured now in days or, in many cases, minutes, yet our time for detecting breaches and infiltrations and the detection of fraud and response is weeks and months. So the numbers are going against us. Time is not on our side, as some have said.

At a previous hearing, we had OPM up here. They did not even encrypt the Social Security numbers for 21.5 million Federal employees. So while I hear a lot of this positive talk, I am concerned about factually what is going on.

Mr. Powner, the GAO did a great report, by the way. Thank you very much. I appreciate that. But one of the GAO's key findings is, and I quote, "While Federal agencies had specific plans to retire or modernize some of these legacy investments, most of those legacy investments did not have specific plans with time frames, with activities to be performed, or functions to be replaced or enhanced." Is that correct?

Mr. POWNER. That is correct.

Mr. LYNCH. So all this talk here is happy talk, and it worries me, especially as Mr. Lieu's line of questioning.

With respect to the Internal Revenue Service Individual Master File, GAO stated, and I quote, "The agency has general plans to update the system, but there is no time frame established for this transition." Would you agree with that statement?

I want to ask you next, Mr. Milholland.

Mr. POWNER. Yes, that is true.

I will add, though, there has been a lot of good work done to get the ball rolling that ——

Mr. LYNCH. Yes, that's not what I'm asking.

Mr. POWNER.—Mr. Milholland started. I will say his tenure over 6 years, he has done a lot.

Mr. LYNCH. I know.

Mr. POWNER. Hopefully, he can stick around a little bit longer and get IMF decommissioned.

Mr. LYNCH. Yes, that is not what I want to hear, but as Mr. Mulvaney said, this problem didn't happen yesterday. You are not to blame for the existence of this problem, but we have to do better, a lot better.

So, Mr. Milholland, do you want to defend yourself? Go ahead.

Mr. MILHOLLAND. We, in fact, do have ——

Mr. LYNCH. And thank you for your service, by the way.

We just have a problem here, and we have to fix it.

Mr. MILHOLLAND. Yes, sir.

Mr. LYNCH. So a little criticism ——

Mr. MILHOLLAND. I described the replacement of the Individual Master File. We are doing it in three phases. The second phase will end in 2019, at the latest 2020, again, depending on funding.

The principal issue there is now to convert the mainline code from Assembly language to Java. We have, in fact, have tackled the hardest, knottiest, most gruntiest part of this code, which is critical for processing taxpayer returns, to convert it to Java.

Mr. LYNCH. Okay.

Mr. MILHOLLAND. We, in fact, think, literally, we have found a breakthrough that we can do this. We think we can apply for three patents for this that will allow, once we are done, next March ——

Mr. LYNCH. Okay, sounds good.

Let me ask you, the master file there, so is our health care information on that now with Obamacare, because you are the repository for our health care information. How are you protecting that? Is that in the same file?

Mr. MILHOLLAND. It is not in the same file, but there are links to it. It is actually in a relational database that we built separate from the Individual Master File. But the systems are interconnected with appropriate data calls and ——

Mr. LYNCH. All right, let me jump to the GAO here.

The same GAO report found that HHS Medicare appeals system says, this is the report, “Agency officials state that they do not have any plans to address the gaps that were found by GAO and that doing so was contingent on funding.”

So let's go right to Ms. Killoran on that one.

Ms. KILLORAN. So, as I mentioned, for the Medicare appeals system, we actually have been making sure that that system is up-to-date, both with patches and software, and on a platform that is actually supported by the vendors.

So as a total system, we don't have plans to replace, but we are keeping it current and making sure that it is able to be supported.

Mr. LYNCH. Okay, my time is expired. Maybe we will do another round. Thank you.

Chairman CHAFFETZ. We will soon. Thank you.

Mr. Meadows of North Carolina is now recognized for 5 minutes.

Mr. MEADOWS. Thank you, Mr. Chairman.

Ms. Killoran, let me come to you. I think earlier in your testimony, you were talking about the fact that the FISMA reporting, you have submitted that. Is that correct?

Ms. KILLORAN. Yes, sir.

Mr. MEADOWS. So you have submitted that. Who do you submit that to?

Ms. KILLORAN. So we submit that to all of our FISMA committees, and we did that through our legislative channels.

Mr. MEADOWS. Okay. So who is responsible for that oversight? Is that Mr. Scott at OMB? Is he charged with making sure that those are all submitted properly? Do you submit it to OMB?

Ms. KILLORAN. So if you could clarify the question, are you talking about the report or ——

Mr. MEADOWS. Let me ask Mr. Scott. Mr. Scott, as the chief financial officer, is it your responsibility, I guess, for the executive branch, for the implementation of FISMA?

Mr. SCOTT. Yes, and we collect—I am the chief information officer, not the chief financial officer, but it is our ——

Mr. MEADOWS. Excuse me. You are the CIO for the Federal Government.

So essentially, it all comes to you, so they are required to submit that to you and to Congress, is that correct?

Mr. SCOTT. Correct. We aggregate and then submit to Congress.

Mr. MEADOWS. All right. So as it is submitted in those FISMA reports, as we look at that, each agency is required to do that. Is that correct, Mr. Scott?

Mr. SCOTT. Right.

Mr. MEADOWS. So let me ask you this. It appears that the Executive Office of the President, basically the White House, including OMB and the National Security Council, hasn't submitted the required FISMA. Is that correct?

Mr. SCOTT. I don't know off the top my head. I would have to check and get back to you. I don't know ——

Mr. MEADOWS. Well, we have done some checking, and we have been looking. Can you name a single year where the Executive Office of the President and OMB and the National Security Council have submitted a FISMA report?

Mr. SCOTT. We submit to Congress what has been submitted to us.

Mr. MEADOWS. I am talking about you. I understand they are doing it, but you are the one that has the charge. So has OMB, the White House, submitted it?

Mr. SCOTT. Oh, I see.

Mr. MEADOWS. Because we couldn't find yours.

Mr. SCOTT. Yes, we are not required by the law ——

Mr. MEADOWS. Well, but that's not correct.

Mr. SCOTT. That is our ——

Mr. MEADOWS. Is that what you're saying?

Mr. SCOTT. Our legal counsel has given us that ——

Mr. MEADOWS. Well, your legal counsel doesn't make the law.

So, Mr. Scott, let me remind you, Congress was very clear, extremely clear, that, indeed, the White House, and, indeed, OMB, is required to submit that. Yet we can't find where you've done it, and we specifically in the legislation mention the White House.

So you are saying your legal counsel has told you that?

Mr. SCOTT. That is the opinion we have gotten.

Mr. MEADOWS. When did you get that?

Mr. SCOTT. I have asked multiple times.

Mr. MEADOWS. Okay, I would suggest that you go back, check the law, and report back to this. Do you not think that if you are required by law to do it, and all these other folks are doing it, that it sets a bad example for you not to do that?

Would that set a bad example, if you are required to do that?

Mr. SCOTT. If we are required to, I think it sets a bad example, correct.

Mr. MEADOWS. All right. So you have counsel behind you. Are they saying that you are not required to by law?

Mr. SCOTT. I will go back and check and report back to you.

Mr. MEADOWS. Okay. And we would like to know some of the correspondence and actually where you've gotten that opinion from. Are you willing to give that to this committee as well?

Mr. SCOTT. That is not my call, sir.

Mr. MEADOWS. Okay, well, obviously, you are saying that you were told that, that you checked on it, and this is a conscious decision not to give a FISMA report on behalf of OMB and the office of the executive branch. Is that correct? That was a conscious decision?

Mr. SCOTT. It was a discussion and that was the conclusion that we came to.

Mr. MEADOWS. So what rationale would you really embark on embracing that would suggest that it is not a good idea to give information that you are requiring all the other agencies to give to Congress? Why would it not be a good idea for you?

Mr. SCOTT. Again, our intent is to comply with the law.

Mr. MEADOWS. But do you think it is a good idea that, even if it is not required, since you are requiring all the other agencies, don't you think it would be a good idea for you? I think the answer—don't you think it would be good idea?

Mr. SCOTT. I don't have an opinion on that, sir.

Mr. MEADOWS. Well, I do, and I think it would be a good idea. Let me come to the GAO. We are talking about all these legacy systems, and we continue to have hearing after hearing after hearing. What I find troubling is, is there a lot of savings that could be realized if we get rid of the legacy systems, jump off the cliff and say, "Let's make a commitment. We are going to do it." Is there substantial savings that could happen?

Mr. POWNER. Yes, there are. That $60 billion we spend on O&M. We have old legacy that if we could get more efficient systems, it would be less costly to maintain, it would be more secure. Then you already know that we have duplicative spending on commodity IT and inefficient data centers.

So the $60 billion has all kinds of inefficiencies in it. Our point is, we need more plans. I agree not everyone needs a plan. There might be some higher priorities. But we need more plans, so that we move that spending from 60 into the 20 bucket.

Mr. MEADOWS. Well, thank you. And I thank your staff for their great work.

And I yield back, Mr. Chairman.

Chairman CHAFFETZ. I thank the gentleman.

I'll recognize the ranking member, Mr. Cummings, for 5 minutes.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

I intentionally wanted to wait and listen to some of the testimony. I listened to Mr. Lieu, and I agree with him. When we read the resumes of you all, we realize that you could be somewhere else, making a lot more money. I think, in a way, that's what is kind of depressing about this. We have people who, first of all, care, who are experts. You come into government to try to make a difference, or you have been in government, and we seem to be going in a circle, trying to get off the merry-go-round, Mr. Scott, but still going in a circle.

I'm not blaming you all. It just seems that we have a set of circumstances where we have an old system that is breaking down, trying to keep that afloat, and at the same time trying to catch up with technology that is not changing by the week, but changing by the hour. That is a tough one.

Sometimes we can start talking politics, and we still don't get to where we have to go to. That's what I want to talk about for a moment here.

Mr. Scott, you have been in your job a little less than 2 years?

Mr. SCOTT. About 1.5 years, sir.

Mr. CUMMINGS. The chairman was very complimentary, gave you a lot of nice compliments, and they are deserved. You come from private industry, is that right?

Mr. SCOTT. That's correct.

Mr. CUMMINGS. Do you see, first of all, progress? You've been there 1.5 years. Do you see us moving in the right direction?

And this is the thing that bothers me, this wrestling with this issue of money. I don't want to sit here and wrongfully say that, if we had more money, we can do better, if that is wrong, if that is not accurate. But on the other hand, if we need the money, I don't want to act like we don't.

And then there's a second part of it. We may need the money, but then the question is whether or not we are using the funds that we have effectively and efficiently.

Can you address that for me? And then tell me how does the modernization act, because I understand it is like the best practices, it's an example of best practices from private industry, how that would remedy this.

I know I have said a lot.

Mr. SCOTT. Sure, I'd be happy to.

I would say, in answer to one of your questions, I do think we are making progress, just not fast enough and comprehensively enough. Almost every agency is trying to prioritize in some way or another, and address the most urgent issues. But what we see quite often is that it takes too long for them to put together the money to go do the replacement, or to try to harvest savings to put together in one place to go fix things.

I think there is a broader set of issues that ITMF tries to address.

Comprehensively, what it does is marries management, money, and a different mode of operation than the pattern that we have been in. The world of digitization, and our government is digitizing just like every other enterprise, digitization starts to tear down traditional boundaries of the org chart, and so on, and comes at what we do from a citizen-centric perspective.

Today, because of our boundaries and our funding models and the way we have architected IT, we require our citizens to decode our org chart in a way that, frankly, they don't want to do.

So this modernization fund relies on principles that we borrowed from the private sector. If you are in the private sector, you go to a capital committee, and you come in and you make a business case for why you want to do what you're going to do. And the capital committee evaluates your ability to do that. They look at the business case. They ensure the commitment, that the money is going to get paid back.

We think that that commitment of management, along with this different mode of operation that we are proposing, will start to help us along the path to a much more and needed modernization of our Federal Government.

I will note as well that if we continue to do the same thing we have been doing before, we are just making the situation worse. A good friend of mine once told me, if you are riding a dead horse, best dismount. I think it is time for us to dismount from this past practice and get onto a more modern method.

Mr. CUMMINGS. You don't have to tell us what your plans are, but if I were to guess, you probably will not be in this position but so much longer.

So the question becomes, what are you doing to try to put something in place so that, after you leave, there is at least the mechanism to take us where you just said we need to go? Because I can see somebody else coming in and saying, “You know what? Scott was a nice guy, but now he's gone, and now we're going to start all over,” and our problems are 10 times worse.

By the way, the reason I am asking is because the American people are just totally, totally frustrated with us.

Mr. SCOTT. Certainly.

Mr. CUMMINGS. They feel like we cannot get anything done, and I'm trying to figure out how we get something done that makes sense, solve the problems that we are talking about here, Mr. Mulvaney and all of us trying to figure out, how do we spend our money wisely and how do we get the American people what they deserve? That is a well-run system that keeps up with, as best we can, the changes in technology and, at the same time, serve them well?

Mr. SCOTT. Well, there are a couple things we're doing.

First of all, we're putting together a set of requirements that will require the agencies to identify modernization efforts in a much more comprehensive way, whether this fund comes through or not.

Secondly, we are revising the job descriptions for CIOs to make sure that, as we hire future CIOs, we get the right kind of talent in place.

Frankly, this is important work, and I think there are quite a number of people who, given the right point in their career, are perfectly willing to come and do public service and help fix this, if there is hope that they can make progress. Nobody wants to come in and say, "I just want to be saddled with the old dead horse way of doing things." So I think that is key to attracting talent and continuing to make progress on this.

Lastly, I will say I intend to be involved and influence one way or another even beyond this job. I think it is critically important that we do this. I think our relevance to citizens is going to depend on how good a job we do in this area.

The ITMF is my best guess about the fastest way to accelerate progress toward that goal. I'm happy to listen to any other alternatives.

What I do know is what won't work. Going around tin-cupping 7,000 different investments across the Federal Government is the slow way to nowhere, as far as I'm concerned.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

Chairman CHAFFETZ. Thank you. I now recognize myself.

Mr. Milholland, you have been a good witness to us a couple times. You provide a lot of candor. The question is, why did we have to subpoena you this time to attend?

Mr. MILHOLLAND. That was the decision of the Commissioner, and he wanted to testify himself. I understand the reasoning. He didn't speak to me about it, but in the past, he thinks that the political appointee should be the one to speak to the Congress, not careerists like me.

Chairman CHAFFETZ. Were you willing to testify without a subpoena?

Mr. MILHOLLAND. Yes, sir.

Chairman CHAFFETZ. This is something we are going to have to continue to discuss, because on the one hand, in another committee, the IRS Commissioner said he was too busy and didn't have time to prepare, couldn't show up to answer hard questions. Then we have a hearing here, where we have to dive deep into how the IT systems are working, and he is begging to come and, in fact, told our office that we have to issue a subpoena to have Mr. Milholland come here.

I think it puts a bad light on the IRS. I think it puts a bad light on you personally. But I did want to clarify and appreciate your candor in saying that was totally and wholly unnecessary. We did it. It's paperwork. I can do it unilaterally, but I shouldn't have to do it. Nobody else required a subpoena to be here.

Again, it is not a personal reflection on you, but I think it is a personal reflection on Mr. Koskinen and the ridiculous manner in which he tries to manage a 90,000-person organization.

The Congress of the United States of America and certainly the Oversight Committee, we can talk to anybody at any time. We can investigate anything anywhere and we can call anybody we want before this committee, not just the Senate-confirmed IRS Commissioner. It is arrogant. It is beyond belief. And it continues to thwart our activities here in Congress.

And I am not letting go of this. I do think he should be impeached. I do think he should get out of government. He should do the right thing for this country, and somebody else should be at the helm. He was hired by the President with the best of intentions, and the President made a personal commitment. He made a personal commitment that we are going to work together. We are going to do is hand-in-hand. And that is not happening. And this is another example here today.

Enough of that speech about that. I do want to talk about the Obamacare files that were mentioned before.

Mr. Powner, do you have a position on this? Have you looked at how, from the GAO perspective, how this is going? It is a massive undertaking, a great vulnerability.

Have you done anything in this regard? Do you have any perspective on this?

Mr. POWNER. I have colleagues who have looked at Obamacare implementation, as well as some of the IT issues, in particular, security around the systems with Obamacare. We have some outstanding recommendations on security.

I, personally, have not done that. I will say, though, I did testify in front of this committee when there was the initial failure with the rollout, and I will say I worked closely with Mr. Milholland, because at the time I was doing IRS work and I knew where they were at getting their systems ready for Obamacare, which was different than where HHS and some others were.

Chairman CHAFFETZ. So the housing of all this data and information, I guess as a follow-up, Mr. Milholland, at the IRS, and certainly Mr. Powner from the GAO, we would love to, and request, if we need to do this formally, we will do it formally, but we would appreciate a keen eye on this, just because of the vulnerability and sensitivity and the sheer number of people that will be involved and engaged in this.

Mr. POWNER. Okay.

Mr. MILHOLLAND. Yes, sir.

Chairman CHAFFETZ. I want to switch gears here to HHS, Health and Human Services.

This is your first time testifying, and I appreciate that. How long have you been working IT at HHS?

Ms. KILLORAN. About a year and a half.

Chairman CHAFFETZ. A year and a half, okay.

The committee made a request. I thought it was a fairly benign request, and it gives us a perspective. We asked to identify the top three mission-critical IT systems in need of modernization. That seems like a simple request. Every other agency and department we asked for it was willing to cooperate. The only one that wasn't was HHS.

You claim that it was classified information. It is not the Department of Defense. This is not the CIA. This is Health and Human Services. Why claim it's classified?

Ms. KILLORAN. It is around the sensitivity of the information that is stored in the systems. As folks have mentioned today, some of my colleagues, information, especially around personal health information, it is one of the increasing threat vectors across the organization and in the public overall. So we want to make sure that we are protecting the American public and the health information.

Chairman CHAFFETZ. But you understand that that information that we are asking for is not classified, correct?

Ms. KILLORAN. As an individual system, but there are concerns about what those systems are and the targets that would ——

Chairman CHAFFETZ. And you understand that the Oversight Committee can access classified information, correct?

Ms. KILLORAN. Yes. We were actually able to—we actually had members of the committee come over yesterday to our ——

Chairman CHAFFETZ. Why should the committee have to come to you? Why do we have to go to look at in camera?

Ms. KILLORAN. We are just concerned about what those systems are and putting ——

Chairman CHAFFETZ. Yes, well, here's what you need to understand. We are entrusted with nuclear secrets, CIA information, a lot of very sensitive information. You cannot as an agency start to make up new classifications and new rules saying, "Well, we're sensitive and we don't trust Congress." We shouldn't have to go to HHS to review this information in camera.

In fact, it gives us a real sense that you really don't know what you're doing over there.

Ms. KILLORAN. These are not classified systems. We actually transmitted the information to OMB that it requested as classified. These are not classified systems, and they do not have ——

Chairman CHAFFETZ. Correct. You used a classified system to transmit it, but then when we request it, why do we have to ratchet this up?

Again, Health and Human Services has already identified one of the three systems to GAO, and another system that the HHS told us about was shut down.

We are just asking for the top-level review of what are the three mission-critical systems. Then we finally get to see one, and then it is figured out that you had to come back to us and say, "No, it was really shut down."

Can you see where you have a flashing red light over there at HHS that nobody else has?

Ms. KILLORAN. Understood. Like I said, we are actually willing to provide that information.

Chairman CHAFFETZ. Okay, just to be clear, and again, you strike me as an exceptionally nice person. You are going to provide—the request that we made, by this committee, you are going to provide those to us, correct?

You have a staff person there. Feel free to talk to them, if you want to confer.

But I need to know if we are going to get this information or not.

Ms. KILLORAN. Yes. Yes, you will.

Chairman CHAFFETZ. Okay.

I have some other questions, but let me recognize another member, and I will come back on another round here.

Let's recognize Mr. Lynch of Massachusetts.

Mr. LYNCH. Thank you, Mr. Chairman.

I have to say, it is a bipartisan frustration sometimes, especially with these data breaches. Everybody is getting hacked. All the agencies are getting hacked. It seems like the hackers have better access to the information than the Oversight Committee does. That is the frustration here, that the information is going out the door, and then there is some stonewalling going on. When this committee asks for information, it is not forthcoming. So that is some of what you are hearing.

I want to go back to Mr. Scott. I know you have a set of guidelines, a guidance, I guess you would call it, to these agencies on how to prioritize their responses to some of these high-risk legacy systems.

Are any of the agencies on that right now? Have any of the agencies actually adopted that guidance and are implementing it?

Mr. SCOTT. Let me clarify the guidance that you are referring to. As a part of the Cyber National Action Plan, and the earlier Cyber Sprint, we asked agencies to look at their high-value assets, and then some corrective measures were taken immediately on the initial set of things.

There is a review going on now with a larger set of identified high-value assets. That is in progress right now.

Mr. LYNCH. Maybe you could drill down on that a little bit more. High value, is that the same as high risk? Because in the GAO report, it indicated there was a guidance to prioritize high-risk legacy systems. Now, that may not be high-value systems, but ones with greatest vulnerability, I guess.

Mr. SCOTT. Let me talk about our guidance, generally.

It is best practice to constantly be evaluating your systems for all kinds of different things. Risk would be one of the factors that you would look at there. Technology obsolescence would be another one. So that is, in fact, a part of our guidance.

Mr. LYNCH. Okay. It indicated in this report that the Department of Transportation and USDA had started acting in compliance with this. I thought you might have some information regarding that.

Mr. SCOTT. It is work in progress right now.

Mr. LYNCH. All right.

Mr. POWNER. If I could clarify that?

Mr. LYNCH. Please.

Mr. POWNER. So there was draft guidance, and we did our review. We think that guidance is really good. We would like to see OMB finalize that guidance and have agencies apply the guidance, so that we could have a prioritization of these things that need to be replaced, similar to the chairman's questions that he asked directly with this data call, and that we would like to see more action on the prioritization and what we are tackling to modernize.

I actually think that's needed to implement the modernization fund, if, in fact, that moved forward.

Mr. LYNCH. Yes, it makes sense, especially when you talk about the continuity problem that Mr. Cummings raised where, if Mr. Scott leaves at some point, we want the person coming in behind him to follow that same guidance and maintain those same priorities and get that job done, rather than somebody coming in with a whole new idea and taking us in a new direction.

So those are some of the problems we see coming down the pike.

But look, I appreciate your work, and I know you are all trying to do the right thing. We just need to do it faster.

Thank you. I yield back.

Chairman CHAFFETZ. I thank the gentleman. I will recognize myself again. I want to pick up on Health and Human Services.

Health and Human Services, unlike the DOD, which has had significant cuts in its budget by billions of dollars in annual expenditure, Health and Human Services has more than doubled—doubled—the funding for your operations in the IT sector, going from roughly $5.6 billion to more than $13 billion. So they are in a totally different mode here.

Your responsibility includes CMS. Is that right?

Ms. KILLORAN. That is correct.

Chairman CHAFFETZ. I want to talk about, for a second, Health and Human Services has to deal with Medicare appeals. And from the information I've read, the HHS Inspector General's Office reported that the Office of Medicare Hearings and Appeals, OMHA, is still largely paper-based. It is so bad that Medicare contractors were converting records from electronic to paper format to send to administrative law judges.

Can you give us the status of where this is at and what is being done to solve this?

Ms. KILLORAN. Thank you for the question.

Yes, that is the case, but they actually are in the process right now of establishing a system to do that automated process. And CMS is actually working with that organization, as that system comes online, of how to integrate the medical appeals system with the system that OMHA is working on right now.

Chairman CHAFFETZ. Health and Human Services entered into a $1.3 billion settlement with hospitals to clear the backlog on Medicare appeals. This lack of automation, did that contribute to this problem?

Ms. KILLORAN. That I would have to get back to you on, because, obviously, I need to get to program and get a full answer on what were the factors in that particular issue.

Chairman CHAFFETZ. So with a little bit more specificity, when do we expect the implementation of this plan that CMS—is there a CMS plan?

Ms. KILLORAN. So the system that you are specifically talking about is actually not in CMS. It is in the Office of Medicare Hearings and Appeals. And yes, they do have a plan. That process—that program is in development, and they are working toward an implementation within the next year.

Chairman CHAFFETZ. Are they building their own system or are they buying something or leasing something?

Ms. KILLORAN. It is a combination of some custom development and also commercial off-the-shelf.

Chairman CHAFFETZ. Has that been contracted out yet?

Ms. KILLORAN. Yes. Development is actually in plan. We are actually working with them to do security testing and are in the final stages of development.

Chairman CHAFFETZ. We will send a letter, but are you committed to providing us the details of that plan?

Ms. KILLORAN. Yes, sir.

Chairman CHAFFETZ. Thank you. That would be very helpful.

Let me go back to the Department of Defense here. The Department of Defense identified a system called the MOCAS, which stands for Mechanization of Contract Administration Services. It is an example of a mission-critical system scheduled for modernization. It had its 50th birthday in 2008, so it is a bit old. We congratulate on how robust it is.

But this contract management payment system for DOD is jointly managed by the Defense Contract Management Agency, the DCMA, and DFAS, the Defense Finance and Accounting System.

It was originally developed, as I said, back in the 1960s. It supports business processes for more than 350,000 DOD active contracts with roughly $1.6 trillion in contract obligations and entitlements valued at approximately $230 billion annually.

The DOD in 2014 released a request for information for ideas on how to modernize this. Can you give us a sense of where this monster is? And what is the plan is moving forward?

Mr. HALVORSEN. We definitely need to modernize the front end of that system. One of the reasons that we are delayed a little bit is, in looking at that, I wanted more input from the private sector. This is one where I do believe we could buy the front end of this.

The backend of the system is in pretty good shape. It is old, but it is in COBOL language. It supports it.

One of the things I do think that we want to recognize here is that the front end of systems, obviously, many times, we need to fix those. When you are interacting with customers, we've got that, and we have examples of that. Some of these backend systems I do think we want to make that investment the same way the private sector would, which is to do the business case to say, "Does it pay to change that?" In many cases right now, it will not pay to change the backend of some of the systems we have.

COBOL is not going away anytime soon. The predictions you look at, it is going to be around as our major business system for a while.

The front ends, make it look more consumer-friendly. Go with what the private sector is doing there. And that is what we will end up with here.

Chairman CHAFFETZ. When do you think you have a game plan in order to actually address this?

Mr. HALVORSEN. By the end of the summer.

Chairman CHAFFETZ. Okay.

One more question back for Health and Human Services.

Today, the committee issued a report about Cover Oregon. We looked at this for a year. The Federal Government, through HHS, gave the State of Oregon more than $300 million to develop a Web site. They never got a Web site. They never got any money back.

What is Health and Human Services doing about that?

Ms. KILLORAN. So that would be done through our grants programs, so we would actually have to talk to—I would have to get back to you with our grant system owners and make sure I provide you with the right answer of how they are doing oversight and giving the grants. It is outside of the purview that I have.

Chairman CHAFFETZ. So the money that is appropriated to Health and Human Services for IT, help me on how it is broken down. So you don't feel any obligation, you have no responsibility to oversee the grants that are given?

Ms. KILLORAN. There are two sets of funds. There is internal IT funding, which is $5 billion that we spend internally. That is where the oversight I have authority and responsibility over.

There is another over $7 billion that is given to our grants programs through that business mechanism. They are responsible through legislation for providing those grants out to States, locals, tribal, and education, universities, and other things for either access to our systems or to do research on our behalf. All of that funding is actually the responsibility of those individual programs to provide out and to provide oversight to.

Chairman CHAFFETZ. Okay, you can let Health and Human Services—they are about to get some inquiries from the Oversight Committee about what obligation they think they have or don't have when they give out a grant. Because in this case, $300-plus million went out the door, again, no Web site and no money back.

I think there was a lot of misrepresentation. I think there was fraud. I think there are potential criminal elements to this that we have referred now to the Office of Attorney General here in the United States and also the Attorney General, who we believe who should recuse herself there in Oregon, because the mix of political with the government, it was something that I believe was done fraudulently.

We issued about a 150-page report, and we will continue to follow up.

But I appreciate the clarification, because the grant system is the majority of that IT budget, and it does make you wonder. We are looking for $3 billion. There is $7 billion that is given to HHS that is just given away to other entities not even within the Federal Government.

So if we want to go capture and claw back and find $3 billion to make major changes—I really am warming up to this idea that Mr. Hoyer has presented, and Mr. Cummings and others.

And I do believe you and your perspective, Mr. Scott.

This may be the type of area where maybe we are going to have to trim those feathers back in order to do the right thing with the Federal dollars and the Federal obligations.

I will now recognize Mr. Cummings for 5 minutes.

Mr. CUMMINGS. Mr. Scott, I want to just follow up on a few things. I want to go back to this modernization act and how it works.

According to estimates by the administration, after an initial funding of the $3.1 billion, the fund would be self-sustaining and would address at least $12 billion in modernization projects over the next 10 years. Is that right?

Mr. SCOTT. That is correct.

Mr. CUMMINGS. Can you explain to us how the fund would be self-sustaining over that period of time?

Mr. SCOTT. Essentially, as projects get funded, and then either go live or—each project would have its own contracted repayment schedule. As those funds are paid back to the fund, they could then be reused for the next series of projects.

As was mentioned before, one of the criteria for funding a project would be its elimination of risk, its adoption of modern technology, and the business case that underlies it.

So we think there is a high likelihood, given the governance model we put in place, that the funds would both be repaid, but also be able to be reused.

Mr. CUMMINGS. So how would the funds support modernization projects that exceed the initial amount of funding?

Mr. SCOTT. The modernization fund could supplement what an agency has in its budget and accelerate plans. That is one example. We have seen cases where agencies are doing the right thing, but they have a project that will last 5 or 6 or 7 years, and they tell us they could do it in 2 or 3 years, save a ton of money, and start the savings actually that would come from modernization much sooner.

That is just one example of a business case.

Mr. CUMMINGS. As part of the proposal, the fund would be overseen by an independent review board, as I understand it, and that would provide technical assistance to agencies in connection with any upgrade projects the board approves. Is that the way it works?

Mr. SCOTT. That is our proposal.

Mr. CUMMINGS. Can you explain how that review board would work in overseeing the fund?

Mr. SCOTT. Sure. The idea behind the board is we wanted to take a more holistic look at the factors that make a project successful. So is the right governance in place? Is this the right technical architecture? Do we have the right procurement strategy in place? Do the economics make sense?

Some of those kinds of factors that, frankly, in the private sector are now just the norm and are sometimes missing from what we see.

But we also, and this is an important point, want to encourage cross-agency collaboration for shared services in some of these projects. Getting that to work across agencies is not a mechanism that works terribly well today.

Mr. CUMMINGS. So I take it one of the things that they would be doing, this board, is trying to make sure that folks use best practices. Is that right?

Mr. SCOTT. Correct.

Mr. CUMMINGS. And how would they accomplish that?

Mr. SCOTT. First, the sharing of best practices as we find them in the Federal Government is one of the key things, but we would also leverage expertise from the private sector and make sure that that was available to projects that are funded by the fund.

Mr. CUMMINGS. Now what are the cost savings the Federal Government would realize if this bill were adopted and implemented? I mean, I know you have to guess that.

Mr. SCOTT. Well, I think our common experience in the private sector is that if you get in a continuous refresh mode, you can either do one of two things. You can either can increase your capacity or you can lower costs, or something in between.

I think, in this case, we will see some of both. We have, certainly, agencies where there is more demand than we can satisfy today, and some of the savings could be used to address that demand. But we have many other cases, such as data center consolidation, where this activity would accelerate consolidation and accelerate savings, and that money could then be used for other purposes.

Mr. CUMMINGS. So I guess it would be safe to say that it would exceed the $3.1 billion.

Mr. SCOTT. I'm quite comfortable in that. You saw it in the chart that I showed earlier. We have direct evidence where injection of modernization funds leads to savings, and the question is just, do we want to accelerate that?

Mr. CUMMINGS. My last question, folks in Washington—that is us, Members—get concerned about risk. What are the arguments against doing something like this?

Mr. SCOTT. Well, I think the risk that we all see is that we have an accelerating amount of risk. The longer we don't address these ——

Mr. CUMMINGS. That is the greater risk.

Mr. SCOTT. That is the greater risk. I am quite concerned about it, in total.

In particular, it is not just applications. We also have to address the infrastructure, the networks and the storage and all of the other components, not just the applications. We have to address this holistically.

Mr. CUMMINGS. I want to thank all of you very much.

Mr. Chairman, I yield back.

Chairman CHAFFETZ. Thank you. I would just like to allow you each 30 or 45 seconds, you can go shorter or a little bit longer, if you want. What are the things the Congress, what would you like to see us do in order to make sure we are moving in the right direction?

Let's start with Mr. Scott and go this direction.

Mr. Powner, you take a lot longer, if you like.

Mr. SCOTT. Sure. I'll be quick, because I think I have said most of what I had to say earlier.

But I appreciate the support this committee has shown for this important topic. And in formulating the idea for the modernization fund, we looked at a number of different alternatives. Our team at OMB asked a bunch of hard questions about how else could we do this, what would be the best way, what is faster rather than slower, what is more effective? We borrowed heavily from private sector best practice, in terms of formulating this.

While we are open to any alternative that makes sense, it is our recommendation at this point that this is the best we can think of, in terms of how to go forward.

So I appreciate all the support that we felt in a bipartisan way on this topic. Thank you.

Chairman CHAFFETZ. Thank you.

Ms. KILLORAN. So HHS also agrees that what OMB is putting forward on the ITMF is the right move. Being able to invest in our technology and making sure that we are using technology that is current, that is scalable, and meets not only the needs of today, but is scalable for the needs of the future, is the right direction for us to go into.

We have been able to make small incremental changes with the funding that we have, and we have actually seen those successes. So we are a good case study on what positively can happen in this type of situation, and we would be willing, obviously, to share that not only with the members of this committee, but also with OMB as we move forward and work to adopt this model.

Thank you.

Chairman CHAFFETZ. Thank you.

Mr. Halvorsen?

Mr. HALVORSEN. I thank the committee. This committee has taken this problem seriously, and I do appreciate that. And I think you've understood the complexity of the problem, which is very helpful, in itself.

The other area that this committee has been helpful with, and I hope that will continue, is giving us some flexibility on how we hire the cyber and IT work force.

Thank you.

Chairman CHAFFETZ. Thank you. I happen to agree. I think the personnel issue is probably as big as anything. Attracting the talent, retaining the talent, I mean, it's—I have a new son-in-law, a couple weeks old, this son-in-law. But he just graduated and that kid is more employable than I am, so I agree.

[Laughter.]

Mr. Milholland, you are now recognized.

Mr. MILHOLLAND. Thank you for asking that question. I think there are two things. I put it in my written statement and in my opening remarks.

It comes down to, from an IT point of view, certainty in our budget, at least restore us back to the levels we were at a number of years ago. It has really handicapped our ability to modernize our legacy environments and our aging infrastructure and provide the services that taxpayers need.

The second thing deals with the people issue you just mentioned, and it is the streamlined critical pay authority. We have nine IT folk who a year from now will disappear. They are absolutely critical to the architecture work we are doing for legacy system modernization, the engineering, the implementation and operations. And they said that they would serve their country, but right now, if the law is not renewed, they will literally leave and increase the risk on the IT organization to serve the taxpayers of this country.

So thank you.

Chairman CHAFFETZ. Again, not your fault, not your issue, the senior leadership, the Commissioner himself, is the number one impediment to moving those things forward. Nobody believes him. Nobody trusts them. He is not trustworthy.

I think that problem will continue to linger as long as he is the Commissioner. If he changes out, I think the world will change.

Mr. Powner, you are now recognized.

Mr. POWNER. Mr. Chairman, I would like to thank you for highlighting this legacy IT issue. We talked a lot today also about transition. There is a lot of talent sitting here to the left of me. And I would like to highlight the importance of FITARA and your efforts in ensuring that we continue to implement that law.

The first part of FITARA is about strengthening CIO authorities. We need more CIOs like some of the folks sitting here. But FITARA is also about understanding what we spend on IT and then executing it.

Legacy IT management is executing, so it is all part of FITARA.

So your grades looking at areas you looked at to date have made a lot of progress to date, and we need to continue to make progress through this transition period that we are in.

Chairman CHAFFETZ. Thank you. It is important, and again, particularly to the agencies that are represented, and those that aren't, it really is the FITARA model, I think, is a way for us to gain perspective and set reasonable goals and do self-analysis and be candid in where we're at.

Again, I want to thank you all personally for your commitment to our country. It's a difficult thing. If this was easy, it would have been done a long time ago.

Making these transitions away from legacy systems, that is a major, major overhaul and very difficult project, to say the least.

So I appreciate your expertise and working with this committee and your presence here today.

The committee stands adjourned.

[Whereupon, at 11:12 a.m., the committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Major Information Technology Acquisition Failures Per GAO

In the 2015 High Risk Report, GAO identified the following as examples of failed IT investments:

- The Department of Defense's (DOD) Expeditionary Combat Support System, which was canceled in December 2012, after spending more than a billion dollars and failing to deploy within 5 years of initially obligating funds. *Major Automated Information Systems: Selected Defense Programs Need to Implement Key Acquisition Practices*, GAO-13-311 (Mar. 2013), Appendix II, Profiles of Selected DOD MAIS Programs, at 62-63.
- The Department of Homeland Security's Secure Border Initiative Network program, which was ended in January 2011, after obligating more than $1 billion to the program, because it did not meet cost-effectiveness and viability standards. *Secure Border Initiative: DHS Needs to Strengthen Management and Oversight of Its Prime Contractor*, GAO-11-6 (Oct. 2010) at 3-4, 6.
- The Department of Veterans Affairs (VA) Financial and Logistics Integrated Technology Enterprise Program, which was intended to be delivered by 2014 at a total estimated cost of $609 million, but was terminated in October 2011 due to challenges in managing the program. This program was the successor to an earlier program that also failed after spending $249 million. *Information Technology: Actions Needed to Fully Establish Program Management Capability for VA's Financial and Logistics Initiative*, GAO-10-40 (Oct. 2009) at 2-13.
- The Office of Personnel Management's Retirement Systems Modernization program, which was cancelled in February 2011, after spending approximately $231 million on the agency's third attempt to automate the processing of federal employee retirement claims. *Federal Retirement Processing: OPM Is Pursuing Incremental Information Technology Improvements after Canceling a Modernization Plagued by Management Weaknesses*, GAO-13-580T (May 2013) at 5-11.
- The National Oceanic and Atmospheric Administration, Department of Defense, and the National Aeronautics and Space Administration's National Polar-orbiting Operational Environmental Satellite System, which was a tri-agency weather satellite program that was terminated in February 2010 after having spent 16 years and almost $5 billion on the program, which a presidential task force decided to disband. *Polar-Orbiting Environmental Satellites: Agencies Must Act Quickly to Address Risks that Jeopardize the Continuity of Weather and Climate Data*, GAO-10-558 (May 2010) at 6-15.
- The VA Scheduling Replacement Project, which was terminated in September 2009 after spending an estimated $127 million over 9 years. *Information Technology: Management Improvements are Essential to VA's Second Effort to Replace its Outpatient Scheduling System*, GAO-10-579 (May 2010) at 4-9.

GAO

United States Government Accountability Office

Report to Congressional Requesters

May 2016

INFORMATION TECHNOLOGY

Federal Agencies Need to Address Aging Legacy Systems

GAO-16-468

GAO Highlights

Highlights of GAO-16-468, a report to congressional requesters

Why GAO Did This Study

The federal government invests more than $80 billion on IT annually, with much of this amount reportedly spent on operating and maintaining existing (legacy) IT systems. Given the magnitude of these investments, it is important that agencies effectively manage their O&M.

GAO's objectives were to (1) assess federal agencies' IT O&M spending, (2) evaluate the oversight of at-risk legacy investments, and (3) assess the age and obsolescence of federal IT.

To do so, GAO reviewed OMB and 26 agencies' IT O&M spending for fiscal years 2010 through 2017. GAO further reviewed the 12 agencies that reported the highest planned IT spending for fiscal year 2015 to provide specifics on agency spending and individual investments.

What GAO Recommends

GAO is making 16 recommendations, one of which is for OMB to develop a goal for its spending measure and finalize draft guidance to identify and prioritize legacy IT needing to be modernized or replaced. GAO is also recommending that selected agencies address at-risk and obsolete legacy O&M investments. Nine agencies agreed with GAO's recommendations, two agencies partially agreed, and two agencies stated they had no comment. The two agencies that partially agreed, Defense and Energy, outlined plans that were consistent with the intent of our recommendations.

View GAO-16-468. For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

May 2016

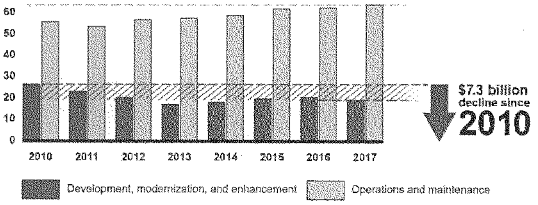
INFORMATION TECHNOLOGY

Federal Agencies Need to Address Aging Legacy Systems

What GAO Found

The federal government spent about 75 percent of the total amount budgeted for information technology (IT) for fiscal year 2015 on operations and maintenance (O&M) investments. Such spending has increased over the past 7 fiscal years, which has resulted in a $7.3 billion decline from fiscal years 2010 to 2017 in development, modernization, and enhancement activities.

Total Federal IT Spending by Type (in billions)

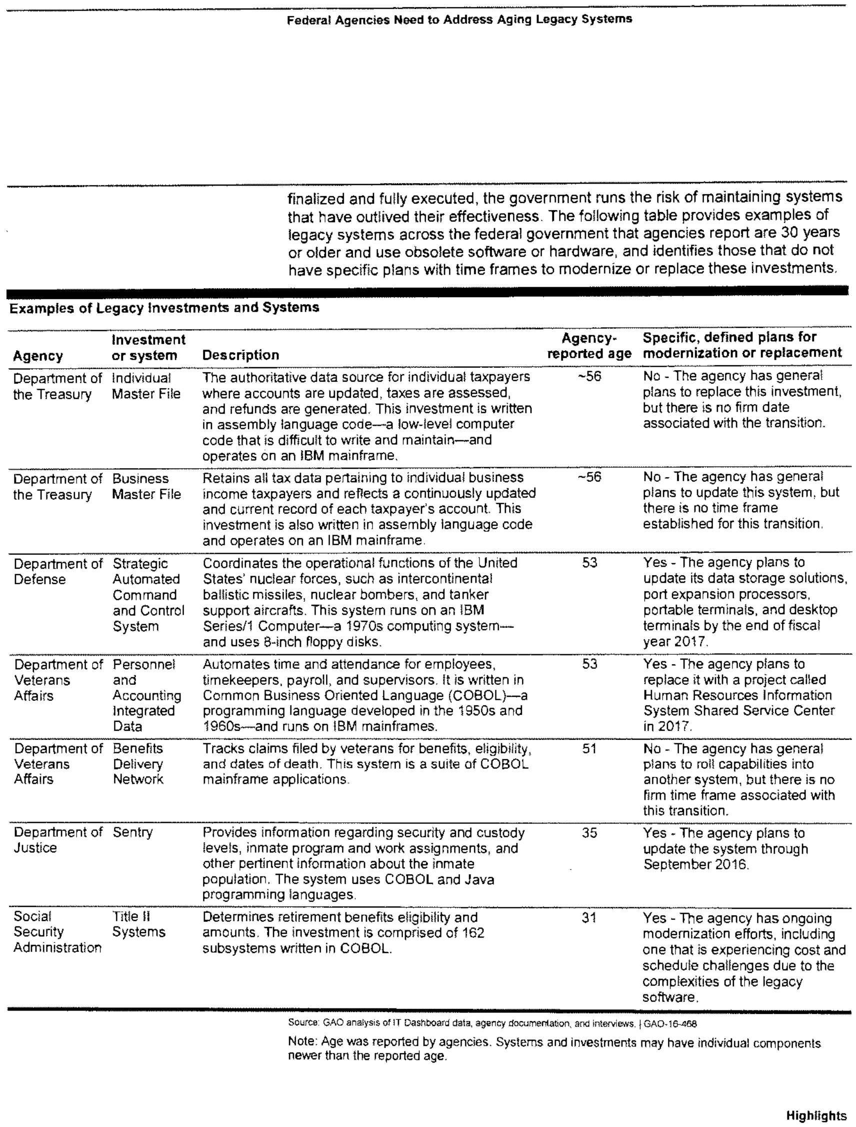


Source: GAO analysis of agency data. | GAO-16-468

Specifically, 5,233 of the government's approximately 7,000 IT investments are spending all of their funds on O&M activities. Moreover, the Office of Management and Budget (OMB) has directed agencies to identify IT O&M expenditures known as non-provisioned services that do not use solutions often viewed as more efficient, such as cloud computing and shared services. Agencies reported planned spending of nearly $55 billion on such non-provisioned IT in fiscal year 2015. OMB has developed a metric for agencies to measure their spending on services such as cloud computing and shared services, but has not identified an associated goal. Thus, agencies may be limited in their ability to evaluate progress.

Many O&M investments in GAO's review were identified as moderate to high risk by agency CIOs, and agencies did not consistently perform required analysis of these at-risk investments. Further, several of the at-risk investments did not have plans to be retired or modernized. Until agencies fully review their at-risk investments, the government's oversight of such investments will be limited and its spending could be wasteful.

Federal legacy IT investments are becoming increasingly obsolete: many use outdated software languages and hardware parts that are unsupported. Agencies reported using several systems that have components that are, in some cases, at least 50 years old. For example, Department of Defense uses 8-inch floppy disks in a legacy system that coordinates the operational functions of the nation's nuclear forces. In addition, Department of the Treasury uses assembly language code—a computer language initially used in the 1950s and typically tied to the hardware for which it was developed. OMB recently began an initiative to modernize, retire, and replace the federal government's legacy IT systems. As part of this, OMB drafted guidance requiring agencies to identify, prioritize, and plan to modernize legacy systems. However, until this policy is



Federal Agencies Need to Address Aging Legacy Systems

finalized and fully executed, the government runs the risk of maintaining systems that have outlived their effectiveness. The following table provides examples of legacy systems across the federal government that agencies report are 30 years or older and use obsolete software or hardware, and identifies those that do not have specific plans with time frames to modernize or replace these investments.

Examples of Legacy Investments and Systems

Agency	Investment or system	Description	Agency-reported age	Specific, defined plans for modernization or replacement
Department of the Treasury	Individual Master File	The authoritative data source for individual taxpayers where accounts are updated, taxes are assessed, and refunds are generated. This investment is written in assembly language code—a low-level computer code that is difficult to write and maintain—and operates on an IBM mainframe.	~56	No - The agency has general plans to replace this investment, but there is no firm date associated with the transition.
Department of the Treasury	Business Master File	Retains all tax data pertaining to individual business income taxpayers and reflects a continuously updated and current record of each taxpayer's account. This investment is also written in assembly language code and operates on an IBM mainframe.	~56	No - The agency has general plans to update this system, but there is no time frame established for this transition.
Department of Defense	Strategic Automated Command and Control System	Coordinates the operational functions of the United States' nuclear forces, such as intercontinental ballistic missiles, nuclear bombers, and tanker support aircrafts. This system runs on an IBM Series/1 Computer—a 1970s computing system—and uses 8-inch floppy disks.	53	Yes - The agency plans to update its data storage solutions, port expansion processors, portable terminals, and desktop terminals by the end of fiscal year 2017.
Department of Veterans Affairs	Personnel and Accounting Integrated Data	Automates time and attendance for employees, timekeepers, payroll, and supervisors. It is written in Common Business Oriented Language (COBOL)—a programming language developed in the 1950s and 1960s—and runs on IBM mainframes.	53	Yes - The agency plans to replace it with a project called Human Resources Information System Shared Service Center in 2017.
Department of Veterans Affairs	Benefits Delivery Network	Tracks claims filed by veterans for benefits, eligibility, and dates of death. This system is a suite of COBOL mainframe applications.	51	No - The agency has general plans to roll capabilities into another system, but there is no firm time frame associated with this transition.
Department of Justice	Sentry	Provides information regarding security and custody levels, inmate program and work assignments, and other pertinent information about the inmate population. The system uses COBOL and Java programming languages.	35	Yes - The agency plans to update the system through September 2016.
Social Security Administration	Title II Systems	Determines retirement benefits eligibility and amounts. The investment is comprised of 162 subsystems written in COBOL.	31	Yes - The agency has ongoing modernization efforts, including one that is experiencing cost and schedule challenges due to the complexities of the legacy software.

Source: GAO analysis of IT Dashboard data, agency documentation, and interviews. | GAO-16-468

Note: Age was reported by agencies. Systems and investments may have individual components newer than the reported age.

Highlights

Contents

Tables

Figures

Abbreviations

CADE 2	Customer Account Data Engine 2
CAS	Core Accounting System
CIO	Chief Information Officer
COBOL	Common Business Oriented Language
Commerce	Department of Commerce
DHS	Department of Homeland Security
DME	development, modernization, and enhancement
DNDO	Domestic Nuclear Detection Office
Defense	Department of Defense
DOT	Department of Transportation
DVIS	Diversity Visa Information System
Energy	Department of Energy
HHS	Department of Health and Human Services
IMF	Individual Master File
IRS	Internal Revenue Service
IT	information technology
Justice	Department of Justice
NWSTG	National Weather Service Telecommunication Gateway
O&M	operations and maintenance
OMB	Office of Management and Budget
PAID	Personnel and Accounting Integrated Data
ROSS	Resource Ordering and Status System
SSA	Social Security Administration
State	Department of State
Treasury	Department of the Treasury
TSA	Transportation Security Administration
USCG	U.S. Coast Guard
USDA	U.S. Department of Agriculture
VA	Department of Veterans Affairs

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 25, 2016

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Jason Chaffetz
Chairman
Committee on Oversight and Government Reform
House of Representatives

The federal government spends more than $80 billion annually on information technology (IT), with about 75 percent reportedly spent on operating and maintaining existing (legacy) IT systems. Given the size and magnitude of these investments, it is important that agencies effectively manage the operations and maintenance (O&M) of existing investments.

Our objectives were to (1) assess federal agencies' IT O&M spending, (2) evaluate the oversight of at-risk legacy investments, and (3) assess the age and obsolescence of federal IT.

Our review of O&M spending included the Office of Management and Budget (OMB) and the 26 agencies that report to OMB's IT Dashboard.[1] For specific information on individual systems or investments, we focused on the 12 agencies that reported the highest planned IT spending for

[1] In June 2009, OMB established the IT Dashboard, a public website that provides detailed information on major IT investments at 26 federal agencies. The 26 agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; U.S. Army Corps of Engineers, Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Archives and Records Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

fiscal year 2015, given that these agencies make up over 90 percent of reported federal IT spending.[2]

To assess federal agencies' IT O&M spending, we reviewed data reported to OMB as part of the budget process for fiscal years 2010 through 2017. We analyzed that data to determine whether spending had changed over those years and compared OMB's associated performance measure to federal best practices.[3]

We evaluated the extent to which the 12 selected federal agencies are performing oversight on their existing legacy investments by reviewing agency IT Dashboard data to identify investments in O&M that had been identified as being moderate to high risk. We also reviewed agency documentation such as TechStat documentation and operational analyses, as available.

To assess the age and obsolescence of federal IT, we reviewed agency documentation, such as operational analyses and enterprise architecture documents, and interviewed agency officials on issues related to legacy investments. We also requested that the 12 agencies provide a list of their three oldest systems. In some cases, agencies reported that they do not track the ages of individual systems. In those cases, we requested that the agency provide their three oldest IT investments. We also compared OMB and agencies' current practices with federal guidance, such as OMB's Circular No. A-11: *Preparation, Submission, and Execution of the Budget* and its associated supplement on capital assets, to determine whether OMB and agencies are adequately managing the age and obsolescence of federal IT. In addition, we profiled selected systems and investments. To select those, we selected a system or investment that was identified as one of the agency's oldest or had been identified as being at-risk. In particular, we selected one system or investment per agency using factors such as investment type (major or

[2] These agencies are the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Homeland Security, Justice, State, Transportation, the Treasury, Veterans Affairs, and the Social Security Administration.

[3] Department of the Navy, Office of the Chief Information Officer, *Guide for Developing and Using Information Technology (IT) Performance Measurements* (Washington, D.C.: October 2001); and General Services Administration, Office of Governmentwide Policy, *Performance-Based Management: Eight Steps To Develop and Use Information Technology Performance Measures Effectively* (Washington, D.C.: 1996).

non-major), system or investment age, and risk level. We reviewed agency documentation and interviewed agency officials on the profiled systems or investments.

To assess the reliability of the OMB budget data and IT Dashboard data, we reviewed related documentation, such as OMB guidance on budget preparation, capital planning, and IT Dashboard submissions. In addition, we corroborated with each agency that the data downloaded were accurate and reflected the data it had reported to OMB. We determined that the data were reliable for the purposes of our reporting objectives. Details of our objectives, scope, and methodology are contained in appendix I.

We conducted this performance audit from April 2015 to May 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Over the last three decades, Congress has enacted several laws to assist agencies and the federal government in managing IT investments. For example, to assist agencies in managing their investments, Congress enacted the Clinger-Cohen Act of 1996.[4] This act requires OMB to establish processes to analyze, track, and evaluate the risks and results of major capital investments in information systems made by federal agencies and report to Congress on the net program performance benefits achieved as a result of these investments. Most recently, in December 2014, Congress enacted IT acquisition reform legislation (commonly referred to as the Federal Information Technology Acquisition Reform Act or FITARA)[5] that, among other things, requires OMB to develop standardized performance metrics, including cost savings, and to submit quarterly reports to Congress on cost savings.

[4] 40 U.S.C. § 11101, et. seq.

[5] Pub. L. No. 113-291, div. A, title VIII, subtitle D ,128 Stat. 3292, 3438-50 (Dec. 19, 2014).

In carrying out its responsibilities, OMB uses several data collection mechanisms to oversee federal IT spending during the annual budget formulation process. Specifically, OMB requires federal departments and agencies to provide information related to their Major IT Business Cases (previously known as exhibit 300) and IT Portfolio Summary (previously known as exhibit 53).[6]

- **Major IT Business Case.** The purpose of this requirement is to provide a business case for each major IT investment and to allow OMB to monitor IT investments once they are funded. Agencies are required to provide information on each major[7] investment's cost, schedule, and performance.
- **IT Portfolio Summary.** The purpose of the IT portfolio summary is to identify all IT investments—both major and non-major —and their associated costs within a federal organization. This information is designed, in part, to help OMB better understand what agencies are spending on IT investments.

OMB directs agencies to break down IT investment costs into two categories: (1) O&M and (2) development, modernization, and enhancement (DME). O&M (also known as steady state) costs refer to the expenses required to operate and maintain an IT asset in a production environment. DME costs refers to those projects and activities that lead to new IT assets/systems, or change or modify existing IT assets to substantively improve capability or performance.

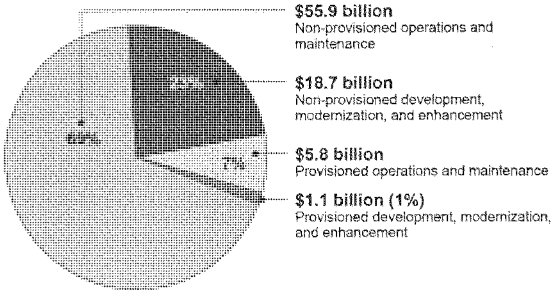
Beginning in 2014, OMB directed agencies to further break down their O&M and DME costs to identify provisioned IT service costs. A provisioned IT service is one that is (1) owned, operated, and provided by an outside vendor or external government organization and (2) consumed by the agency on an as-needed basis. Examples of provisioned IT service could include cloud services or shared services from another federal

[6] OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget* (June 30, 2015).

[7] According to OMB guidance, a major IT investment requires special management attention because of its importance to the mission or function to the government; significant program or policy implications; high executive visibility; high development, operating, or maintenance costs; unusual funding mechanism; or definition as major by the agency's capital planning and investment control process.

agency or a private service provider. About 8.5 percent of federal agencies' planned spending for fiscal year 2016 has gone toward provisioned IT services, leaving the vast majority of spending going toward IT that is non-provisioned. Figure 1 shows the breakdown in planned spending for fiscal year 2016.

Figure 1: Planned Funding of IT Investments for Fiscal Year 2016, in billions



Source: GAO analysis of Office of Management and Budget's Information Technology Dashboard | GAO-16-468

Further, OMB has developed guidance that calls for agencies to develop an operational analysis policy for examining the ongoing performance of existing legacy IT investments to measure, among other things, whether the investment is continuing to meet business and customer needs.[8] This guidance calls for the policy to provide for an annual operational analysis of each investment that addresses cost, schedule, customer satisfaction, strategic and business results, financial goals, and innovation.

Nevertheless, federal IT investments have too frequently failed or incurred cost overruns and schedule slippages while contributing little to

[8] OMB, *Preparation, Submission, and Execution of the Budget*, Circular No. A-11 (June 30, 2015); OMB Memorandum M-10-27 (June 2010), requires agencies to establish a policy for performing operational analyses on steady state investments as a part of managing and monitoring investment baselines. Parts of this guidance do not apply to the Department of Defense.

mission-related outcomes. The federal government has spent billions of dollars on failed and poorly performing IT investments which often suffered from ineffective management, such as project planning, requirements definition, and program oversight and governance.[9]

Accordingly, in February 2015, we introduced a new government-wide high-risk area, *Improving the Management of IT Acquisitions and Operations*.[10] This area highlights several critical IT initiatives underway, including reviews of troubled projects, an emphasis on incremental development, a key transparency website, data center consolidation, and the O&M of legacy systems.

To make progress in this area, we identified actions that OMB and the agencies need to take. These include implementing the recently-enacted statutory requirements promoting IT acquisition reform, as well as implementing our previous recommendations. In the last 6 years, we made approximately 800 recommendations to OMB and multiple agencies to improve effective and efficient investment in IT. As of October 2015, about 32 percent of these recommendations had been implemented.

OMB's Recent Major Initiatives for Overseeing IT Investments

OMB has implemented a series of initiatives to improve the oversight of underperforming investments and more effectively manage IT. These efforts include the following:

- **IT Dashboard.** In June 2009, to further improve the transparency into and oversight of agencies' IT investments, OMB publicly deployed the IT Dashboard. As part of this effort, OMB issued guidance directing federal agencies to report, via the Dashboard, the performance of their IT investments. Currently, the Dashboard publicly displays information on the cost, schedule, and performance of over 700 major federal IT investments at 26 federal agencies. Further, the public display of these data is intended to allow OMB, other oversight bodies, and the general public to hold the government agencies

[9] GAO, *Information Technology: OMB and Agencies Need to More Effectively Implement Major Initiatives to Save Billions of Dollars*, GAO-13-796T (Washington, D.C.: July 25, 2013).

[10] GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

accountable for results and progress. Among other things, agencies are to submit ratings from their Chief Information Officers (CIO), which, according to OMB's instructions, should reflect the level of risk facing an investment relative to that investment's ability to accomplish its goals. To do so, each agency CIO is to assess his or her IT investments against a set of six pre-established evaluation factors identified by OMB and then assign a rating of 1 (high risk and red) to 5 (low risk and green) based on the CIO's best judgement of the level of risk facing the investment. Over the past several years, we have made over 20 recommendations to help improve the accuracy and reliability of the information on the IT Dashboard and to increase its availability.[11] Most agencies agreed with our recommendations or had no comment.

- **TechStat reviews.** In January 2010, the Federal CIO began leading TechStat sessions—face-to-face meetings to terminate or turn around IT investments that are failing or are not producing results. These meetings involve OMB and agency leadership and are intended to increase accountability and improve performance. OMB also empowered agency CIOs to begin to hold their own TechStat sessions within their respective agencies by June 2012. In June 2013, we reported that OMB and selected agencies held multiple TechStats, but additional OMB oversight was needed to ensure that these meetings were having the appropriate impact on underperforming projects and that resulting cost savings were valid.[12] Among other things, we recommended that OMB require agencies to address high-risk investments. OMB generally agreed with this recommendation. However, as of October 28, 2015, OMB had only conducted one TechStat review in the prior 2 years and OMB had not listed any

[11] GAO, *IT Dashboard: Agencies Are Managing Investment Risk, but Related Ratings Need to Be More Accurate and Available,* GAO-14-64 (Washington, D.C.: Dec. 12, 2013); *Information Technology Dashboard: Opportunities Exist to Improve Transparency and Oversight of Investment Risk at Select Agencies,* GAO-13-98 (Washington, D.C.: Oct. 16, 2012); *IT Dashboard: Accuracy Has Improved, and Additional Efforts Are Under Way to Better Inform Decision Making,* GAO-12-210 (Washington, D.C.: Nov. 7, 2011); *Information Technology: OMB Has Made Improvements to Its Dashboard, but Further Work Is Needed by Agencies and OMB to Ensure Data Accuracy,* GAO-11-262 (Washington, D.C.: Mar. 15, 2011); and *Information Technology: OMB's Dashboard Has Increased Transparency and Oversight, but Improvements Needed,* GAO-10-701 (Washington, D.C.: July 16, 2010).

[12] GAO, *Information Technology: Additional Executive Review Sessions Needed to Address Troubled Projects,* GAO-13-524 (Washington, D.C: June 13, 2013).

savings from TechStats in its quarterly reporting to Congress since June 2012.

- **Cloud computing strategy.** In order to accelerate the adoption of cloud computing solutions across the government, OMB's 25-Point IT Reform Plan included a "Cloud First" policy that required each agency CIO to, among other things, implement cloud-based solutions whenever a secure, reliable, and cost-effective cloud option exists.[13] Building on this requirement, in February 2011, OMB issued the Federal Cloud Computing Strategy, which provided definitions of cloud computing services; benefits of cloud services, such as accelerating data center consolidations; case studies to support agencies' migration to cloud computing; and roles and responsibilities for federal agencies.[14] In April 2016, we reported,[15] among other things, that we had identified 10 key practices that if included in cloud service agreements can help agencies ensure services are performed effectively, efficiently, and securely. OMB's guidance, released in February 2012, included most of the key practices, and we recommended that OMB include all 10 key practices in future guidance.

- **PortfolioStat reviews.** To better manage existing IT systems, OMB launched the PortfolioStat initiative in March 2012, which requires agencies to conduct an annual, agency-wide IT portfolio review to, among other things, reduce commodity IT[16] spending and demonstrate how their IT investments align with the agency's mission and business functions. In 2013 and 2015 we reported[17] that agencies

[13] OMB, *25-Point Implementation Plan to Reform Federal Information Technology Management* (Washington, D.C.: Dec. 9, 2010).

[14] OMB, *Federal Cloud Computing Strategy* (Washington, D.C.: Feb. 8, 2011).

[15] GAO, *Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance*, GAO-16-325 (Washington, D.C.: Apr. 7, 2016).

[16] According to OMB, commodity IT includes services such as IT infrastructure (data centers, networks, desktop computers and mobile devices); enterprise IT systems (e-mail, collaboration tools, identity and access management, security, and web infrastructure); and business systems (finance, human resources, and other administrative functions).

[17] GAO, *Information Technology: Additional OMB and Agency Actions Are Needed to Achieve Portfolio Savings*, GAO-14-65 (Washington, D.C.: Nov. 6, 2013); and *Information Technology: Additional OMB and Agency Actions Needed to Ensure Portfolio Savings Are Realized and Effectively Tracked*, GAO-15-296 (Washington, D.C.: Apr. 16, 2015).

had the potential to save at least $3.8 billion through this initiative. However, we noted that weaknesses existed in agencies' implementation of the initiative; therefore, we made more than 60 recommendations to OMB and agencies. OMB partially agreed with our recommendations, and responses from 21 of the agencies varied, with some agreeing and others not.

- **IT Shared Services Strategy.** In May 2012, OMB released its Federal IT Shared Services Strategy.[18] The strategy requires agencies to use shared services—IT functions that are provided for consumption by multiple organizations within or between federal agencies—for IT service delivery in order to increase return on investment, eliminate waste and duplication, and improve the effectiveness of IT solutions. Examples of commodity IT areas to consider migrating to a shared environment, as described in the strategy, include software licenses, e-mail systems, and human resource systems.

GAO Has Reported on the Need to Improve Oversight of Legacy IT

We have previously reported on legacy IT and the need for the federal government to improve its oversight of such investments. For example, in October 2012,[19] we reported on agencies' operational analyses policies and practices. As previously mentioned, operational analysis is a key performance evaluation and oversight mechanism required by OMB to ensure O&M investments continue to meet agency needs. In particular, we reported that although OMB guidance called for agencies to develop an operational analysis policy and perform such analyses annually, the extent to which the selected five federal agencies we reviewed carried out these tasks varied significantly. Specifically, the Departments of Homeland Security (DHS) and Health and Human Services (HHS) developed policies and conducted analyses, but excluded key investments and assessment factors. The Departments of Defense (Defense), the Treasury (Treasury), and Veterans Affairs (VA) had not developed a policy or conducted operational analyses. As such, we recommended that the agencies develop operational analysis policies,

[18] OMB, *Federal Information Technology Shared Services Strategy* (Washington, D.C.: May 2, 2012).

[19] GAO, *Information Technology: Agencies Need to Strengthen Oversight of Billions of Dollars in Operations and Maintenance Investments,* GAO-13-87 (Washington, D.C.: Oct. 16, 2012).

annually perform operational analyses on all investments, and ensure the assessments include all key factors. Further, we recommended that OMB revise its guidance to include directing agencies to post the results of such analyses on the IT Dashboard. OMB and the five selected agencies agreed with our recommendations and have efforts planned and underway to address them. In particular, OMB issued guidance in August 2012 directing agencies to report operational analysis results along with their fiscal year 2014 budget submission documentation (e.g., exhibit 300) to OMB. Thus far, operational analyses have not yet been posted on the IT Dashboard.

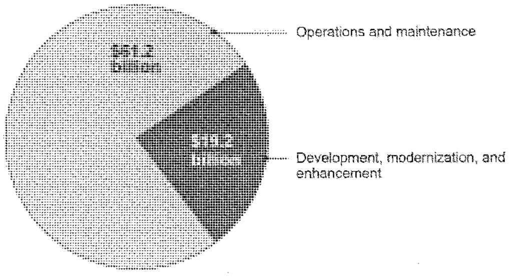
We further reported in November 2013 that agencies were not conducting proper analyses. Specifically, we reported[20] on IT O&M investments and the use of operational analyses at selected agencies and determined that of the top 10 investments with the largest spending in O&M, only the DHS investment underwent an operational analysis. DHS's analysis addressed most, but not all, of the factors that OMB called for (e.g., comparing current cost and schedule against original estimates). DHS officials attributed this to the department still being in the process of implementing its new operational analysis policy. The remaining agencies did not assess their investments, which accounted for $7.4 billion in reported O&M spending. Agency officials cited several reasons for not doing so, including relying on budget submission and related management reviews that measure performance; however, OMB has noted that these are not a substitute for an operational analysis. Consequently, we recommended that seven agencies perform operational analyses on their IT O&M investments and that DHS ensure that its analysis was complete and addressed all OMB factors. Three of the agencies agreed with our recommendations; two partially agreed; and two agencies had no comments.

[20] GAO, *Information Technology: Agencies Need to Strengthen Oversight of Multibillion Dollar Investments in Operations and Maintenance*, GAO-14-66 (Washington, D.C.: Nov. 6, 2013).

Government-wide Spending on IT Operations and Maintenance Is Increasing

Federal agencies reported spending the majority of their fiscal year 2015 IT funds on operating and maintaining a large number of legacy (i.e., steady-state) investments. Of the more than $80 billion reportedly spent on federal IT in fiscal year 2015, 26 federal agencies[21] spent about $61 billion on O&M, more than three-quarters of the total amount spent. Specifically, data from the IT Dashboard shows that, in 2015, 5,233 of the government's nearly 7,000 investments were spending all of their funds on O&M activities. This is a little more than three times the amount spent on DME activities (See figure 2).

Figure 2: Fiscal Year 2015 Federal Spending on IT Operations and Maintenance and Development, Modernization, and Enhancement



Source: GAO analysis of Office of Management and Budget's Information Technology Dashboard | GAO-16-468

According to agency data reported to OMB's IT Dashboard, the 10 IT investments spending the most on O&M for fiscal year 2015 total $12.5 billion, 20 percent of the total O&M spending, and range from $4.4 billion on the Department of Health and Human Services' (HHS) Centers for Medicare and Medicaid Services' Medicaid Management Information

[21] This $80 billion represents what 26 agencies reported to OMB on planned IT spending. However, this $80 billion figure is understated. This figure does not include spending for Defense classified IT systems; and 58 independent executive branch agencies, including the Central Intelligence Agency. Additionally, not all executive branch IT investments are included in this estimate because agencies have differed on what they considered an IT investment. For example, some have considered research and development systems as IT investments, while others have not.

System[22] to $666.1 million on HHS's Centers for Medicare and Medicaid Services IT Infrastructure investment (see table 1).

Table 1: Ten Largest Expenditures on Operations and Maintenance Investments in Fiscal Year 2015, in millions

Agency	Investment	Fiscal year 2015 funds in millions
Department of Health and Human Services	Centers for Medicare and Medicaid Services' Medicare Management Information System[a]	$4,381.0
Department of Defense	Defense Information Systems Network	$1,252.2
Department of Veterans Affairs	Medical IT Support	$1,234.9
Department of Defense	Next Generation Enterprise Network Increment 1	$1,057.7
Social Security Administration	Infrastructure Operations and Maintenance	$864.0
Department of Veterans Affairs	Enterprise IT Support	$809.5
Department of Defense	Network Enterprise Technology Command	$767.5
Department of Defense	Network Enterprise Center Staff Operations Costs	$752.8
Department of Defense	Non-Defense Information Systems Network Telecomm	$688.8
Department of Health and Human Services	Centers for Medicare and Medicaid Services IT Infrastructure – Ongoing	$666.1
Total		**$12,474.5 million**

Source: GAO analysis of agency budgetary data. | GAO-16-468

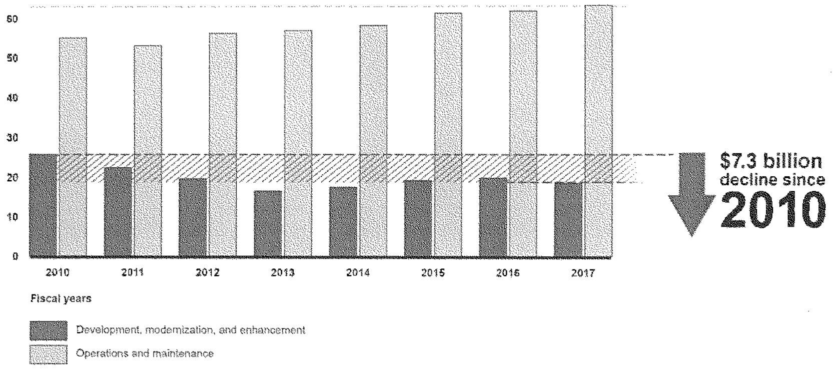
Note: [a]This investment represents the federal share of state Medicaid systems' cost. In technical comments on a draft of this report, the Department of Health and Human Services stated that it does not manage any of these IT assets or control how this money is spent.

[22] The 50 states, the District of Columbia, and the 5 U.S. territories each administer a state-based Medicaid program. Every state must implement a claims processing and information retrieval system to support the administration of the program. This investment represents the federal share of state Medicaid systems' cost. In technical comments on a draft of this report, HHS stated that it does not manage any of these IT assets or control how this money is spent.

Spending on O&M Has Increased over 7 Years

Over the past 7 fiscal years, O&M spending has increased, while the amount invested in developing new systems has decreased by about $7.3 billion since fiscal year 2010. (See figure 3.)

Figure 3: Summary of IT Spending by Fiscal Year from 2010 through 2017 (Dollars in Billions)

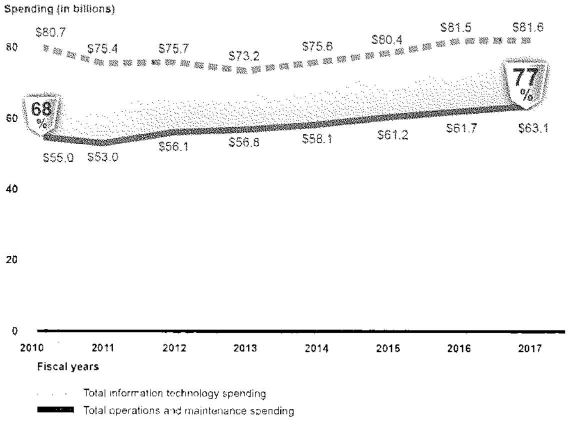


Source: GAO analysis of agency data. | GAO-16-468

Note: According to DOD officials, the department's fiscal year 2010 IT expenditures reported to the IT Dashboard includes both classified and unclassified spending, whereas its fiscal year 2011 to 2017 expenditures only include unclassified spending.

Further, agencies have increased the amount of O&M spending relative to their overall IT spending by 9 percent since 2010. Specifically, in fiscal year 2010, O&M spending was 68 percent of the federal IT budget, while in fiscal year 2017, agencies plan to spend 77 percent of their IT funds on O&M. (See figure 4.)

Figure 4: Percentage of IT Spending on Operations and Maintenance from Fiscal Year 2010 to Fiscal Year 2017



Source: GAO analysis of agency data. | GAO-16-468

Further, 15 of the 26 agencies have increased their spending on O&M from fiscal year 2010 to fiscal year 2015, with 10 of these agencies having over a $100 million increase. The spending changes per agency range from an approximately $4 billion increase (HHS) to a decrease of $600 million (National Aeronautics and Space Administration). See table 2 for more details on agency spending.

Table 2: Change in Agency Spending on Operations and Maintenance from Fiscal Year 2010 to 2015

Agency	Change in spending, in millions (percent change)
Department of Health and Human Services	$4,288.7 (-10.5%)
Department of Veterans Affairs	$792.8 (2.5%)
Department of Homeland Security	$632.8 (16.6%)
Department of Agriculture	$582.0 (6.6%)
Department of Transportation	$361.3 (6.8%)
Social Security Administration	$292.0 (9.4%)
Department of Justice	$258.9 (14.6%)
Department of the Treasury	$211.4 (-8.1%)
Department of the Interior	$116.8 (5.0%)
Department of State	$109.0 (-0.9%)
Department of Labor	$80.9 (2.2%)
Department of Education	$61.3 (19.5%)
Nuclear Regulatory Commission	$27.0 (5.6%)
National Science Foundation	$15.0 (1.0%)
Office of Personnel Management	$10.5 (-16.3%)
Small Business Administration	$-3.2 (11.1%)
National Archives and Records Administration	$-4.7 (9.3%)
U.S. Agency for International Development	$-8.6 (19.1%)
General Services Administration	$-19.7 (-5.9%)
Environmental Protection Agency	$-28.4 (7.0%)
U.S. Army Corps of Engineers	$-38.4 (3.5%)
Department of Housing and Urban Development	$-50.7 (-1.5%)
Department of Commerce	$-112.6 (17.0%)
Department of Energy	$-303.5 (1.8%)
Department of Defense	$-450.3 (13.9%)
National Aeronautics and Space Administration	$-600.2 (1.2%)

Source: GAO analysis of IT Dashboard data. | GAO-16-468

In addition, 20 of the 26 agencies have increased the percentage of total IT spending on O&M from fiscal year 2010 to fiscal year 2015, with 13 agencies having an increase of over 5 percent. The percentage of total IT spending on O&M ranges from a 20 percent increase (Department of Education) to a 16 percent decrease (Office of Personnel Management). Appendix II provides detailed information on agency spending on operations and maintenance from fiscal year 2010 to fiscal year 2015.

According to agency officials, reasons for the increase in O&M spending include the recent shift of major systems from DME to O&M (as the investment completed development activities and began O&M activities); and rising costs to maintain legacy IT infrastructure, such as those that use older programming languages. They also noted that improved reporting (i.e., ensuring that O&M expenditures were properly reported as O&M instead of as DME) has made it appear that O&M spending has increased.

For example, a DHS official in the Office of the CIO stated that one reason for the increased spending on O&M as a percentage of its total is because initially DHS had high DME spending to setup the agency, but now that the major parts of the agency are established, the funding has shifted to O&M.[23] DHS officials stated that they anticipate future increases in DME funding as prioritized IT modernization efforts are approved and funded. Further, an official in Department of State's (State) Bureau of Information Resource Management stated that the increase is largely due to increased costs of maintaining the infrastructure, including meeting security requirements. Moreover, VA officials stated that updates to its technology are the primary reason for the increase in spending. In addition, an official in HHS's Office of the CIO stated that the increased spending on O&M was largely due to grants to states and local entities for new programs, such as the Affordable Care Act.

Conversely, several agencies have decreased spending on O&M. For example, as we have previously reported, the Department of Energy (Energy) reduced spending by approximately $300 million, which it attributed to the reclassification of high performance computers from the IT portfolio to facilities.[24] According to Energy officials, these investments were re-categorized because they include both supercomputers and laboratory facilities.[25] Similarly, the Department of Commerce (Commerce) reduced spending by approximately $110 million and attributed it to the reclassification of satellite ground systems from its IT portfolio. In making this decision, Commerce determined that it needed to

[23] DHS was established in 2002 and combined 22 different departments and agencies into one cabinet-level agency.

[24] GAO-14-64.

[25] While Energy has reportedly established a separate process to report to OMB on these computers, these expenditures are not included in federal estimates of IT O&M spending.

refocus oversight efforts to a more appropriate level and consequently minimized the role of the CIO and others in the oversight of satellites. We disagreed with these reclassifications, and reported that they run contrary to the Clinger-Cohen Act of 1996, which specifies requirements for the management of IT. Further, we reported that by gathering incomplete information on IT investments, OMB increases the risk of not fulfilling its oversight responsibilities, of agencies making inefficient and ineffective investment decisions, and of Congress and the public being misinformed as to the performance of federal IT investments. We recommended that Energy and Commerce appropriately categorize their IT investments, but both agencies disagreed.

A policy analyst within OMB's Office of E-Government and Information Technology expressed concern when agencies, or their bureaus, spend a low percentage of their IT funds on DME. The analyst further stated that this could indicate that the agency's maintenance costs are reducing its flexibility and the agency or bureau is unable to innovate. For example, 5 of the 26 agencies that report to the IT Dashboard reported spending less than 10 percent on DME activities in fiscal year 2015 (see table 3).

Table 3: Federal Agencies Reporting Less than 10 Percent of Their IT Spending on Development, Modernization, and Enhancement (DME) in Fiscal Year 2015

Agency	Percent spent on DME activities
Department of Housing and Urban Development	7.55%
Department of the Interior	8.17%
Environmental Protection Agency	9.92%
National Aeronautics and Space Administration	8.70%
U.S. Army Corps of Engineers	0.75%

Source: GAO analysis of IT Dashboard data. | GAO-16-468

Further, 34 percent of bureaus (i.e., 51 of the 151) spent less than 10 percent on DME. For more details on the bureaus spending less than 10 percent on DME activities, see appendix III.

According to agency officials, reasons for these bureaus' low spending on DME include the size and mission of the bureau (e.g., smaller bureaus do not perform much DME work), as well as several bureaus having recently completed major DME work that is now in the O&M phase. Further, according to Commerce officials, one of their bureaus had no actual IT systems in its budget, as its IT has been absorbed by headquarters, and thus any DME spending is part of the Office of IT Services' budget.

OMB staff in the Office of E-Government and Information Technology have recognized the upward trend of O&M spending and identified several contributing factors, including (1) the support of O&M activities requires maintaining legacy hardware, which costs more over time, and (2) costs are increased in maintaining applications and systems that use older programming languages, since programmers knowledgeable in these older languages are becoming increasingly rare and thus more expensive. Further, OMB officials stated that in several situations where agencies are not sure whether to report costs as O&M or DME, agencies default to reporting as O&M. According to OMB, agencies tend to categorize investments as O&M because they attract less oversight, require reduced documentation, and have a lower risk of losing funding.

Less than a Quarter of Federal IT Spending Is Categorized as Provisioned

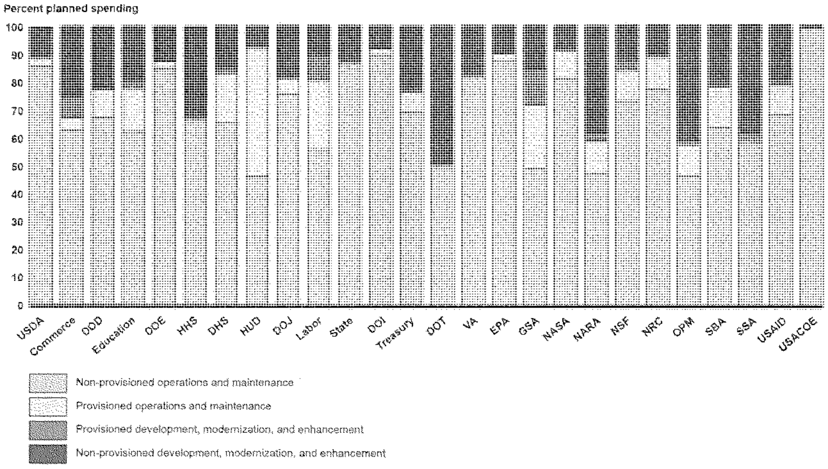
OMB encourages agencies to adopt provisioned IT services, such as cloud computing and shared services, to make IT more efficient and agile, and enable innovation.[26] Specifically, it provides an approach for agencies to implement cloud-based solutions whenever a secure, reliable, and cost-effective cloud option exists and to use shared services for IT service delivery in order to increase return on investment, eliminate waste and duplication, and improve the effectiveness of IT solutions. Further, as part of its guidance on the implementation of recent IT legislation,[27] OMB identified a series of performance metrics for agencies' PortfolioStat sessions to measure the federal government's progress in driving value in federal IT investments. One measure is the percent of IT spending on non-provisioned O&M spending. An OMB official stated that focusing on the O&M spending that has not been provisioned will allow OMB to identify legacy systems in need of modernization.

Federal agencies reported spending $55 billion—69 percent of total IT spending—on non-provisioned O&M in fiscal year 2015, with the percent allocated to non-provisioned O&M varying by agency. For example, State allocates about 87 percent of its IT spending on non-provisioned O&M, whereas the Department of Transportation (DOT) allocates 50 percent. See figure 5 for details on agencies' planned spending allocations.

[26] OMB, *Federal Cloud Computing Strategy*, (Washington, D.C.: Feb. 8, 2011).

[27] OMB, *Management and Oversight of Federal Information Technology*, M-15-14 (Washington, D.C.: June 10, 2015).

Figure 5: Allocation of Planned IT Spending for Fiscal Year 2015, by agency



Abbreviations:
USDA (United States Department of Agriculture), Commerce (Department of Commerce), DOD (Department of Defense), Education (Department of Education), DOE (Department of Energy), HHS (Department of Health and Human Services), DHS (Department of Homeland Security), HUD (Department of Housing and Urban Development), DOJ (Department of Justice), Labor (Department of Labor), State (Department of State), DOI (Department of the Interior), Treasury (Department of the Treasury), DOT (Department of Transportation), VA (Department of Veterans Affairs), EPA (Environmental Protection Agency), GSA (General Services Administration), NASA (National Aeronautics and Space Administration), NARA (National Archives and Records Administration), NSF (National Science Foundation), NRC (Nuclear Regulatory Commission), OPM (Office of Personnel Management), SBA (Small Business Administration), SSA (Social Security Administration), USAID (United States Agency for International Development), USACOE (U.S. Army Corps of Engineers)

Source: GAO analysis of Information Technology Dashboard data. | GAO-16-468

Additionally, OMB has not identified an associated goal with its non-provisioned IT measure that is part of PortfolioStat process. An OMB official within the Office of E-Government and Information Technology stated that the aim is for the amount of spending on DME and provisioned IT services to rise, thus reducing the percent of spending on non-provisioned IT. This official also stated that OMB has not identified a specific goal for the measure because it would be ever changing. While goals for performance measures may change over time, it is still important for OMB to set a target by which agencies can measure their progress in meeting this measure.

In particular, leading practices stress that organizations should measure performance in order to evaluate the success or failure of their activities and programs.[28] Performance measurement involves identifying performance goals and measures, identifying targets for improving performance, and measuring progress against those targets. Without links to outcomes and goals, organizations are not able to effectively measure progress toward those goals. Further, OMB's own website, performance.gov[29] states that when measuring performance, a goal is a simple but powerful way to motivate people and communicate priorities. In addition, the website states that the federal government operates more effectively when agency leaders, at all levels of the organization, starting at the top, set clear measurable goals aligned to achieving better outcomes.

Until OMB develops a specific goal associated with measuring non-provisioned services, OMB and agencies will be limited in their ability to evaluate progress that has been made and whether or not they are achieving their goals to increase the amount spent on development activities and provisioned IT services.

Many O&M Investments Were at Risk and Lacked Proper Oversight

According to OMB guidance,[30] the O&M phase is often the longest phase of an investment and can consume more than 80 percent of the total lifecycle costs. As such, agencies must actively manage their investment during this phase. To help them do so, OMB requires that CIOs submit ratings that reflect the level of risk facing an investment.

[28] Department of the Navy, Office of the Chief Information Officer, *Guide for Developing and Using Information Technology (IT) Performance Measurements* (Washington, D.C.: October 2001); and General Services Administration, Office of Governmentwide Policy, *Performance-Based Management: Eight Steps To Develop and Use Information Technology Performance Measures Effectively* (Washington, D.C.: 1996).

[29] In 2011, OMB established a single, performance-related website (http://performance.gov) that is intended to provide both a public view into government performance to support transparency as well as providing executive branch management capabilities to enhance senior leadership decision making.

[30] OMB, *Preparation, Submission, and Execution of the Budget*, Circular No. A-11 (2015).

Several O&M investments were rated as moderate to high risk in fiscal year 2015. Specifically, CIOs from the 12 selected agencies reported that 23 of their 187 major IT O&M investments were moderate to high risk as of August 2015. They requested $922.9 million in fiscal year 2016 for these investments. Of the 23 investments, agencies had plans to replace or modernize 19 investments. However, the plans for 12 of those were general or tentative in that the agencies did not provide specificity on time frames, activities to be performed, or functions to be replaced or enhanced. Further, agencies did not plan to modernize or replace 4 of the investments (see table 4).

Table 4: Moderate to High-Risk Operations and Maintenance Investments

Agency	Investment title (IT portfolio)	CIO rating, as of August 2015	Specific, defined plans for modernization or replacement
Department of Agriculture	Resource Ordering and Status System[a]	Moderate	Yes - Agency plans to replace the system in 2018.
	Public Safety Land Mobile Radio System	Moderate	No - Agency recently began a modernization initiative; however, it is not clear when it will be completed.
	Forest Service Computer Base	Moderate	No - Agency has general plans to restructure the investment to allow better visibility into the underlying systems, but has not provided plans for functions to be replaced or enhanced.
	Enterprise Telecommunications Shared Services	High	Yes - Agency has several modernization efforts underway, including one to consolidate networks.
Department of Commerce	National Oceanic and Atmospheric Administration/ National Weather Service Telecommunication Gateway System[a]	High	Yes - Agency plans to retire the system in fiscal year 2017, and replace it with a new system.
	Office of Chief Information Officer Enterprise Cyber Security Monitoring and Operations	Moderate	No - Agency has general plans to update cyber monitoring across the agency, but has not provided specific activities or timelines associated with this effort.
Department of Energy	Contractor Business Financial and Administrative Systems[a]	Moderate	No - Agency has no firm future plans for retirement or modernization.
Department of Health and Human Services	Centers for Medicare and Medicaid Services Medicare Appeals System[a]	Moderate	No - The agency has general plans for continuous modernization, as funding allows; but has not provided specific activities or timelines associated with this effort.
	Trusted Internet Connection Investment	High[b]	No - Agency has general plans to continually evaluate the investment and perform necessary improvements as needed; but has not provided plans for specific functions to be replaced or enhanced.
Department of Homeland Security	Immigration and Customs Enforcement - Detention and Removal Operations Modernization	Moderate	Yes - Agency has specific plans to improve the core database infrastructure in fiscal year 2016.

Agency	Investment title (IT portfolio)	CIO rating, as of August 2015	Specific, defined plans for modernization or replacement
	Immigration and Customs Enforcement - IT Infrastructure	Moderate	Yes - Agency plans to replace its IT equipment that is outdated in 2016.
	National Protection and Programs Directorate - Infrastructure Security Compliance - Chemical Security Assessment Tool	Moderate	No - Agency has general plans for minor enhancements, but has not provided specific timelines associated with this effort.
	OneNet	Moderate	No - Agency has general plans for continuous updates to this investment as user requirements change, but has not provided specific timelines associated with this effort.
	Coast Guard - Vessel Logistics System	Moderate	No - Agency has plans to decommission one system within the investment in 2016. The agency has general plans to replace the full investment in the future with the Logistics Information Management System, but there is no firm transition date.
	Coast Guard - Core Accounting System Suite[a]	Moderate	Yes - Agency plans to retire the system in fiscal year 2018 with a migration to federal shared services.
	Coast Guard - Standard Workstation Infrastructure Recapitalization and Sustainment	Moderate	No - Agency has general plans, including a migration to Windows 10, but did not provide dates on when this would happen.
	Customs and Border Protection - Tactical Communications Modernization	Moderate	Yes - Agency plans to decommission obsolete equipment by the end of fiscal year 2017.
	Customs and Border Protection - Integrated Fixed Towers	High[b]	No - Agency has no plans for retirement or modernization at this time because the investment only reached initial operating capability in October 2015. It plans to reach final operating capability in fiscal year 2020.
	National Protection and Programs Directorate – Federal Protective Service Tac Com Equipment and Support	Moderate	No - Agency has general plans to update the program, but no firm date associated with the effort.
	Customs and Border Protection - Tethered Aerostat Radar System	Moderate	No - Agency has no plans for replacement or modernization of the investment, but is currently undergoing an analysis of alternatives to determine whether they should modernize or replace the system.
	Customs and Border Protection – TRIRIGA	Moderate	No - Agency has no plans for replacement or modernization of the investment.
Department of the Treasury	Departmental Offices IT Infrastructure Mainframes and Servers Services and Support	Moderate	No - Agency has general plans to update this investment, but has not provided specific activities or timelines associated with this effort.
	Departmental Offices IT Infrastructure End User Systems and Support	Moderate	No - Agency has general plans to update this investment, but has not provided specific activities or timelines associated with this effort.

Source: GAO analysis of IT Dashboard data, agency documentation, and interviews. | GAO-16-468

Notes:

[a] Investment was selected for profiling and will be discussed further in an appendix of the report.

[b] According to agency officials, this investment has since been lowered to moderate risk.

The lack of specific plans to modernize or replace these investments could result in wasteful spending on moderate- and high-risk investments.

Many O&M Investments Lacked Reviews and Oversight

In instances where investments experience problems, agencies can perform a TechStat, a face-to-face meeting to terminate or turn around IT investments that are failing or not producing results.[31] In addition, OMB directs agencies to monitor O&M investments through operational analyses, which should be performed annually and assess costs, schedules, whether the investment is still meeting customer and business needs, and investment performance.

While agencies generally conducted the required operational analyses, they did not consistently perform TechStat reviews on all of the at-risk investments. Table 5 provides details on the 23 investments and whether the operational analyses and TechStats were performed.

Table 5: At-Risk Investments and Required Analyses and Oversight Activities

Agency	Investment	TechStat performed	Operational analysis performed
Department of Agriculture	Resource Ordering and Status System	X	X
	Public Safety Land Mobile Radio System		X
	Forest Service Computer Base		X
	Enterprise Telecommunications Shared Services		X
Department of Commerce	National Oceanic and Atmospheric Administration/ National Weather Service Telecommunication Gateway System	X	X
	Office of Chief Information Officer Enterprise Cyber Security Monitoring and Operations		
Department of Energy	Contractor Business Financial and Administrative Systems	X	X
Department of Health and Human Services	Centers for Medicare and Medicaid Services Medicare Appeals System	X	X
	Trusted Internet Connection Investment		X

[31] OMB, *25-Point Implementation Plan to Reform Federal Information Technology Management* (Washington, D.C.: Dec. 9, 2010).

Agency	Investment	TechStat performed	Operational analysis performed
Department of Homeland Security	Immigration and Customs Enforcement - Detention and Removal Operations Modernization		X
	Immigration and Customs Enforcement - IT Infrastructure		X
	National Protection and Programs Directorate - Infrastructure Security Compliance - Chemical Security Assessment Tool		X
	OneNet		X
	Coast Guard - Vessel Logistics System		X
	Coast Guard - Core Accounting System Suite		X
	Coast Guard - Standard Workstation Infrastructure Recapitalization and Sustainment		X
	Customs and Border Protection - Tactical Communications Modernization		X
	Customs and Border Protection - Integrated Fixed Towers		
	National Protection and Programs Directorate – Federal Protective Service Tac Com Equipment and Support	X	X
	Customs and Border Protection - Tethered Aerostat Radar System		X
	Customs and Border Protection – TRIRIGA		X
Department of the Treasury	Departmental Offices IT Infrastructure Mainframes and Servers Services and Support		
	Departmental Offices IT Infrastructure End User Systems and Support		

Source: GAO analysis of agency documentation. | GAO-16-468

Although not required, agencies had performed TechStats on only five of the at-risk investments. Moreover, TechStats were not performed on three of the four investments rated as high risk:

- DHS's Customs and Border Protection - Integrated Fixed Towers,
- HHS's Trusted Internet Connection Investment, and
- U.S. Department of Agriculture's (USDA) Enterprise Telecommunications Shared Services.

Agencies provided several reasons for not conducting TechStats. For example, according to agency officials, several of the investments' risk levels were reduced to low or moderately-low risk in the months since the IT Dashboard had been publicly updated.[32] An Acting Deputy Executive Director in DHS's Enterprise Business Management Office stated that the

[32] The public portion of the IT Dashboard is not updated during the formulation of President's Budget.

agency had performed an internal "health assessment" on its Integrated Fixed Towers investment, understood the issues it was facing, and decided that a TechStat was not necessary. An official from HHS's Office of the CIO stated that, at the time it was evaluated, its Trusted Internet Connection Investment did not meet its internal TechStat criteria of having cost variance over 10 percent. An official from USDA's Office of the CIO stated that while the office did not hold a formal TechStat, the program was required to work on a corrective action plan and has since been upgraded from high to moderate risk.

It should be noted that recent legislation requires agencies to perform a review of each major IT investment that receives a high-risk rating for 4 consecutive quarters.[33] Further, the associated OMB guidance requires agencies to hold a TechStat on an investment if it has been rated as high risk for 3 consecutive months.[34]

In addition, operational analyses were not conducted for four at-risk investments. These investments were:

- Commerce's Enterprise Cyber Security Monitoring and Operations,
- DHS's Integrated Fixed Towers,
- Treasury's Departmental Offices IT Infrastructure Mainframes and Servers Services and Support, and
- Treasury's Departmental Offices IT Infrastructure End User Systems and Support.

An official from Commerce's Office of the CIO stated that, in place of operational analyses, National Weather Service (the responsible bureau) reviews the status of the previous month's activities for the development, integration, modification, and procurement to report issues to management. However, Commerce's monthly process does not include all of the key elements of an operational analysis. The Integrated Fixed Towers Program Manager stated that since the investment had only

[33] 40 U.S.C. § 11302(c)(4). The statute does not specify that a TechStat must be conducted but requires a review that shall identify the (1) root causes of the high risk, (2) extent to which the causes can be addressed, and (3) probability of future success. The assessment of Defense's major IT investments may be accomplished in accordance with 10 U.S.C. § 2445c.

[34] OMB, *Management and Oversight of Federal Information Technology*, Memorandum M-15-14 (Washington, D.C.: June 10, 2015).

become operational in October 2015, an operational analysis was not yet required. DHS plans to perform the analysis on the investment in August 2017. Performing the analysis once the investment is operational will enable DHS to determine whether it is meeting the needs of the agency and delivering the expected value.

The Director of Treasury's Capital Planning and Investment Control program stated that the department's policy does not require infrastructure investments to have an operational analysis performed.[35] However, OMB's guidance on operational analyses does not exclude infrastructure investments.

Until agencies ensure that their O&M investments are fully reviewed, the government's oversight of old and vulnerable investments will be impaired and the associated spending could be wasteful.

IT Investments Are Becoming Obsolete and Agencies Are Not Required to Identify Investments That Need Attention

Legacy IT investments across the federal government are becoming increasingly obsolete. Specifically, many use outdated languages and old parts. Numerous old investments are using obsolete programming languages. Several agencies, such as the Department of Justice (Justice), DHS, HHS, Treasury, USDA, and VA, reported using Common Business Oriented Language (COBOL)—a programming language developed in the late 1950s and early 1960s—to program their legacy systems. It is widely known that agencies need to move to more modern, maintainable languages, as appropriate and feasible. For example, the Gartner Group, a leading IT research and advisory company, has reported that organizations using COBOL should consider replacing the language and in 2010 noted that there should be a shift in focus to using more modern languages for new products.[36]

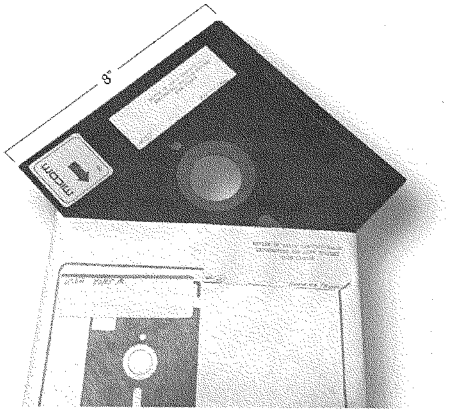
In addition, some legacy systems may use parts that are obsolete and more difficult to find. For instance, Defense is still using 8-inch floppy

[35] As of 2015, Treasury's bureau, the Internal Revenue Service, developed and implemented a process to prioritize its operations support activities that addresses prioritization and comparison of IT assets against each other and criteria for making selection and prioritization decisions.

[36] Gartner, *IT Market Clock for Application Development*, August 2010.

disks in a legacy system that coordinates the operational functions of the United States' nuclear forces.[37] (See figure 6).

Figure 6: Example of an 8-Inch Floppy Disk



Source: GAO. | GAO-16-468

Further, in some cases, the vendors no longer provide support for hardware or software, creating security vulnerabilities and additional costs. For example, each of the 12 selected agencies reported using unsupported operating systems and components in their fiscal year 2014 reports pursuant to the Federal Information Security Management Act of 2002. Commerce, Defense, DOT, HHS, and VA reported using 1980s and 1990s Microsoft operating systems that stopped being supported by the vendor more than a decade ago.

[37] Introduced in the 1970s, the 8-inch floppy disk is a disk-based storage medium that holds 80 kilobytes of data. In comparison, a single modern flash drive can contain data from the equivalent of more than 3.2 million floppy disks.

Lastly, legacy systems may become increasingly more expensive as agencies have to deal with the previously mentioned issues and may pay a premium to hire staff or contractors with the knowledge to maintain outdated systems. For example, one agency (SSA) reported re-hiring retired employees to maintain its COBOL systems.

Selected agencies reported that they continue to maintain old investments in O&M. For example, Treasury reported systems that were about 56 years old.

Table 6 shows the 10 oldest investments and/or systems, as reported by selected agencies.[38] Agencies reported having plans to modernize or replace each of these investments and systems. However, the plans for five of those were general or tentative in that the agencies did not provide specific time frames, activities to be performed, or functions to be replaced or enhanced. For a full list of the agencies' reported oldest systems, see appendix IV.

Table 6: Ten Oldest IT Investments or Systems as Reported by 12 Selected Agencies

Agency	Investment or system	Description	Agency-reported age	Specific, defined plans for modernization or replacement
Department of the Treasury	Individual Master File	This investment is the authoritative data source for individual taxpayer accounts where accounts are updated, taxes are assessed, and refunds are generated during the tax filing period. It is written in assembly language code—a low-level computer code that is difficult to write and maintain. However, the hardware has been upgraded to a more modern IBM mainframe.	~56	No - A new investment will eventually replace this investment, but there is no firm date associated with the transition.
Department of the Treasury	Business Master File	This investment retains all tax data pertaining to individual business income taxpayers and reflects a continuously updated and current record of each taxpayer's account. It is also written in assembly language code and operates on an IBM mainframe.	~56	No - The agency has general plans to update this system, but there is no date associated with this update.

[38] Not all agencies track systems and their associated ages in the same manner—some track individual systems and others track by investment. An investment may be made up of several systems and infrastructure. In some cases, agencies were unsure of the actual age of the system or investment and had to approximate the initiation date.

Agency	Investment or system	Description	Agency-reported age	Specific, defined plans for modernization or replacement
Department of Defense	Strategic Automated Command and Control System	This system coordinates the operational functions of the United States' nuclear forces, such as intercontinental ballistic missiles, nuclear bombers, and tanker support aircrafts. It runs on an IBM Series/1 Computer—a 1970s computing system—and uses 8-inch floppy disks.	53	Yes - The agency is planning to update data storage solutions, port expansion processors, portable terminals, and desktop terminals; which are all scheduled to be completed by the end of fiscal year 2017.
Department of Veterans Affairs	Personnel and Accounting Integrated Data	This system automates time and attendance for employees, timekeepers, payroll, and supervisors. It is written in COBOL—a programming language developed in the 1950s and 1960s—and runs on IBM mainframes.	53	Yes - The agency plans to replace it with a project called Human Resources Information System Shared Service Center in 2017.
Department of Defense	Compass	This system is a command and control system that is used for deliberate and crisis action planning, strategic mobility analysis, and mobilization and deployment movement execution. It runs on a Windows 2008 server and is programed in Java—a programming language first released in 1995. It also uses a 2009 Oracle 11g database.	52	Yes - The system is currently using an Oracle 11g database, but the agency plans to migrate it to a 2012 SQL server by the end of the year.
Department of Veterans Affairs	Benefits Delivery Network	This system tracks claims filed by veterans for benefits, eligibility, and dates of death. It is a suite of COBOL mainframe applications.	51	No - The agency has general plans to roll capabilities into another system, but there is no firm date associated with this transition.
Department of Transportation	Hazardous Materials Information System at the Pipeline and Hazardous Materials Safety Administration	This system allows the agency to maintain comprehensive information on hazardous materials incidents. The software applications and processes used by the system, such as Classic Active Server Pages and Microsoft.NET, have become outdated and costly to maintain. In addition, the system uses an application that is no longer supported by the manufacturer, which can cause security risks, among other issues.	~46	Yes - All legacy components within this system are scheduled to be replaced by 2018.
Department of Commerce	National Oceanic and Atmospheric Administration/ National Weather Service Dissemination Systems	This investment includes three information dissemination systems used to provide the US public and emergency managers warnings of severe weather events. It runs a variety of operating systems and software, including Windows Server 2003, which is no longer supported by the vendor, and uses a variety of programming languages including FORTRAN—a high-level programming language developed in the 1950s for scientific and engineering applications.	46	No - The agency has general plans to continuously update system components.

Agency	Investment or system	Description	Agency-reported age	Specific, defined plans for modernization or replacement
Department of Commerce	National Oceanic and Atmospheric Administration/ National Weather Service/ National Data Buoy Center Ocean Observing System of Systems	This investment supports systems that include meteorological, oceanographic, tsunami, and climate observing platforms. It runs on both Windows and Linux operating systems, including Windows Server 2003, which is no longer supported by the vendor. In addition, it uses a version of Oracle that is also no longer fully supported by the vendor. This investment also uses a variety of programming languages, including FORTRAN.	46	No - The agency has general plans for continuous incremental upgrades to this investment.
Department of Homeland Security	Immigration and Customs Enforcement - Hiring Tracking Systems	This system is used by the agency to track current and prior hiring actions and maintains information about individuals who are selected for vacant positions. It runs on a 2008 IBM z10 mainframe using COBOL, among other languages. The web component runs on a Windows 2012 server using Java.	39	Yes - The agency plans to replace the existing mainframe with a service-oriented architecture to allow for integration with new systems beginning in fiscal year 2016, contingent upon receiving funding.

Source. GAO analysis of agency data. | GAO-16-468

Note: Systems and investments may have selected components newer than the reported age.

Separately, we profiled one system or investment from each of the 12 selected agencies. The selected systems and investments range from 11 to approximately 56 years old, and serve a variety of purposes. For example, Treasury's Individual Master File was first initiated about 56 years ago and currently is the authoritative data source for individual taxpayer accounts where accounts are updated, taxes are assessed, and refunds are generated during the tax filing period. In addition, DOT's profiled system was initiated about 46 years ago and allows the agency to maintain comprehensive information on hazardous materials incidents. Of the 12 investments or systems, agencies had plans to replace or modernize 11 of these. However, the plans for 3 of those were general or tentative in that the agencies did not provide specificity on time frames, activities to be performed, or functions to be replaced or enhanced. Further, there were no plans to replace or modernize 1 investment. The profiles of these systems and investments are summarized in table 7 and can be found in appendix V.

Table 7: Summary of Investments and Systems Profiled in Appendix V

Agency	Investment or system	Description	Agency-reported age	Specific, defined plans for modernization or replacement
Department of Commerce	National Weather Service Telecommunication Gateway	This investment is the nation's hub for the collection and distribution of weather data and products. The agency replaced its hardware and software with Power7 IBM servers and Unix operating systems; however, the investment still lacks full backup capability for 26 percent of its functions.	31	Yes - The agency plans to retire the system in fiscal year 2017 and replace it with a new system.
Department of Defense	Strategic Automated Command and Control System	This system coordinates the operational functions of the nation's nuclear forces. This system is running on an IBM Series/1 Computer—a 1970s computing system—and uses 8-inch floppy disks.	53	Yes - The agency is planning to update data storage solutions, port expansion processors, portable terminals, and desktop terminals are scheduled for completion by the end of fiscal year 2017. A full system replacement is scheduled to be completed in fiscal year 2020.
Department of Homeland Security	Core Accounting System Suite	This investment is the primary financial management system for the Coast Guard and other Department of Homeland Security agencies. The system relies on outdated and heavily customized Oracle Federal Financials software that was first available in 2004, and the extended vendor support for the software ended in November 2013. As a result, it has become expensive to support. Further, it relies on Windows 2003 servers and any changes would require recoding of many functions within its suite. In some cases, Coast Guard is unable to upgrade the system to the newest version of software because it is dependent on older versions of supporting software.	18	Yes - The agency plans to transition to federal shared services in fiscal year 2018.
Department of Transportation	Hazardous Material Information System	This system maintains and provides access to comprehensive information on hazardous materials incidents, among other things. The software applications and processes used by the system, such as Classic Active Server Pages and Microsoft.NET, have become outdated and costly to maintain. In addition, the system uses an application that is no longer supported by the manufacturer, which can cause security risks, among other issues.	~46	Yes - The agency is developing a new system to replace legacy modules and plans to retire the legacy modules by the end of fiscal year 2018.

Agency	Investment or system	Description	Agency-reported age	Specific, defined plans for modernization or replacement
Department of Energy	Contractor Business Financial and Administrative Systems	This investment is the business and administrative systems for a management and operating contractor, liquid waste contractor, and the site security contractor to manage human resources, financial reporting, supply chain, and project management. It runs on Windows and Unix servers and uses Oracle's PeopleSoft applications. The investment has gone through several updates, with the last including the retirement of 16 associated legacy applications in 2011.	12	No - The agency does not have future plans for retirement or modernization.
Department of Health and Human Services	Medicare Appeals System	This system facilitates the maintenance and transfer of case-specific data with regard to Medicare appeals through multiple levels of the appeal process. The system runs on a Solaris 10 operating system and uses commercial-off-the-shelf systems for case management and reporting.	11	No - The agency has general plans to continuously update the system.
Department of Justice	Sentry	This system provides information regarding security and custody levels, inmate program and work assignments, and other pertinent information about the inmate population. When the system was first deployed, it was comprised of approximately 700 program routines written in COBOL and ran on a mainframe platform. Over the years, the agency has updated the system to allow for web accessibility.	35	Yes – The agency plans to update the user interface and integrate system data through September 2016.
Social Security Administration	Title II Systems	These systems determine retirement benefits eligibility and amounts. The investment is comprised of 162 subsystems, and some are still written in COBOL.	31	Yes - The agency has ongoing modernization efforts, including one that is experiencing cost and schedule challenges due to the complexities of the legacy software.
Department of State	Diversity Visa Information System	This system is an electronic case management system to track and validate application information submitted by foreign nationals under the Diversity Visa immigration program. The interface software, PowerBuilder, is no longer supported by the vendor.	~26	No - The agency plans to replace the investment at an unknown date and has general plans to upgrade unsupported software to a new version, which is also not supported.
Department of the Treasury	Individual Master File	This investment is the authoritative data source for individual taxpayer accounts where accounts are updated, taxes are assessed, and refunds are generated during the tax filing period. This investment is written in assembly language code—a low-level computer code that is difficult to write and maintain—and operates on an IBM mainframe.	~56	No - The agency plans to replace the investment at an unknown date.

Agency	Investment or system	Description	Agency-reported age	Specific, defined plans for modernization or replacement
Department of Agriculture	Resource Ordering and Status System	This investment mobilizes and deploys a multitude of resources, including qualified individuals, teams, aircraft, equipment, and supplies to fight wildland fires and respond to all hazard incidents. One of the applications the system uses is no longer supported by the vendor, creating vulnerability issues.	18	Yes - The agency plans to replace the system in 2018.
Department of Veterans Affairs	Personnel and Accounting Integrated Data	This system automates time and attendance for employees, timekeepers, payroll, and supervisors. This system is written in COBOL—a programming language developed in the 1950s and 1960s—and runs on IBM mainframes.	53	Yes - The agency plans to replace most of the system's functionality in 2017.

Source: GAO analysis of agency documentation and interviews. | GAO-16-468

Note: Systems and investments may have components newer than the reported age.

We have previously provided guidance that organizations should periodically identify, evaluate, and prioritize their investments, including those that are in O&M; at, near, or exceeding their planned life cycles; and/or are based on technology that is now obsolete, to determine whether the investment should be kept as-is, modernized, replaced or retired.[39] This critical process allows the agency to identify and address high-cost or low-value investments in need of update, replacement, or retirement.

Agencies are, in part, maintaining obsolete investments because they are not required to identify, evaluate, and prioritize their O&M investments to determine whether they should be kept as-is, modernized, replaced, or retired. According to OMB staff from the Office of E-Government and Information Technology, OMB has created draft guidance that will require agencies to identify and prioritize legacy information systems that are in need of replacement or modernization. Specifically, the guidance is intended to develop criteria through which agencies can identify the highest priority legacy systems, evaluate and prioritize their portfolio of existing IT systems, and develop modernization plans that will guide agencies' efforts to streamline and improve their IT systems.

[39] GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, Version 1.1, GAO-04-394G (Washington, D.C.: March 2004).

The draft guidance includes time frames for the efforts regarding developing criteria, identifying and prioritizing systems, and planning for modernization. However, OMB did not commit to a firm time frame for when the policy would be issued. Until OMB's policy is finalized and carried out, the federal government runs the risk of continuing to maintain investments that have outlived their effectiveness and are consuming resources that outweigh their benefits.

Regarding upgrading obsolete investments, in April 2016, the IT Modernization Act[40] was introduced into the U.S. House of Representatives. If enacted, it would establish a revolving fund of $3 billion that could be used to retire, replace, or upgrade legacy IT systems to transition to new, more secure, efficient, modern IT systems. It also would establish processes to evaluate proposals for modernization submitted by agencies and monitor progress and performance in executing approved projects.

Conclusions

Of the more than $80 billion that the 26 agencies reported spending for federal IT in fiscal year 2015, the agencies spent about $61 billion on O&M. This O&M spending has steadily increased and as a result, key agencies are devoting a small amount of IT spending to DME activities. To its credit, OMB has identified a performance metric to measure the percent of IT spending on non-provisioned IT spending. However, it has not identified an associated goal with this measure. Until it does so, OMB and agencies will be constrained in their ability to evaluate their progress in adopting cloud and shared services.

Several of the 12 selected agencies' major O&M investments were rated as moderate or high risk in fiscal year 2015. While the agencies had specific plans to retire or modernize some of these investments, most investments did not have specific plans with time frames, activities to be performed, or functions to be replaced or enhanced. Further, agencies did not consistently perform required analysis on at-risk investments. Until agencies fully review at-risk O&M investments, the government's oversight of such investments will be impaired and its spending could be wasteful.

[40] *Information Technology Modernization Act*, H.R. 4897, 114th Cong. (2016).

Finally, legacy federal IT investments are becoming obsolete. Several aging investments are using unsupported components, many of which did not have specific plans for modernization or replacement. This is contrary to OMB's draft initiative, which calls for agencies to analyze and review O&M investments. Until this policy is finalized and implemented, the federal government runs the risk of continuing to maintain investments that have outlived their effectiveness and are consuming resources that outweigh their benefits.

Recommendations for Executive Action

To better manage legacy systems and investments, we are making 2 recommendations to OMB and 14 recommendations to federal agencies.

Specifically, we recommend that the Director of OMB

- identify and publish a specific goal associated with its non-provisioned O&M spending measure, and
- commit to a firm date by which its draft guidance on legacy systems will be issued, and subsequently direct agencies to identify legacy systems and/or investments needing to be modernized or replaced.

To monitor whether existing investments are meeting the needs of their agencies, we recommend that the Secretaries of Commerce and the Treasury direct the respective agency CIO to ensure that required analyses are performed on investments in the operations and maintenance phase.

Further, to address obsolete IT investments in need of modernization or replacement, we recommend that the Secretaries of Agriculture, Commerce, Defense, Energy, Health and Human Services, Homeland Security, State, the Treasury, Transportation, and Veterans Affairs; the Attorney General; and the Commissioner of Social Security direct their respective agency CIOs to identify and plan to modernize or replace legacy systems as needed and consistent with OMB's draft guidance, including time frames, activities to be performed, and functions to be replaced or enhanced.

Agency Comments and Our Evaluation

We received comments on a draft of this report from OMB and the other 12 agencies in our review. Eight agencies (USDA, Commerce, HHS, DHS, State, Transportation, VA, and SSA) and OMB agreed with our recommendations, Defense and Energy partially agreed, and Justice and the Treasury stated they had no comment on the recommendations. Each agency's comments are discussed in more detail below.

- In comments provided via e-mail on May 12, 2016, an official from OMB's Office of E-Government and Technology stated that it concurred with our recommendations. The agency also provided technical comments, which we have incorporated in the report as appropriate.

- In comments provided via e-mail on May 3, 2016, an official from USDA's Office of the CIO's Oversight and Compliance Division stated that the department concurred with our recommendation.

- In written comments, Commerce concurred with both of its recommendations. Regarding the recommendation that the department ensure that required analyses are performed on investments in the O&M phase, the department concurred and stated that it will reiterate and expand the department's existing policies requiring such analyses. The department also concurred with the recommendation to identify and plan to modernize or replace legacy systems and stated that it is already appropriately replacing and modernizing systems as needed within budget constraints. Commerce's comments are reprinted in appendix VI. The department also provided technical comments, which we have incorporated in the report as appropriate.

- In written comments, Defense partially concurred with our recommendation to address obsolete IT investments in need of modernization or replacement. It stated that the department has modernized, upgraded, or retired hundreds of systems in the last several years through an investment review process. The department stated it plans to continue to identify, prioritize, and manage legacy systems that should be modernized or replaced, based on existing department policies and processes, and consistent to the extent practicable with OMB's draft guidance. Defense's plan to be consistent with OMB's guidance to the extent practicable is consistent with the intent of our recommendation. Defense's comments are reprinted in appendix VII.

- In written comments, Energy partially concurred with our recommendation to address obsolete IT investments and stated that the department continues to take steps to modernize its legacy investments and systems, as needed and as funding is available. It further stated that all four of the systems listed in appendix IV have been identified for modernization or replacement and three have been modernized as recently as fiscal year 2015. However, since OMB's draft guidance has not yet been issued, Energy could not concur with this part of the recommendation, but plans to review and consider implementation of such guidance. Energy's plan to consider OMB's guidance when it is finalized is consistent with the intent of our recommendation. Energy's comments are reprinted in appendix VIII. The department also provided technical comments, which we have incorporated in the report as appropriate.

- In written comments, HHS stated that it concurred with our recommendation and is working to identify and plan to modernize or replace IT systems. HHS's comments are reprinted in appendix IX. The department also provided technical comments, which we have incorporated in the report as appropriate.
- In written comments, DHS stated that it concurred with its recommendation and that the department plans to establish a framework for identifying and replacing or modernizing legacy systems after receipt of the finalized guidance. DHS's comments are reprinted in appendix X. The department also provided technical comments, which we have incorporated in the report as appropriate.
- In comments provided via e-mail on May 11, 2016, an official from Justice's audit liaison group, speaking on behalf of the department, stated that it had no comment on the recommendation but plans to follow OMB's guidance once it is formally issued. The department also provided technical comments, which we have incorporated in the report as appropriate.
- In written comments, State agreed with the recommendation and noted that it is currently awaiting final modernization guidance from OMB. Upon publication of OMB's guidance, it plans to work with OMB to develop detailed plans for modernization. State's comments are reprinted in appendix XI. The department also provided technical comments, which we have incorporated in the report as appropriate.
- In comments provided via e-mail on May 12, 2016, an official from Treasury's Office of the CIO stated that the department had no comments on the draft report.
- In comments provided via e-mail on May 6, 2016, an official from Transportation's Office of the Secretary stated that the department

concurred with the draft findings and recommendations and had no additional comments on the report.

- In written comments, VA concurred with our recommendation and stated that it launched a new office in April 2016 that will provide lifecycle management oversight for portfolios of systems. In addition, it stated that the department is planning to retire two high-risk, COBOL-based systems (Personnel and Accounting Integrated Data and Benefits Delivery Network) in 2017 and 2018, respectively. VA's comments are reprinted in appendix XII.
- In written comments, SSA stated that it agreed with our recommendation and that it has already initiated numerous activities to modernize or replace legacy systems. SSA's comments are reprinted in appendix XIII.

We are sending copies of this report to interested congressional committees; the Secretaries of Agriculture, Commerce, Defense, Energy, Health and Human Services, Homeland Security, State, the Treasury, Transportation, and Veterans Affairs; the U.S. Attorney General of the Department of Justice; the Commissioner of the Social Security Administration; the Director of the Office of Management and Budget and other interested parties. This report will also be available at no charge on our website at http://www.gao.gov.

If you or your staffs have any questions on matters discussed in this report, please contact me at (202) 512-9286 or pownerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix XIV.

David a. Pow

David A. Powner
Director
Information Technology Management Issues

Appendix I: Objectives, Scope and Methodology

Our objectives were to (1) assess the extent to which federal agencies have invested in operating and maintaining existing information technology (IT), (2) evaluate the oversight of at-risk legacy investments, and (3) assess the age and obsolescence of federal IT.

For our first objective, our review included the Office of Management and Budget (OMB) and the 26 agencies that report to OMB's IT Dashboard.[1] For all three objectives, to identify specific reasons for changes in spending and specific information on individual systems or investments, we focused on the 12 agencies with the highest planned IT spending for fiscal year 2015, given that these agencies make up over 90 percent of reported federal IT spending:

- Department of Agriculture,
- Department of Commerce,
- Department of Defense,
- Department of Energy,
- Department of Health and Human Services,
- Department of Homeland Security,
- Department of Justice,
- Department of State,
- Department of the Treasury,
- Department of Transportation,
- Department of Veterans Affairs, and
- Social Security Administration.

To assess the extent to which federal agencies have invested in operating and maintaining existing IT, we reviewed data reported to OMB as part of the budget process to determine operations and maintenance (O&M) spending for fiscal years 2010 through 2017. We analyzed that data to determine the extent to which spending had changed over those years. We also compared OMB's associated performance measure on

[1] The 26 agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; as well as the U.S. Army Corps of Engineers, Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Archives and Records Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

driving value in federal IT investments (the percent of IT spending that is on development, modernization, and enhancement (DME) activities or provisioned O&M services) to federal best practices.[2] To assess the cause of the changes in spending, we evaluated OMB budget data and interviewed officials at the 12 selected agencies and OMB.

To evaluate the oversight of at-risk legacy investments, we reviewed agency IT Dashboard data from the 12 selected agencies to identify investments in O&M that had been identified as being moderate to high risk. Specifically, we reviewed IT Dashboard data on O&M investments to identify those that were rated as moderate to high risk by the agency chief information officer (CIO). We reviewed agency documentation such as TechStat documentation and operational analyses that had been performed on the investments, as available. In addition, we interviewed agency officials to determine plans for replacing or modernizing the investments.

To assess the age and obsolescence of federal IT, we reviewed agency documentation associated with their legacy investments, such as operational analyses and enterprise architecture documents, and interviewed agency officials on the issues related to legacy investments. We also requested that agencies provide a list of their three oldest systems. In some cases, agencies reported that they do not track the ages of individual systems. In those cases, we requested that the agencies provide their three oldest IT investments. Agencies noted that these systems and investments may have components that are newer than their operational age. We also compared OMB and agencies' current practices with federal guidance, such as OMB's Circular No. A-11: *Preparation, Submission, and Execution of the Budget* and its associated supplement on capital assets, to determine whether OMB and agencies are adequately managing the age and obsolescence of federal IT. We then interviewed agency officials to confirm and obtain additional information on the systems or investments.

[2] Department of the Navy, Office of the Chief Information Officer, *Guide for Developing and Using Information Technology (IT) Performance Measurements* (Washington, D.C.: October 2001); and General Services Administration, Office of Governmentwide Policy, *Performance-Based Management: Eight Steps To Develop and Use Information Technology Performance Measures Effectively* (Washington, D.C.: 1996).

To select systems or investments to profile, we identified agencies' existing investments in O&M that were rated as medium or high risk by their agencies' CIO (from the previous objective on oversight). Since not all of our selected agencies had identified an at-risk O&M investment (the Departments of Defense, Justice, State, Transportation, and Veterans Affairs and the Social Security Administration did not), we also used the list of agency-identified oldest systems or investments. From the resulting list of systems and investments, we selected one system or investment per agency using the following factors: investment type (major or non-major), system or investment age, and risk level as of November 2015. In particular, we sought to have a mix of systems and investments that included both major and non-major investment types; a range of ages; and a range of risk ratings. We also reviewed agency documentation and interviewed agency officials on those profiled systems or investments.

To assess the reliability of the OMB budget data and IT Dashboard data, we reviewed related documentation, such as OMB guidance on budget preparation, capital planning, and IT Dashboard submissions. In addition, we corroborated with each agency that the data downloaded were accurate and reflected the data it had reported to OMB. We determined that the budget and IT Dashboard data were reliable for our purposes of reporting IT O&M spending and related information on O&M investments.

We conducted this performance audit from April 2015 to May 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Agency-Reported Spending on O&M

Table 8 provides the reported spending by agency on operations and maintenance (O&M) and the percentage of IT spending on O&M for fiscal years 2010 and 2015.

Table 8: Agency Spending on Operations and Maintenance (O&M) (in millions) and Percentage of IT Spending on O&M for Fiscal Years 2010 and 2015

Agency	2010 O&M (% of IT spending on O&M)	2015 O&M (% of IT spending on O&M)	Change in spending 2010 to 2015 (% of spending on O&M)
Department of Agriculture	$2,137.6 (82.4%)	$2,719.7 (89.0%)	$582.0 (6.6%)
Department of Commerce	1,525.5 (50.1)	1,413.0 (67.1)	-112.6 (17.0)[a]
Department of Defense	23,940.0 (63.4)	23,490.0 (77.2)	-450.3 (13.9)[b]
Department of Education	473.2 (58.3)	548.8 (77.8)	61.3 (19.5)
Department of Energy	1,691.1 (85.6)	1,387.5 (87.4)	-303.5 (1.8)
Department of Health and Human Services	4,905.8 (77.9)	9,194.5 (67.4)	4,288.7 (-10.5)
Department of Homeland Security	4,287.3 (66.6)	4,920.1 (83.2)	632.8 (16.6)
Department of Housing and Urban Development	335.4 (94.0)	284.7 (92.5)	-50.7 (-1.5)
Department of the Interior	830.8 (86.8)	947.6 (91.8)	116.8 (5.0)
Department of Justice	1,891.0 (66.6)	2,150.5 (81.2)	258.9 (14.6)
Department of Labor	456.5 (78.3)	537.3 (80.5)	80.9 (2.2)
Department of State	1,269.5 (88.3)	1,378.5 (87.4)	109.0 (-0.9)
Department of Transportation	1,291.9 (43.6)	1,653.2 (50.4)	361.3 (6.8)
Department of the Treasury	2,675.2 (84.7)	2,886.6 (76.6)	211.4 (-8.1)
Department of Veterans Affairs	2,686.6 (80.4)	3,479.3 (82.9)	792.8 (2.5)
Environmental Protection Agency	383.4 (83.1)	355.0 (90.1)	-28.4 (7.0)
General Services Administration	485.0 (77.5)	465.3 (71.6)	-19.7 (-5.9)
National Aeronautics and Space Administration	1,865.4 (90.1)	1,265.2 (91.3)	-600.2 (1.2)
National Archives and Records Administration	69.5 (49.4)	64.8 (58.7)	-4.7 (9.3)
National Science Foundation	78.8 (83.1)	93.9 (84.1)	15.0 (1.0)
Nuclear Regulatory Commission	131.6 (83.0)	158.5 (88.7)	27.0 (5.6)
Office of Personnel Management	60.8 (73.9)	71.4 (57.6)	10.5 (-16.3)
Small Business Administration	83.2 (66.9)	80.0 (78.0)	-3.2 (11.1)
Social Security Administration	811.0 (49.9)	1,103.0 (59.3)	292.0 (9.4)
U.S. Agency for International Development	111.9 (59.4)	103.3 (78.6)	-8.6 (19.1)
U.S. Army Corps of Engineers	479.1 (95.8)	440.7 (99.3)	-38.4 (3.5)
Totals	**$54,958.0 (68.1)**	**$60,177.9 (76.1)**	**$6,220.0 (8.0)**

Source: GAO analysis of data reported by agencies to the Office of Management and Budget's IT Dashboard. | GAO-16-468

[a] Agency officials stated that the increase in O&M spending was due to the reclassification of satellite ground systems that are no longer considered an IT investment. As previously reported, we disagree

with these reclassifications and believe that they run contrary to the Clinger-Cohen Act of 1996, which specifies requirements for the management of IT.

[b] According to Department of Defense officials, the department's fiscal year 2010 IT expenditures reported to the IT Dashboard includes both classified and unclassified spending, whereas its fiscal year 2011 to 2017 expenditures only include unclassified spending.

Appendix III: Bureaus Reporting Spending Less than 10 Percent on Development, Modernization, and Enhancement

Table 9 lists the 51 federal bureaus which reported spending less than 10 percent of their IT funds on development, modernization, and enhancement in fiscal year 2015.

Table 9: Federal Bureaus Which Reported Spending Less than 10 Percent of their IT Funds on Development, Modernization, and Enhancement (DME) in Fiscal Years 2015

Agency	Bureau	Percent spent on DME
Department of Agriculture	Agricultural Research Service	9.24%
	Executive Operations	0%
	Forest Service	0.86%
	National Agricultural Statistics Service	6.7%
	Office of Chief Financial Officer	0%
	Office of Chief Information Officer	4.66%
	Office of Inspector General	0%
	Office of the General Counsel	0%
Department of Commerce	Department of Commerce[a]	8.06%
	Economic Development Administration	0%
	Economics and Statistics Administration	8.38%
	National Institute of Standards and Technology	0%
Department of Energy	Departmental Administration	8.78%
	Energy Programs	9.50%
	Environmental and Other Defense Activities	4.82%
Department of Health and Human Services	Administration for Children and Families[b]	4.07%
	Agency for Healthcare Research and Quality	8.25%
	Indian Health Service	8.30%
Department of Homeland Security	Department of Homeland Security[a]	9.41%
	Federal Emergency Management Agency	5.17%
	Federal Law Enforcement Training Center	1.82%
	Office of the Inspector General	0%
	Transportation Security Administration	5.7%
	U.S. Customs and Border Protection	9.43%
Department of Housing and Urban Development	Department of Housing and Urban Development[a]	7.59%
	Management and Administration	0%
Department of Justice	Federal Prison System	4.22%
	Office of Justice Programs	8.80%
	United States Parole Commission	0%

Agency	Bureau	Percent spent on DME
Department of Labor	Bureau of Labor Statistics	7.97%
	Employee Benefits Security Administration	0%
	Employment and Training Administration	8.95%
	Office of Federal Contract Compliance Programs	0%
	Office of Labor Management Standards	0%
	Office of Workers Compensation Programs	6.16%
	Wage and Hour Division	0%
Department of the Interior	Bureau of Land Management	9.86%
	Department of the Interior[a]	7.28%
	Office of Surface Mining Reclamation and Enforcement	5.09%
	Office of the Special Trustee for American Indians	2.82%
	United States Geological Survey	0.19%
Department of the Treasury	Alcohol and Tobacco Tax and Trade Bureau	0%
	Comptroller of the Currency	0%
	Financial Crimes Enforcement Network	3.87%
	United States Mint	2.64%
Department of Transportation	Federal Railroad Administration	6.85%
	Maritime Administration	3.01%
	Office of Inspector General	0%
Environmental Protection Agency	Environmental Protection Agency	9.92%
National Aeronautics and Space Administration	National Aeronautics and Space Administration[a]	8.7%
U.S. Army Corps of Engineers	Corps of Engineers-Civil Works	0.75%

Source: GAO analysis of IT Dashboard data. | GAO-16-468

[a] Some agencies have bureaus named the same as the agency, but these are one of several bureaus and do not necessarily include all of that particular agency's investments.

[b] According to the Department of Health and Human Services, 89 percent ($593 million) of the Administration for Children and Families is allocated to grants to state and local IT investments. Out of the remaining funds, the Administration for Children and Families spends 35.6 percent of its IT budget on DME activities.

Appendix IV: Agency-Reported Oldest Systems or Investments

As part of this review, we requested that agencies provide a list of their three oldest systems. In some cases, agencies reported that they do not track the ages of individual systems, and as a result, we requested that the agency provide their 3 oldest IT investments and their approximate age. Table 10 provides a listing these systems or investments, as reported by agencies.

Table 10: Agency-Reported Oldest Investments or Systems

Agency	Investment/system	Year operational	Approximate age
Department of Agriculture	Forest Service Automated Timber Sale Accounting	1980	36
	Farm Service Agency Consolidated General Sales Manager #107	1982	34
	Forest Service Computer Base	1983	33
Department of Commerce	National Weather Service Dissemination Systems	1970	46
	National Data Buoy Center Ocean Observing System of Systems	1970	46
	National Oceanic and Atmospheric Administration Office of the Chief Information Officer Financial Management IT Operations	1978	38
Department of Homeland Security	Immigration and Customs Enforcement Hiring Tracking Systems	1977	39
	Customs and Border Protection Computerized Aircraft Reporting and Material Control	1979	37
	Federal Emergency Management Agency United States Fire Administration Systems	1982	34
Department of Defense	Strategic Automated Command and Control System	1963	53
	Compass	1964	52
	AN/WLR-9B(V) Series	1971	45
Department of Energy[a]	Office of Environmental Management Savannah River Telecommunications Networks – Telephone System	1989	27
	Associate Under Secretary for Environment, Health, Safety and Security Enterprise Personnel Security Systems	1990s	~26
	Associate Under Secretary for Environment, Health, Safety and Security Enterprise Health and Safety Reporting Systems	1990s	~26
	Associate Under Secretary for Environment, Health, Safety and Security Enterprise Security Program Systems	1990s	~26
Department of Health and Human Services	Centers for Medicare and Medicaid Services Medicare Beneficiary Enrollment Data Management	1984	32
	Indian Health Service Resource and Patient Management System - Maintenance and Enhancements	1984	32
	Substance Abuse and Mental Health Services Administration - Center for Behavioral Health Statistics and Quality National Survey on Drug Use and Health	1984	32

Agency	Investment/system	Year operational	Approximate age
Department of Justice	Federal Bureau of Prisons SENTRY	1981	35
	Federal Bureau of Prisons BOPNet	1981	35
	Federal Bureau of Investigation Digital Collection	1993	23
Social Security Administration	Title II Systems	1985	31
	FALCON Data Entry System	1991	25
	Supplemental Security Income Record Maintenance System	1992	24
Department of State	Diversity Immigrant Visa Information System	1994	22
	Immigrant Visa Information System	1994	22
	Non-Immigrant Visa System	1995	21
Department of Transportation	Hazardous Materials Information System at Pipeline and Hazardous Materials Safety Administration	1970s	~46
	Financial Management System of Saint Lawrence Seaway Development Corporation	1986	30
	2001 TranStats (Bureau of Transportation Statistics)	2001	15
Department of the Treasury	Individual Master File	1960s	~56
	Business Master File non-major	1960s	~56
	Integrated Data Retrieval System	1973	43
Department of Veterans Affairs	Personnel and Accounting Integrated Data	1963	53
	Benefits Delivery Network	1965	51
	Electronic Health Record VistA	1981	35

Source: GAO analysis of agency documentation and interviews | GAO-16-468

Notes: The systems and investments listed here may have components newer than the age listed.

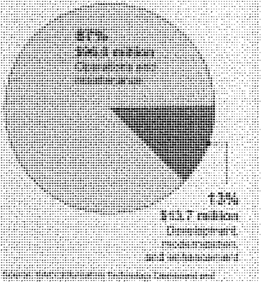
[a]The Department of Energy provided a list of multiple old investments. Because three were tied for second oldest, we include four investments here.

Appendix V: Profiles of 12 Legacy Investments or Systems

We selected one system or investment per agency using a combination of factors including investment type (major or non-major), system or investment age, and risk level as of November 2015. In particular, we sought to have a mix of systems and investments that included both major and non-major investment types, a range of ages, and a range of risk ratings.

Contractor Business Financial and Administrative Systems

Department of Energy
Number of users: [illegible] users
Investment start date: [illegible]
Age: [illegible] years
Investment anticipated end date: None
Fiscal year 2016 funding: [illegible] million
Total estimated life-cycle costs (through fiscal year 2016): [illegible] million
Development costs: $13.7 million
Operations and maintenance costs: [illegible] million
Plans for retirement or modernization: None



Source: GAO analysis of Information Technology Dashboard and agency documentation. | GAO-16-468

The Contractor Business Financial and Administrative Systems investment is intended to provide business and administrative systems for the Department of Energy's (Energy) Savannah River Site's[1] management and operating contractor,[2] liquid waste contractor, and the site security contractor to manage human resources (including payroll, benefits, and retirement for 13,000 employees and pensioners), transparent financial reporting to Energy, supply chain, and project management.

The investment is a commercial off-the-shelf system that runs on Windows and Unix servers using Oracle's PeopleSoft applications. Specifically, the investment uses the PeopleSoft Supply Chain Management and PeopleSoft Financials modules. According to an agency official in Savannah River Operations, the vendors still support all of the hardware and software used by this investment.

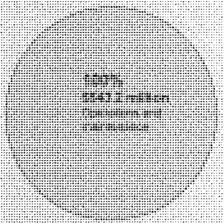
The agency is not currently planning future modernization activity because the investment has gone through several updates in the past, with the last allowing the retirement of 16 associated legacy applications in 2011 and retired two mainframe systems. The officials stated that there is no projected end of life date, and they plan to continue to maintain and use the system.

[1] The Savannah River Site is an Energy industrial complex responsible for the environmental stewardship, environmental cleanup, waste management, and disposition of nuclear materials.

[2] Management and operating contracts are agreements under which the government contracts for the operation, maintenance, or support, on its behalf, of a government-owned or -controlled research, development, special production, or testing establishment wholly or principally devoted to one or more of the major programs of the contracting federal agency. Federal Acquisition Regulation (FAR), 48 C.F.R. § 17.601.

Core Accounting System Suite

Department of Homeland Security—U.S. Coast Guard
Number of users: 14,000 Coast Guard users and also services the Transportation Security Administration
Investment start date: [illegible]
Age: [illegible] years
Investment anticipated end date: 2018
Fiscal year 2016 funding: [illegible] million
Total estimated life-cycle costs: [illegible] million
Development costs: $0
Operations and maintenance costs: [illegible] million
Plans for retirement or modernization: Agency plans to transition to federal shared services in fiscal year 2018



Source: GAO analysis of information technology Dashboard and agency documentation. | GAO-16-468

The Core Accounting System (CAS) Suite is the primary financial management system for the U.S. Coast Guard (USCG) and, as a shared service, the financial management system for the Transportation Security Administration (TSA) and the Domestic Nuclear Detection Office (DNDO). CAS is a set of several applications that assist the agencies in several areas, including accounts receivable, accounts payable, purchasing, asset management, procurement, and document imaging and processing.

According to the investment's operational analysis document, CAS relies on outdated and heavily customized Oracle software and has become expensive to support. Specifically, it uses a version of Oracle Federal Financials software that was first available in 2004 and the extended vendor support for the software ended in November 2013. Further, it relies on Windows 2003 servers and any changes would require recoding of many functions within the CAS suite.

The agency plans to pursue using other shared services to provide its financial management services and, therefore, began the Financial Management Service Improvement Initiative to migrate the services from CAS to the Department of the Interior's shared service offering for financial management. In August 2014, the agencies agreed to a staggered transition of these services, with DNDO transitioning in fiscal year 2016, TSA in fiscal year 2017, and USCG in fiscal year 2018. Until the migration is complete and CAS can be decommissioned, USCG plans to resolve emergent issues and maintain applications. In the meantime, due to the costs associated with implementing a full fix and the impending transition to shared services, USCG has accepted the security risks associated with its legacy software.

Diversity Visa Information System

Department of State

Number of users: Approximately 30 to 40 consular center staff and 55,000 applicants annually

System start date: early 1990s

Age: Approximately 26 years

System anticipated end date: 2020

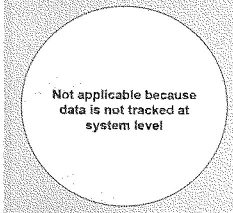
Fiscal year 2016 funding: about $164,000

Total estimated life-cycle costs: $2.4 million

Development costs: Not tracked at system level

Operations and maintenance costs: Not tracked at system level

Plans for retirement or modernization: Plans to replace with ConsularOne at an unknown time.



Source: GAO (agency documentation). | GAO-16-468

The Diversity Visa Information System (DVIS) is an electronic case management system used by approximately 30 federal employees and contractor staff working at the Department of State's (State) Kentucky Consular Center to track and validate application information submitted by foreign nationals under the Diversity Visa immigration program.[3]

The DVIS interface software, PowerBuilder, is no longer supported by the vendor. According to State officials, the main challenges in maintaining DVIS's aging technology are related to information security and infrastructure concerns.

In 2013, State initiated an effort to replace numerous legacy systems, including DVIS. As a part of this effort, State plans to replace DVIS's functionality with a project called ConsularOne. According to State officials, the replacement effort is to begin in October 2018 and they plan to retire DVIS when appropriate. In the meantime, the department plans to upgrade the unsupported software to a new version, which is also not supported.

[3] The Diversity Visa Program is provided by law to promote immigration from countries with historically low rates of immigration to the United States. The program creates an internet based lottery and randomly selects individuals from a pool of eligible entrants and qualifies them to apply for immigrant visas.

Hazardous Materials Information System

Department of Transportation—Pipeline and Hazardous Materials Safety Administration

Number of users: [illegible] federal users, [illegible] active hazardous materials facilities, [illegible] active pipeline operators, and several million [illegible]

Investment start date: 1970s

Age: about 41 years

Investment anticipated end date: 2018

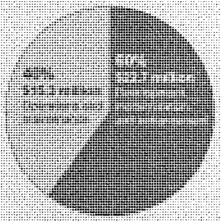
Fiscal year 2015 funding: [illegible]

Total estimated life-cycle costs: $36.0 million

Development costs: $22.7 million

Operations and maintenance costs: $13.3 million

Plans for retirement or modernization: Developing new system to replace legacy modules, and plan to retire the legacy modules by the end of fiscal year 2018



Source: [illegible] | GAO-16-468

The Department of Transportation's (DOT) Hazardous Materials Information System maintains and provides access to comprehensive information on hazardous materials incidents, exemptions and approvals, enforcement actions, and other elements that support the regulatory program. The system consists of five modules that register carriers and shippers, document incidents involving hazardous materials, issue special permits, facilitate approvals and exemptions pertaining to safety regulations, and document standards.

Officials from Pipeline and Hazardous Material Safety's Office of the Chief Information Officer stated that software applications and processes used by the system have become outdated and costly to maintain.[4] For example, the system uses Microsoft.NET[5] and Classic Active Server Pages.[6] Officials stated that costs have increased due to maintaining the personnel with the knowledge to use these older applications. In particular, the costly applications include those for scanning, imaging, and documentation management. Further, these applications are compartmentalized, so data is duplicated and not integrated. Finally, the system uses an application that is no longer supported by the manufacturer, which can cause security risks, among other issues. Specifically, the system uses Kofax Indicius software to perform optical character recognition on scanned hazardous materials incident reports; the software was no longer supported by the vendor, as of December 2014.

DOT is in the process of updating the functions performed by the system. The new system's modules are intended to be integrated, automated, and improve efficiency, effectiveness, and data quality. Further, the unsupported application is planned to be eliminated. While DOT does not have dates for when individual legacy modules will be retired, officials stated that they plan to have all the legacy modules retired by the end of fiscal year 2018.

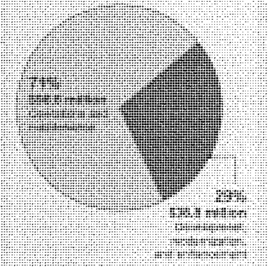
[4] According to Transportation, a photograph could not be provided due to security reasons.

[5] Microsoft.NET is a general purpose development platform that provides capabilities for building applications. It was first available in 2002.

[6] Active Server Pages enables web servers to dynamically generate web pages and create interactive web applications by using server-side scripting technology. Active Server Pages was first available in the late 1990s.

Individual Master File

Department of the Treasury—Internal Revenue Service
Number of users: Approximately 230 million tax accounts
Investment start date: 1960s
Age: Approximately 56 years
Investment anticipated end date: [illegible]
Fiscal year 2015 funding: [illegible]
Total estimated life-cycle costs: $135.4 million
Development costs: $38.9 million
Operations and maintenance costs: $96.5 million
Plans for retirement or modernization: Will be replaced by Customer Account Data Engine 2 at an unknown date.



Source: GAO analysis of agency documentation and data. | GAO-16-468

The Internal Revenue Service's (IRS), Individual Master File (IMF) is the authoritative data source for individual taxpayer accounts. Within IMF, accounts are updated, taxes are assessed, and refunds are generated as required during each tax filing period. Virtually all IRS information system applications and processes depend on output, directly or indirectly, from this data source.

IMF was written in an outdated assembly language code[7] and operates on a 2010 IBM z196/2817-m32 mainframe.[8] This has resulted in difficulty delivering technical capabilities addressing identify theft and refund fraud, among other things. In addition, there is a risk of inaccuracies and system failures due to complexity of managing dozens of systems synchronizing individual taxpayer data across multiple data files and databases, limitations in meeting normal financial requirements and security controls, and keeping pace with modern financial institutions.

IRS plans to address these issues by replacing IMF with the Customer Account Data Engine 2 (CADE 2) investment. The CADE 2 investment includes plans to re-engineer the IMF by: (1) applying modern programming languages, (2) establishing CADE 2 as the authoritative data source, and (3) implementing functionality to address the IRS financial material weakness. However, the replacement date is currently unknown. In addition, we have previously reported on IRS's difficulty in

[7] Assembly language code is a low-level computer language initially used in the 1950s. Programs written in assembly language are conservative of machine resources and quite fast; however, they are much more difficult to write and maintain than other languages. Programs written in assembly language are also typically able to run only on the make of computer for which they were originally developed.

[8] A large and very fast computer that can handle multiple tasks concurrently and to which other computers can be connected so that they can share facilities the mainframe provides. The term usually refers to hardware only, namely, main storage, execution circuitry, and peripheral units. According to Treasury, a photograph could not be provided due to security reasons.

delivering planned capabilities on time and on budget.[9] Further, a key phase of the replacement project was initially to be completed by March 2015, but IRS is currently planning to complete parts of this phase well into 2020. As a result, the agency will continue to maintain two separate systems until the replacement is complete.

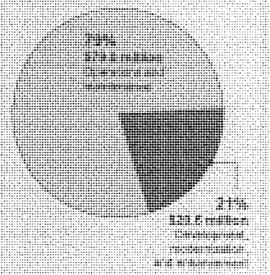
Medicare Appeals System

The Centers for Medicare and Medicaid Services' Medicare Appeals System is a case tracking system that is to facilitate maintenance and transfer of case specific data with regard to Medicare appeals through multiple levels of the appeal process. In addition, the system is to provide the capability to report on appeals data and enable more accurate and expedient responses to Congressional questions.

The system runs on a Solaris 10 operating system, last updated in February 2016, and uses commercial off-the-shelf systems for case management and reporting. According to the agency, the software is still supported by the vendors. The system has faced challenges due to the rapid growth in appeals processed each year, expanded use of settlements, and the increased interest in appeals data. This has resulted in an increased need for infrastructure changes, such as more storage, licenses, and processing capacity.

Agency officials stated that they do not have any plans to address these gaps and that doing so is contingent on funding. They also noted general plans to continuously update the system, but they too are contingent on receiving funding.

Department of Health and Human Services - Centers for Medicare and Medicaid Services
Number of users: [illegible] system users
Investment start date: [illegible]
Age: 11 years
Investment anticipated end date: none
Fiscal year 2016 funding: [illegible] million
Total estimated life-cycle costs (through fiscal year 2017): [illegible] million
Development costs: [illegible] million
Operations and maintenance costs: [illegible] million
Plans for retirement or modernization: The agency has general plans to continuously update the system.



Source: GAO (Information Technology Dashboard and agency documentation). | GAO-16-468

[9] GAO, *Information Technology: Management Needs to Address Reporting of IRS Investments' Cost, Schedule, and Scope Information*, GAO-15-297 (Washington, D.C.: Feb. 25, 2015).

National Weather Service Telecommunication Gateway

Department of Commerce—National Oceanic and Atmospheric Administration

Number of users: Thousands of users across the federal, state, and local levels, in addition to those in the international and academic communities

Investment start date: 1985

Age: 31 years

Investment anticipated end date: 2017

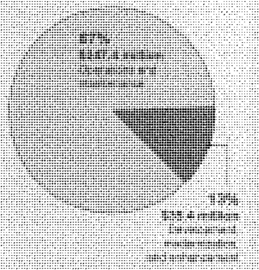
Fiscal year 2015 funding: $12.1 million

Total estimated life cycle costs: $282.8 million

Development costs: $35.4 million

Operations and maintenance costs: $247.4 million

Plans for retirement or modernization: Agency plans to retire the system in fiscal year 2017 and replace it with a new system.

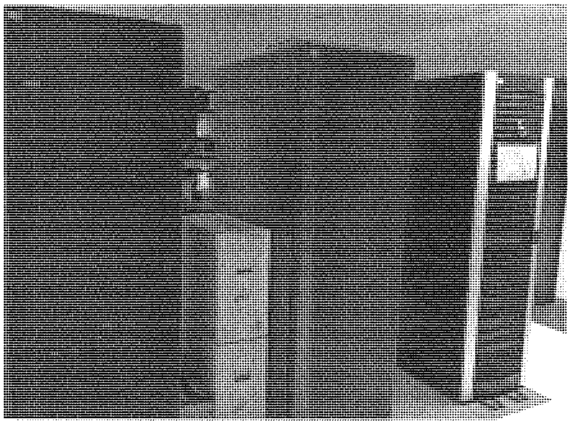


Source: GAO analysis of agency documentation. | GAO-16-468

The National Weather Service Telecommunication Gateway (NWSTG) system is operated by the National Oceanic and Atmospheric Administration, a component of the Department of Commerce. It is the nation's hub for the collection and distribution of weather data and products and provides national and global real-time exchange services using automated communications resources to collect and distribute a wide variety of environmental data such as observations, analysis, and forecast products. Thousands of customers worldwide use data distributed by the NWSTG and these data affect a wide range of economic and emergency management decisions.

Concerns with the system had been increasing because the investment faced risks and challenges associated with an aging and unsupportable infrastructure, limited backup capability, and un-scalable architecture to support future data volume collection and dissemination. In 2013, the agency upgraded its hardware and software to Power7 IBM servers and Unix operating systems (as depicted in the figure); however, NWSTG still lacks full backup capability for 26 percent of its functions.

Figure 7: National Weather Service Telecommunication Gateway Server



Source: GAO. | GAO-16-468

In fiscal year 2013, a major rearchitecture and redesign effort began which, according to Department of Commerce officials, will result in an entirely new dissemination architecture which will replace the NWSTG with an integrated system that is more capable, more reliable, and have 100 percent backup capability. According to officials, a detailed project plan to rearchitecture NWSTG is now being carried out and is scheduled to replace the NWSTG in early fiscal year 2017.

Personnel and Accounting Integrated Data

The Personnel and Accounting Integrated Data (PAID) system automates time and attendance for employees, timekeepers, payroll, and supervisors in the Department of Veterans Affairs (VA). The PAID software has three major modules: Time and Attendance, Employee Master Record Downloads, and Education Tracking.

According to VA officials, PAID is a 50-year old COBOL-based[10] system at the end of its life span. The system runs on IBM mainframes[11] and uses an IBM database. Officials stated the system is not user friendly and requires extensive training in order to use the system successfully. As a result, the cost of maintaining the personnel to manage the system is high.

VA officials stated that PAID is intended to be mostly replaced by Human Resources Information System Shared Service Center in 2017, which is to consolidate human resources IT functions and services to provide core human resources-related functions, such as benefits and compensation. However, the target solution is experiencing cost overruns of $14.8 million and VA officials stated that they will not be able to replace all of PAID's functions. The agency is currently working on a transition plan and will determine whether VA should find another solution for the missing functionality or continue to keep PAID running indefinitely.

Department of Veterans Affairs

Number of users: 2,900 system users across 200 human resources offices

System start date: 1963

Age: 53 years

System anticipated end date: 2017

Fiscal year 2016 funding: $6.7 million

Total estimated life-cycle costs: n/a, not tracked by system

Development costs: n/a, not tracked by system

Operations and maintenance costs: $6.6 million yearly

Plans for retirement or modernization: The system will mostly be replaced by the Human Resources Information System Shared Service Center, which will consolidate several IT services to provide core human resources-related functions.

Not applicable because data is not tracked at system level

Source: GAO (agency documentation). | GAO-16-468

[10] COBOL is a programming language developed in the late 1950s and early 1960s. The Gartner Group, a leading IT research and advisory company, has reported that organizations using COBOL should consider replacing the language, as procurement and operating costs will steadily rise, and because there is a decrease in people available with the proper skill sets.

[11] A large and very fast computer that can handle multiple tasks concurrently and to which other computers can be connected so that they can share facilities the mainframe provides. The term usually refers to hardware only, namely, main storage, execution circuitry, and peripheral units.

Resource Ordering and Status System

U.S. Department of Agriculture—U.S. Forest Service

Number of users: more than 600 federal, state, and local agencies; 30,000 user accounts

Investment start date: 1999

Age: 16 years

Investment anticipated end date: 2018

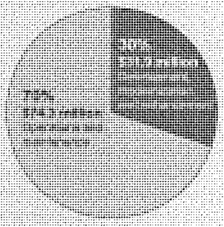
Fiscal year 2015 funding: $5.3 million

Total estimated life-cycle costs: $106.2 million

Development costs: $31.9 million

Operations and maintenance costs: $74.3 million

Plans for retirement or modernization: Being replaced in 2018.



Source: [illegible] | GAO-16-468

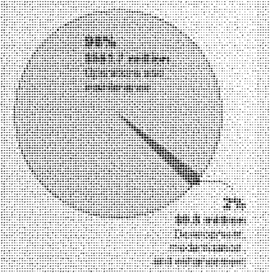
The U.S. Department of Agriculture's (USDA) U.S. Forest Service's Resource Ordering and Status System (ROSS) is used to mobilize and deploy a multitude of resources, including qualified individuals, teams, aircraft, equipment, and supplies to fight wildland fires and respond to all hazard incidents. The system supports the basic needs of the first responders and support personnel at an incident location by processing orders and replenishing supplies.

According to the U.S Forest Service, the technology used by ROSS is on the verge of technical obsolescence. Specifically, one of the applications ROSS uses is no longer supported by the vendor, creating vulnerability issues. In addition, in order to use the system, users must download client software onto their local computers, as opposed to accessing the system through the web.

In September 2015, the U.S. Forest Service issued a request for information for services to develop ROSS's replacement—Interagency Resources Ordering Capability. Additionally, in January 2016, Forest Service officials signed a charter to begin this project. Agency officials estimated that this effort will cost $14 million through fiscal year 2019 and the solution will go live in 2018.

Sentry

Department of Justice—Bureau of Prisons
Number of users: [illegible] Bureau of Prisons staff, [illegible] staff, and other federal agencies
Investment start date: [illegible]
Age: [illegible] years
Investment anticipated end date: [illegible]
Fiscal year 2016 funding: [illegible] million
Total estimated life-cycle costs: [illegible] million
Development costs: [illegible] million
Operations and maintenance costs: [illegible] million
Plans for retirement or modernization: [illegible]



Source: [illegible]

The Bureau of Prisons Sentry is a real-time information system comprised of various modules that are to enable the agency to maintain proper custody of persons committed to their custody. It provides information regarding security and custody levels, inmate program and work assignments, and other pertinent information about the inmate population. Sentry is used to process inmates at all phases of incarceration, including release, transfer, and sentence computation.

When Sentry was first deployed over 30 years ago, it was comprised of approximately 700 program routines written in COBOL[12] and ran on a mainframe platform with an Integrated Database Management System database. It became increasingly more difficult and expensive to maintain complex, highly-customized systems written in older programming languages. Sentry's entire platform—its mainframe operating system, transaction processing software, the system software, and the database software and system were recently updated in 2012 and uses Java and a new database. As part of this, the bureau migrated the older database, merged the legacy data into the newer database platform, and modified the COBOL programs to ensure compatibility with the new software and database. In addition, the legacy Sentry programs are now accessible via a web browser and use a relational database and both COBOL and Java programming languages.[13]

The bureau has plans for updating the user interface and integrating the data through September 2016. According to agency officials, there are no plans to replace Sentry, as the system is the main system used by the bureau.

[12] COBOL is a programming language developed in the late 1950s and early 1960s. The Gartner Group, a leading IT research and advisory company, has reported that organizations using COBOL should consider replacing the language, as procurement and operating costs will steadily rise, and because there is a decrease in people available with the proper skill sets.

[13] According to the agency, a photograph could not be provided due to security reasons.

Strategic Automated Command and Control System

Department of Defense—Air Force

Number of users: 175 users across command functions for intercontinental ballistic missiles, bombers, tankers, [illegible] sites, intelligence, surveillance, and reconnaissance platforms

Investment start date: [illegible]

Age: [illegible] years

Investment anticipated end date: [illegible]

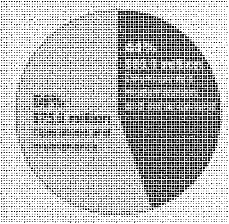
Fiscal year 2016 funding: [illegible] million

Total estimated life cycle costs: [illegible] million through [illegible]

Development costs: Approximately [illegible] million

Operations and maintenance costs: [illegible] million

Plans for retirement or modernization: Defense is initiating a [illegible] million full system replacement which is scheduled to be completed in fiscal year [illegible]



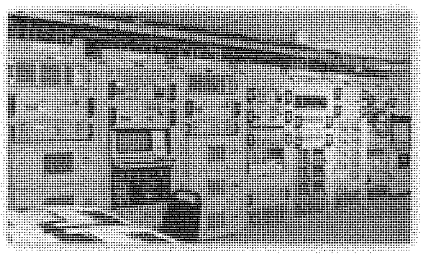
Source: [illegible] | GAO-16-468

The Strategic Automated Command and Control System is the Department of Defense's (Defense) dedicated high-speed data transmission, processing, and display system. The system coordinates the operational functions of the United States' nuclear forces, such as intercontinental ballistic missiles, nuclear bombers, and tanker support aircrafts, among others. For those in the nuclear command area, the system's primary function is to send and receive emergency action messages to nuclear forces.

According to Defense officials, the system is made up of technologies and equipment that are at the end of their useful lives. For example, the system is still running on an IBM Series/1 Computer, which is a 1970s computing system, and written in assembly language code.[14] It also uses 8-inch floppy disks, which are a 1970s-era storage device; and assembly programming code typically used in mainframes. Replacement parts for the system are difficult to find because they are now obsolete.

[14] Assembly language code is a low-level computer language. Programs written in assembly language are conservative of machine resources and quite fast; however, they are much more difficult to write and maintain than other languages. Programs written in assembly language are typically able to run only on the make of computer for which they are originally developed.

Figure 8: Department of Defense Air Force Strategic Automated Command and Control System



Source: U.S. Department of Defense. | GAO-16-468

As of March 2016, Defense is initiating a $60 million full system replacement which is scheduled to be completed in fiscal year 2020. In addition, Defense is also replacing some legacy functions in the near term—according to officials, there is a plan underway to replace the floppy disks with secure digital cards. This effort is underway and is expected to be completed in the fourth quarter of fiscal year 2017.

Title II Systems

Social Security Administration

Number of users: [illegible] 1,200+ field offices with [illegible] employees, as well as other federal agencies

System start date: [illegible]

Age: [illegible] years

Investment anticipated end date: None

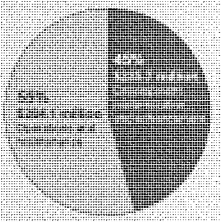
Fiscal year 2015 funding: [illegible] million

Total estimated life-cycle costs through fiscal year 2017: [illegible] million

Development costs: [illegible] million

Operations and maintenance costs: [illegible] million

Plans for retirement or modernization: Agency has ongoing modernization efforts



[illegible]

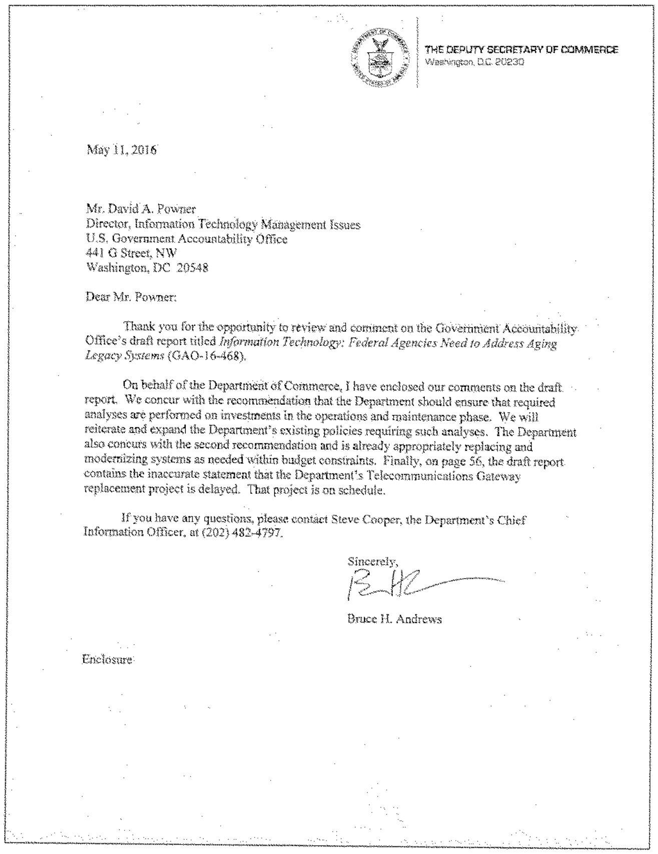
The Social Security Administration's (SSA) Title II investment includes the Title II system which determines retirement benefits eligibility and amounts, 162 subsystems, as well as several smaller IT improvement initiatives and projects. According to SSA officials, the Title II investment accomplished its goal to improve service delivery by eliminating antiquated Title II programs, reducing compartmentalized systems across the agency, and reducing maintenance costs through integration.

SSA officials stated that Title II is comprised of 162 subsystems and some are still written in COBOL.[15] These systems were also built in a compartmentalized structure by SSA, rather than contractors, because the agency determined that there were not commercial programs that could satisfy the agency's business needs and the volume of data needed. SSA officials stated that most of the employees who developed these systems are ready to retire and the agency will lose their collective knowledge. Officials further stated that training new employees to maintain the older systems takes a lot of time.

SSA does not have plans to retire the Title II system. Rather, the agency plans to continue to eliminate and replace Title II's older and more costly subsystems. Specifically, SSA currently is planning to retire four Title II subsystems, including a claims control system, and one that processes changes in earnings transactions. In addition, SSA has other efforts to modernize or consolidate Title II systems, such as its database management systems. To address the issues associated with losing knowledgeable employees, SSA officials stated that the agency has rehired retirees to work on the legacy systems.

[15] COBOL is a programming language developed in the late 1950s and early 1960s. The Gartner Group, a leading IT research and advisory company, has reported that organizations using COBOL should consider replacing the language, as procurement and operating costs will steadily rise, and because there is a decrease in people available with the proper skill sets.

Appendix VI: Comments from Department of Commerce



THE DEPUTY SECRETARY OF COMMERCE
Washington, D.C. 20230

May 11, 2016

Mr. David A. Powner
Director, Information Technology Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Powner:

Thank you for the opportunity to review and comment on the Government Accountability Office's draft report titled *Information Technology: Federal Agencies Need to Address Aging Legacy Systems* (GAO-16-468).

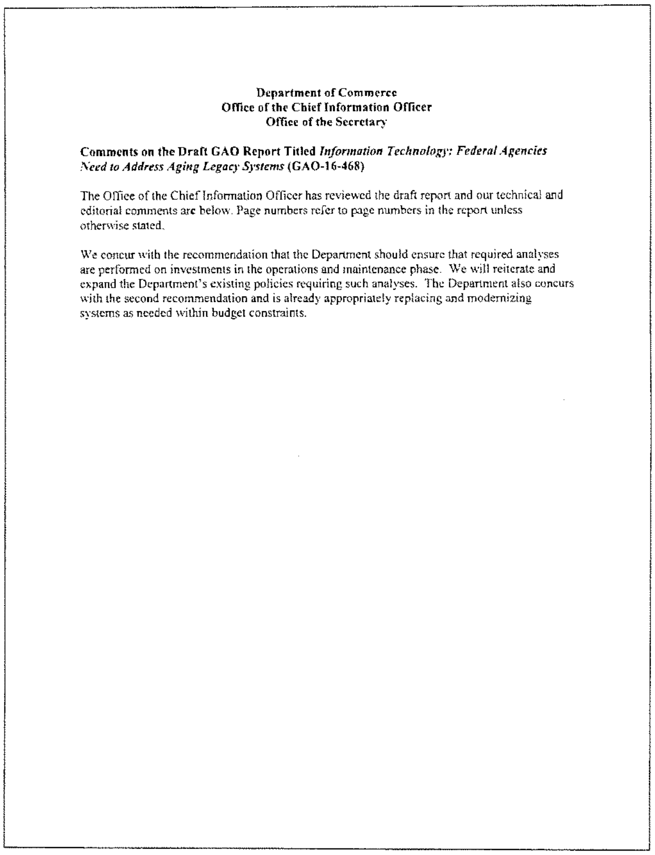
On behalf of the Department of Commerce, I have enclosed our comments on the draft report. We concur with the recommendation that the Department should ensure that required analyses are performed on investments in the operations and maintenance phase. We will reiterate and expand the Department's existing policies requiring such analyses. The Department also concurs with the second recommendation and is already appropriately replacing and modernizing systems as needed within budget constraints. Finally, on page 56, the draft report contains the inaccurate statement that the Department's Telecommunications Gateway replacement project is delayed. That project is on schedule.

If you have any questions, please contact Steve Cooper, the Department's Chief Information Officer, at (202) 482-4797.

Sincerely,

Bruce H. Andrews

Enclosure



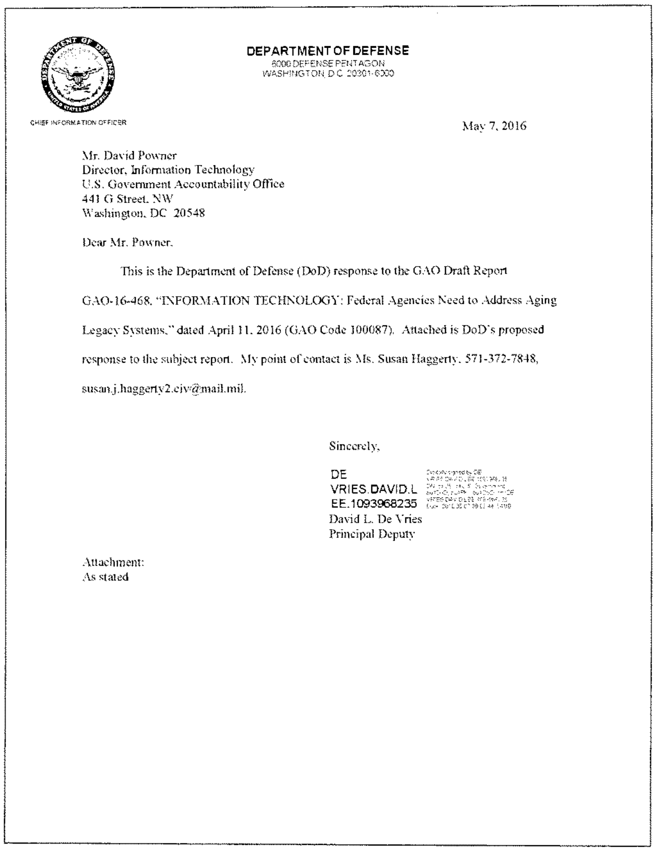
Department of Commerce
Office of the Chief Information Officer
Office of the Secretary

Comments on the Draft GAO Report Titled *Information Technology: Federal Agencies Need to Address Aging Legacy Systems* (GAO-16-468)

The Office of the Chief Information Officer has reviewed the draft report and our technical and editorial comments are below. Page numbers refer to page numbers in the report unless otherwise stated.

We concur with the recommendation that the Department should ensure that required analyses are performed on investments in the operations and maintenance phase. We will reiterate and expand the Department's existing policies requiring such analyses. The Department also concurs with the second recommendation and is already appropriately replacing and modernizing systems as needed within budget constraints.

Appendix VII: Comments from the Department of Defense



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

May 7, 2016

Mr. David Powner
Director, Information Technology
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

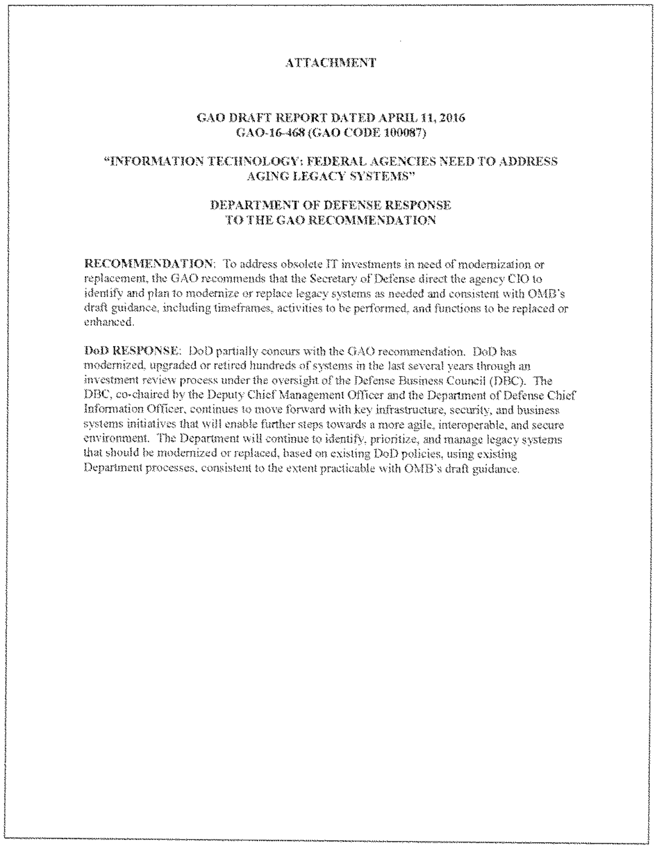
Dear Mr. Powner,

This is the Department of Defense (DoD) response to the GAO Draft Report GAO-16-468, "INFORMATION TECHNOLOGY: Federal Agencies Need to Address Aging Legacy Systems," dated April 11, 2016 (GAO Code 100087). Attached is DoD's proposed response to the subject report. My point of contact is Ms. Susan Haggerty, 571-372-7848, susan.j.haggerty2.civ@mail.mil.

Sincerely,

DE
VRIES.DAVID.L
EE.1093968235
Digitally signed by DE VRIES.DAVID.LEE.1093968235 [illegible]
David L. De Vries
Principal Deputy

Attachment:
As stated



ATTACHMENT

GAO DRAFT REPORT DATED APRIL 11, 2016
GAO-16-468 (GAO CODE 100087)

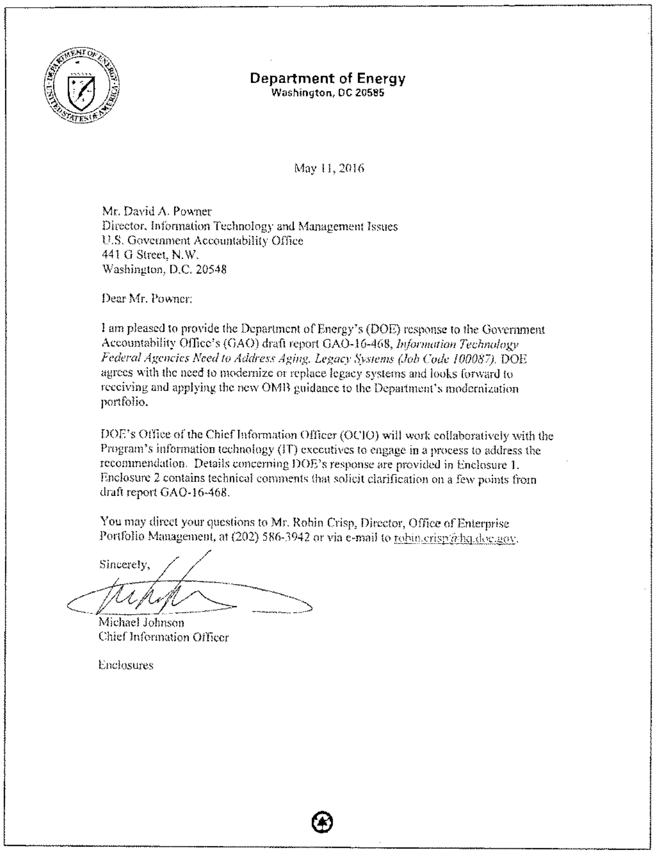
"INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS"

DEPARTMENT OF DEFENSE RESPONSE
TO THE GAO RECOMMENDATION

RECOMMENDATION: To address obsolete IT investments in need of modernization or replacement, the GAO recommends that the Secretary of Defense direct the agency CIO to identify and plan to modernize or replace legacy systems as needed and consistent with OMB's draft guidance, including timeframes, activities to be performed, and functions to be replaced or enhanced.

DoD RESPONSE: DoD partially concurs with the GAO recommendation. DoD has modernized, upgraded or retired hundreds of systems in the last several years through an investment review process under the oversight of the Defense Business Council (DBC). The DBC, co-chaired by the Deputy Chief Management Officer and the Department of Defense Chief Information Officer, continues to move forward with key infrastructure, security, and business systems initiatives that will enable further steps towards a more agile, interoperable, and secure environment. The Department will continue to identify, prioritize, and manage legacy systems that should be modernized or replaced, based on existing DoD policies, using existing Department processes, consistent to the extent practicable with OMB's draft guidance.

Appendix VIII: Comments from the Department of Energy



Department of Energy
Washington, DC 20585

May 11, 2016

Mr. David A. Powner
Director, Information Technology and Management Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Powner:

I am pleased to provide the Department of Energy's (DOE) response to the Government Accountability Office's (GAO) draft report GAO-16-468, *Information Technology Federal Agencies Need to Address Aging, Legacy Systems (Job Code 100087).* DOE agrees with the need to modernize or replace legacy systems and looks forward to receiving and applying the new OMB guidance to the Department's modernization portfolio.

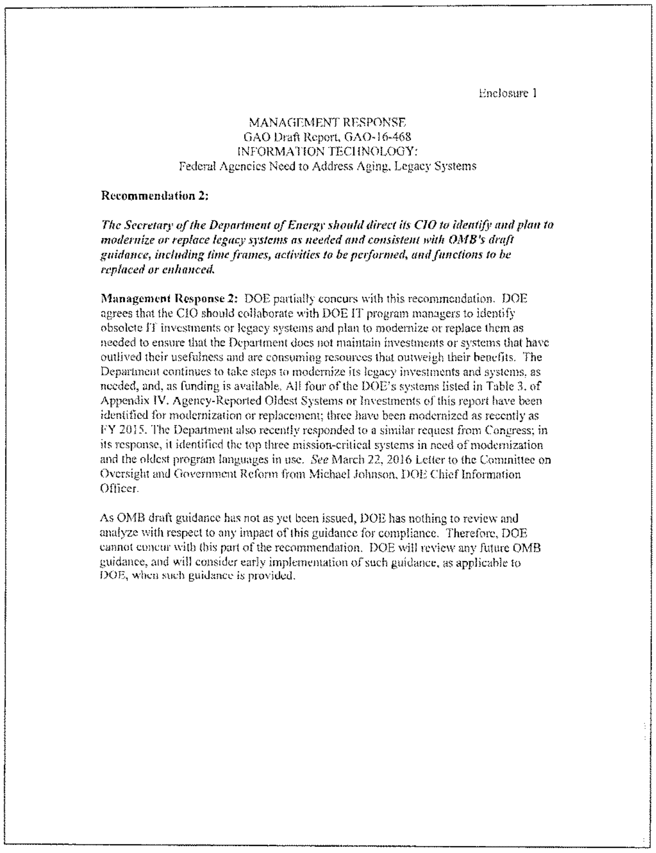
DOE's Office of the Chief Information Officer (OCIO) will work collaboratively with the Program's information technology (IT) executives to engage in a process to address the recommendation. Details concerning DOE's response are provided in Enclosure 1. Enclosure 2 contains technical comments that solicit clarification on a few points from draft report GAO-16-468.

You may direct your questions to Mr. Robin Crisp, Director, Office of Enterprise Portfolio Management, at (202) 586-3942 or via e-mail to robin.crisp@hq.doe.gov.

Sincerely,

Michael Johnson
Chief Information Officer

Enclosures



Enclosure 1

MANAGEMENT RESPONSE
GAO Draft Report, GAO-16-468
INFORMATION TECHNOLOGY:
Federal Agencies Need to Address Aging, Legacy Systems

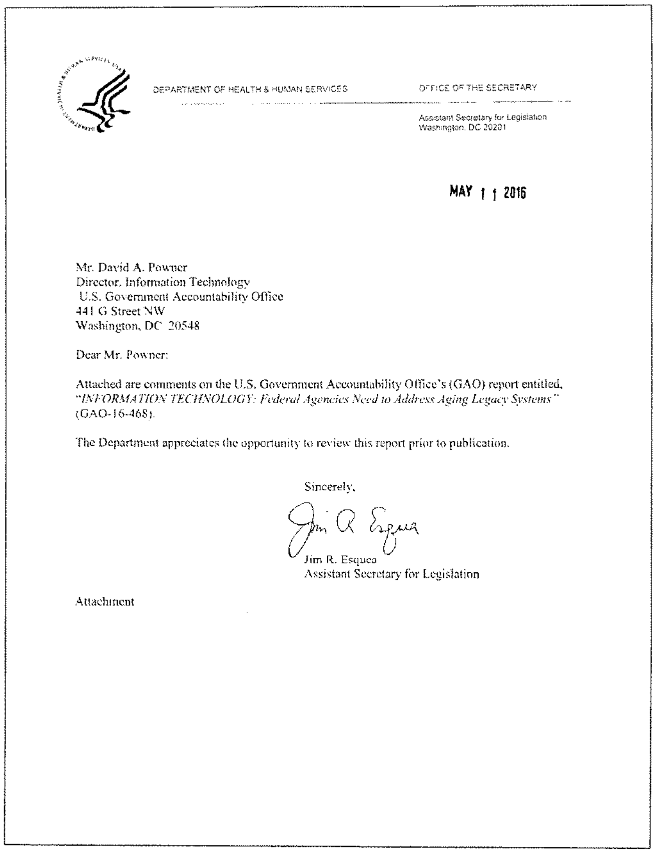
Recommendation 2:

The Secretary of the Department of Energy should direct its CIO to identify and plan to modernize or replace legacy systems as needed and consistent with OMB's draft guidance, including time frames, activities to be performed, and functions to be replaced or enhanced.

Management Response 2: DOE partially concurs with this recommendation. DOE agrees that the CIO should collaborate with DOE IT program managers to identify obsolete IT investments or legacy systems and plan to modernize or replace them as needed to ensure that the Department does not maintain investments or systems that have outlived their usefulness and are consuming resources that outweigh their benefits. The Department continues to take steps to modernize its legacy investments and systems, as needed, and, as funding is available. All four of the DOE's systems listed in Table 3. of Appendix IV. Agency-Reported Oldest Systems or Investments of this report have been identified for modernization or replacement; three have been modernized as recently as FY 2015. The Department also recently responded to a similar request from Congress; in its response, it identified the top three mission-critical systems in need of modernization and the oldest program languages in use. *See* March 22, 2016 Letter to the Committee on Oversight and Government Reform from Michael Johnson, DOE Chief Information Officer.

As OMB draft guidance has not as yet been issued, DOE has nothing to review and analyze with respect to any impact of this guidance for compliance. Therefore, DOE cannot concur with this part of the recommendation. DOE will review any future OMB guidance, and will consider early implementation of such guidance, as applicable to DOE, when such guidance is provided.

Appendix IX: Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

MAY 1 1 2016

Mr. David A. Powner
Director, Information Technology
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Powner:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "*INFORMATION TECHNOLOGY: Federal Agencies Need to Address Aging Legacy Systems*" (GAO-16-468).

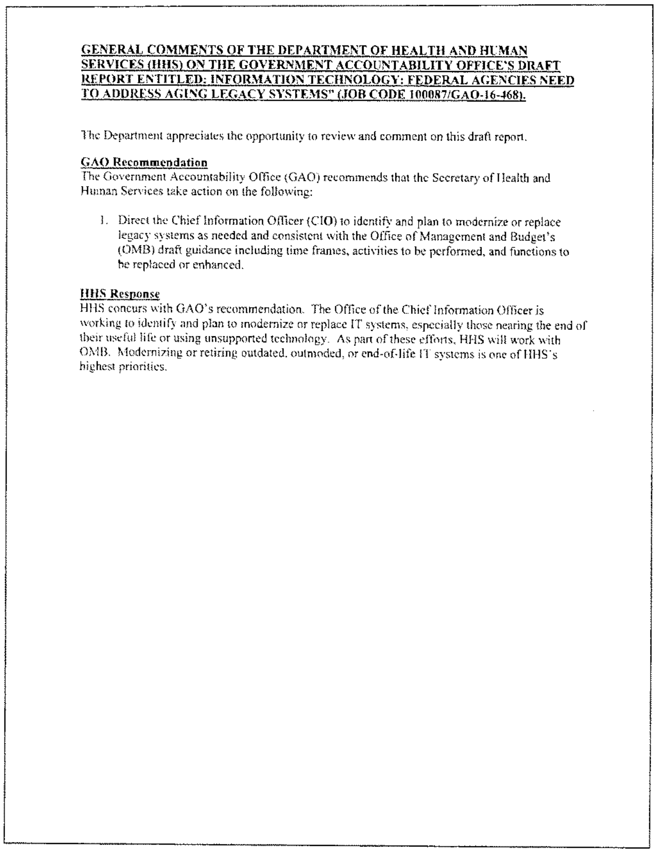
The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Jim R. Esquea

Jim R. Esquea
Assistant Secretary for Legislation

Attachment



GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED: INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS" (JOB CODE 100087/GAO-16-468).

The Department appreciates the opportunity to review and comment on this draft report.

GAO Recommendation

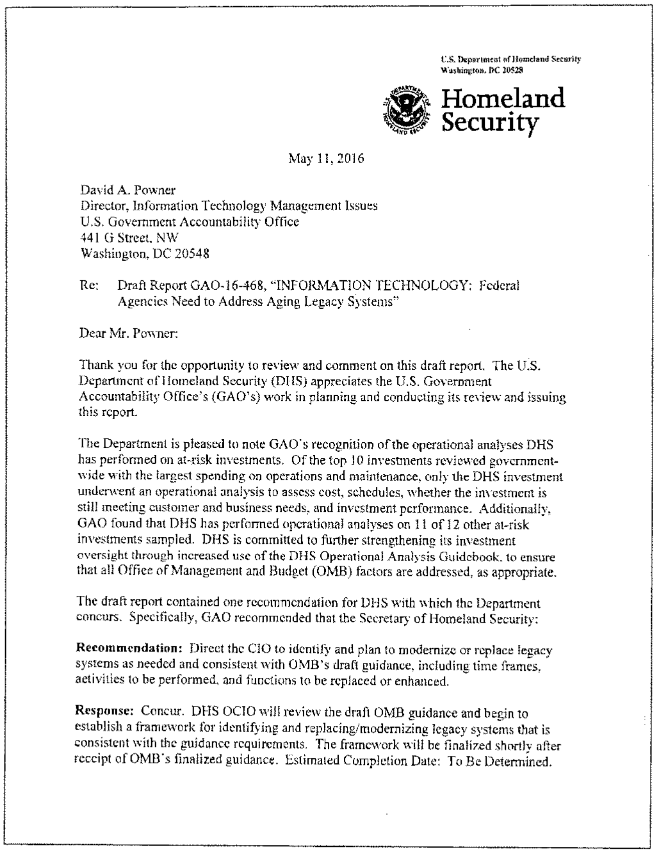
The Government Accountability Office (GAO) recommends that the Secretary of Health and Human Services take action on the following:

1. Direct the Chief Information Officer (CIO) to identify and plan to modernize or replace legacy systems as needed and consistent with the Office of Management and Budget's (OMB) draft guidance including time frames, activities to be performed, and functions to be replaced or enhanced.

HHS Response

HHS concurs with GAO's recommendation. The Office of the Chief Information Officer is working to identify and plan to modernize or replace IT systems, especially those nearing the end of their useful life or using unsupported technology. As part of these efforts, HHS will work with OMB. Modernizing or retiring outdated, outmoded, or end-of-life IT systems is one of HHS's highest priorities.

Appendix X: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

May 11, 2016

David A. Powner
Director, Information Technology Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO-16-468, "INFORMATION TECHNOLOGY: Federal Agencies Need to Address Aging Legacy Systems"

Dear Mr. Powner:

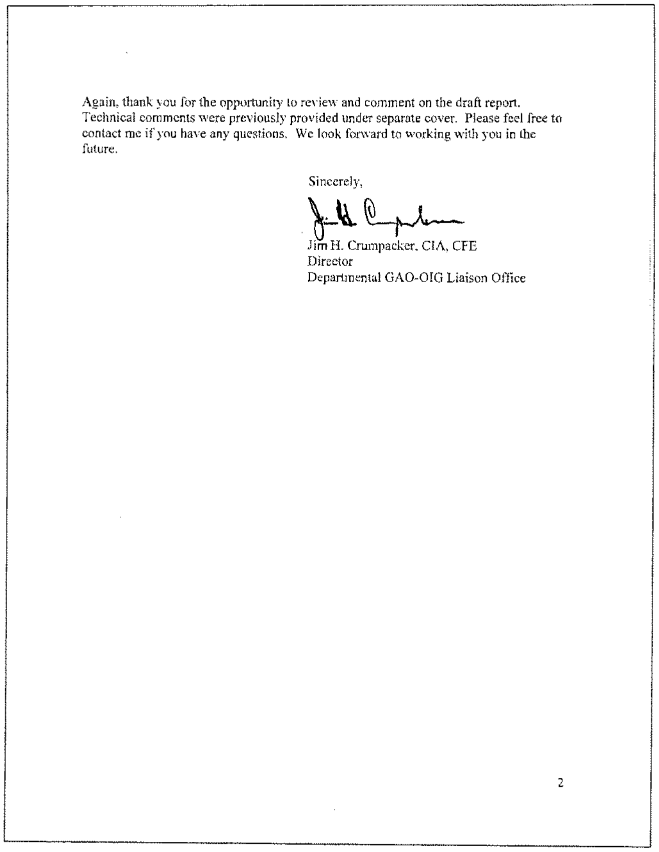
Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition of the operational analyses DHS has performed on at-risk investments. Of the top 10 investments reviewed government-wide with the largest spending on operations and maintenance, only the DHS investment underwent an operational analysis to assess cost, schedules, whether the investment is still meeting customer and business needs, and investment performance. Additionally, GAO found that DHS has performed operational analyses on 11 of 12 other at-risk investments sampled. DHS is committed to further strengthening its investment oversight through increased use of the DHS Operational Analysis Guidebook, to ensure that all Office of Management and Budget (OMB) factors are addressed, as appropriate.

The draft report contained one recommendation for DHS with which the Department concurs. Specifically, GAO recommended that the Secretary of Homeland Security:

Recommendation: Direct the CIO to identify and plan to modernize or replace legacy systems as needed and consistent with OMB's draft guidance, including time frames, activities to be performed, and functions to be replaced or enhanced.

Response: Concur. DHS OCIO will review the draft OMB guidance and begin to establish a framework for identifying and replacing/modernizing legacy systems that is consistent with the guidance requirements. The framework will be finalized shortly after receipt of OMB's finalized guidance. Estimated Completion Date: To Be Determined.

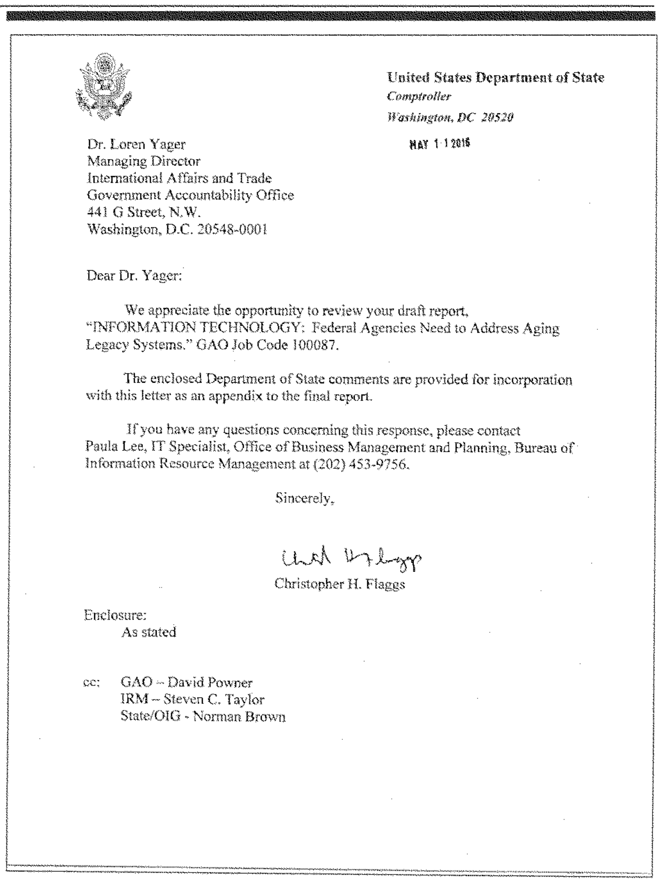


Again, thank you for the opportunity to review and comment on the draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Appendix XI: Comments from the Department of State



United States Department of State
Comptroller
Washington, DC 20520

MAY 1 1 2016

Dr. Loren Yager
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Dr. Yager:

We appreciate the opportunity to review your draft report, "INFORMATION TECHNOLOGY: Federal Agencies Need to Address Aging Legacy Systems." GAO Job Code 100087.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

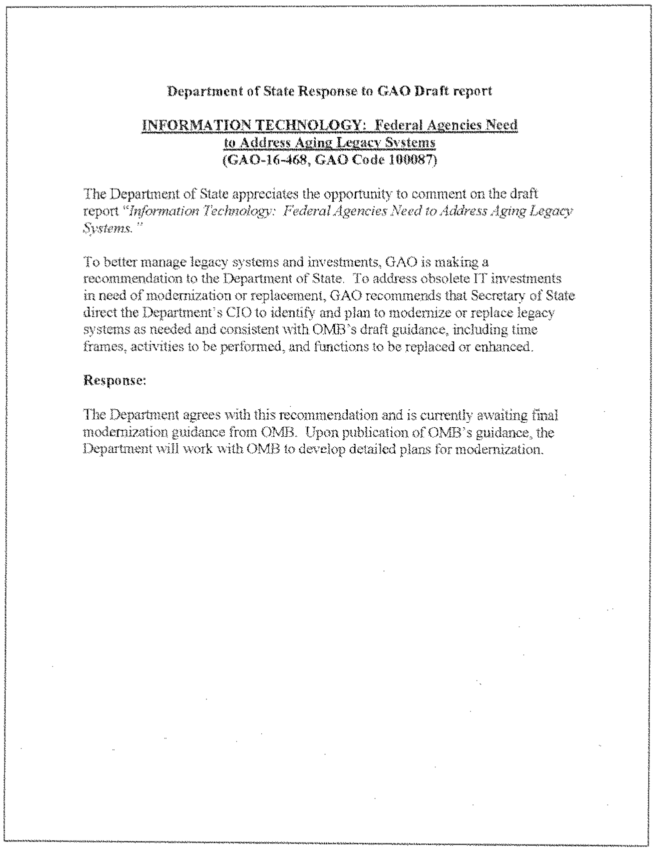
If you have any questions concerning this response, please contact Paula Lee, IT Specialist, Office of Business Management and Planning, Bureau of Information Resource Management at (202) 453-9756.

Sincerely,

Christopher H. Flaggs

Enclosure:
As stated

cc: GAO – David Powner
IRM – Steven C. Taylor
State/OIG - Norman Brown



Department of State Response to GAO Draft report

INFORMATION TECHNOLOGY: Federal Agencies Need to Address Aging Legacy Systems
(GAO-16-468, GAO Code 100087)

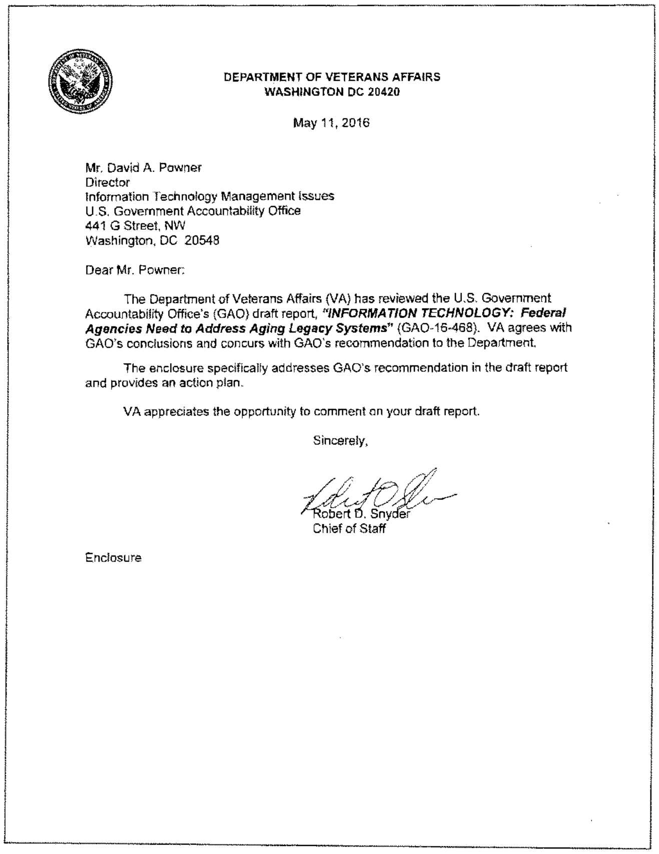
The Department of State appreciates the opportunity to comment on the draft report *"Information Technology: Federal Agencies Need to Address Aging Legacy Systems."*

To better manage legacy systems and investments, GAO is making a recommendation to the Department of State. To address obsolete IT investments in need of modernization or replacement, GAO recommends that Secretary of State direct the Department's CIO to identify and plan to modernize or replace legacy systems as needed and consistent with OMB's draft guidance, including time frames, activities to be performed, and functions to be replaced or enhanced.

Response:

The Department agrees with this recommendation and is currently awaiting final modernization guidance from OMB. Upon publication of OMB's guidance, the Department will work with OMB to develop detailed plans for modernization.

Appendix XII: Comments from the Department of Veterans Affairs



DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON DC 20420

May 11, 2016

Mr. David A. Powner
Director
Information Technology Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Powner:

The Department of Veterans Affairs (VA) has reviewed the U.S. Government Accountability Office's (GAO) draft report, ***"INFORMATION TECHNOLOGY: Federal Agencies Need to Address Aging Legacy Systems"*** (GAO-16-468). VA agrees with GAO's conclusions and concurs with GAO's recommendation to the Department.

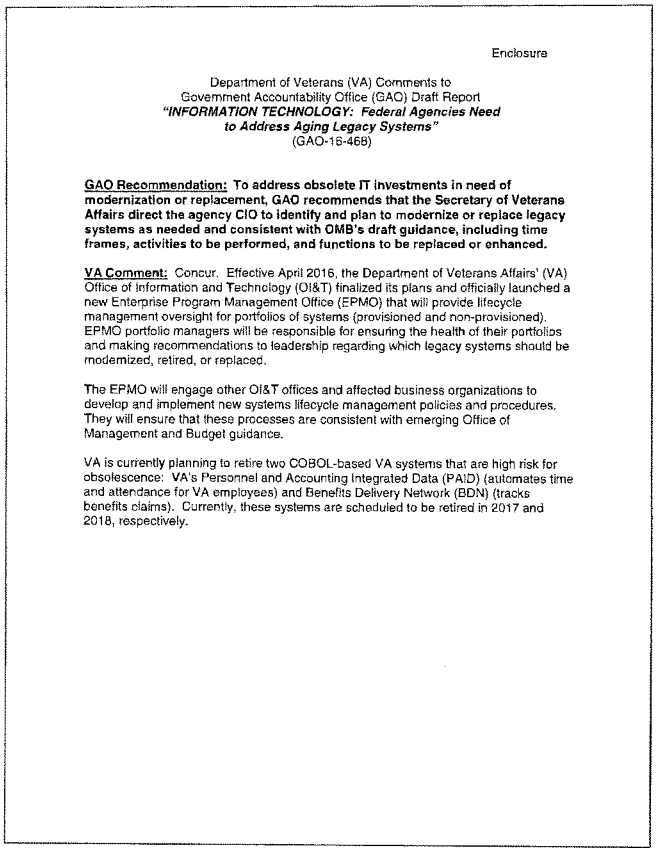
The enclosure specifically addresses GAO's recommendation in the draft report and provides an action plan.

VA appreciates the opportunity to comment on your draft report.

Sincerely,

Robert D. Snyder
Chief of Staff

Enclosure



Enclosure

Department of Veterans (VA) Comments to
Government Accountability Office (GAO) Draft Report
"INFORMATION TECHNOLOGY: Federal Agencies Need
to Address Aging Legacy Systems"
(GAO-16-468)

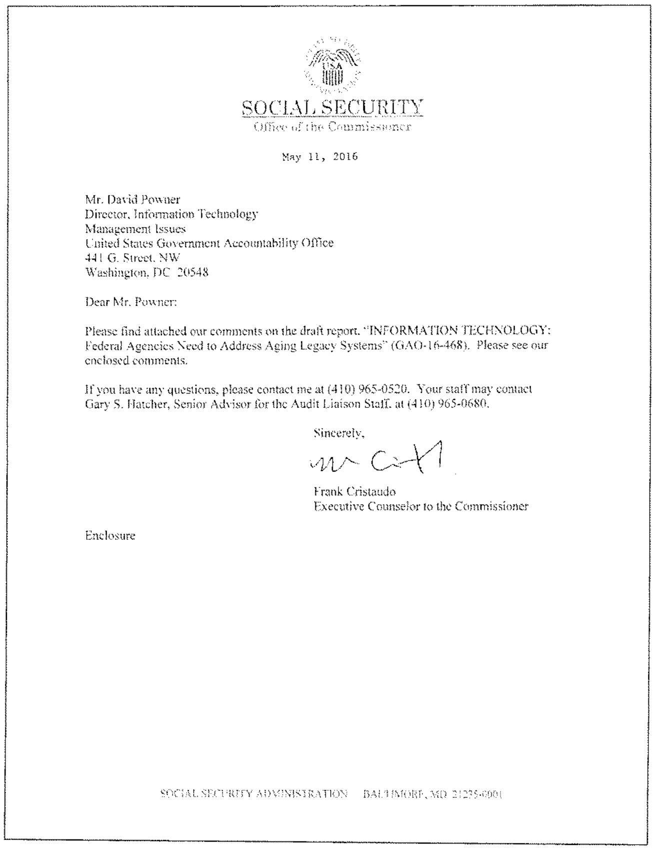
GAO Recommendation: To address obsolete IT investments in need of modernization or replacement, GAO recommends that the Secretary of Veterans Affairs direct the agency CIO to identify and plan to modernize or replace legacy systems as needed and consistent with OMB's draft guidance, including time frames, activities to be performed, and functions to be replaced or enhanced.

VA Comment: Concur. Effective April 2016, the Department of Veterans Affairs' (VA) Office of Information and Technology (OI&T) finalized its plans and officially launched a new Enterprise Program Management Office (EPMO) that will provide lifecycle management oversight for portfolios of systems (provisioned and non-provisioned). EPMO portfolio managers will be responsible for ensuring the health of their portfolios and making recommendations to leadership regarding which legacy systems should be modernized, retired, or replaced.

The EPMO will engage other OI&T offices and affected business organizations to develop and implement new systems lifecycle management policies and procedures. They will ensure that these processes are consistent with emerging Office of Management and Budget guidance.

VA is currently planning to retire two COBOL-based VA systems that are high risk for obsolescence: VA's Personnel and Accounting Integrated Data (PAID) (automates time and attendance for VA employees) and Benefits Delivery Network (BDN) (tracks benefits claims). Currently, these systems are scheduled to be retired in 2017 and 2018, respectively.

Appendix XIII: Comments from the Social Security Administration



SOCIAL SECURITY
Office of the Commissioner

May 11, 2016

Mr. David Powner
Director, Information Technology
Management Issues
United States Government Accountability Office
441 G. Street, NW
Washington, DC 20548

Dear Mr. Powner:

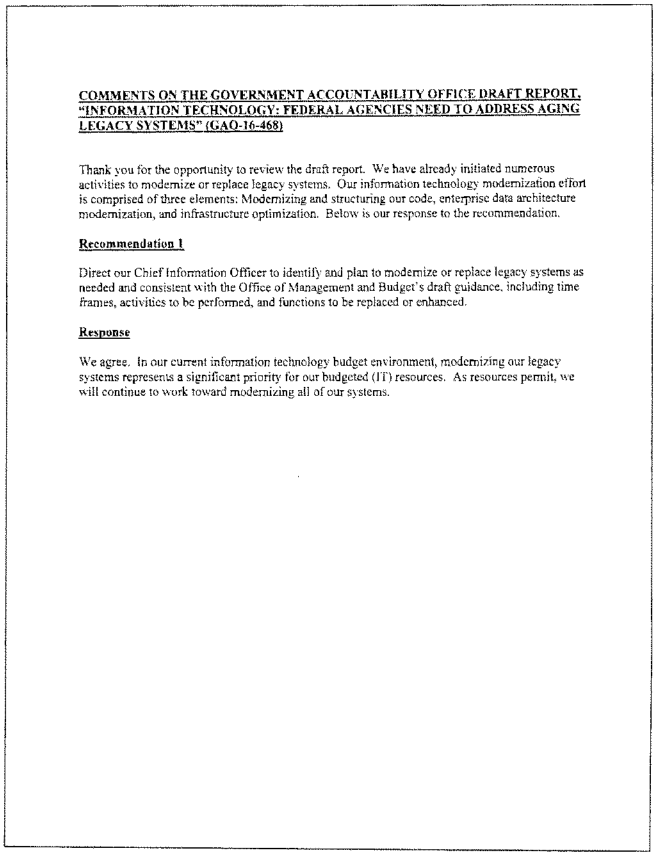
Please find attached our comments on the draft report, "INFORMATION TECHNOLOGY: Federal Agencies Need to Address Aging Legacy Systems" (GAO-16-468). Please see our enclosed comments.

If you have any questions, please contact me at (410) 965-0520. Your staff may contact Gary S. Hatcher, Senior Advisor for the Audit Liaison Staff, at (410) 965-0680.

Sincerely,

Frank Cristaudo
Executive Counselor to the Commissioner

Enclosure



COMMENTS ON THE GOVERNMENT ACCOUNTABILITY OFFICE DRAFT REPORT, "INFORMATION TECHNOLOGY: FEDERAL AGENCIES NEED TO ADDRESS AGING LEGACY SYSTEMS" (GAO-16-468)

Thank you for the opportunity to review the draft report. We have already initiated numerous activities to modernize or replace legacy systems. Our information technology modernization effort is comprised of three elements: Modernizing and structuring our code, enterprise data architecture modernization, and infrastructure optimization. Below is our response to the recommendation.

Recommendation 1

Direct our Chief Information Officer to identify and plan to modernize or replace legacy systems as needed and consistent with the Office of Management and Budget's draft guidance, including time frames, activities to be performed, and functions to be replaced or enhanced.

Response

We agree. In our current information technology budget environment, modernizing our legacy systems represents a significant priority for our budgeted (IT) resources. As resources permit, we will continue to work toward modernizing all of our systems.

Appendix XIV: GAO Contact and Staff Acknowledgments

GAO Contact

David A. Powner, (202) 512-9286 or pownerd@gao.gov

Staff Acknowledgments

In addition to the contact name above, individuals making contributions to this report included Gary Mountjoy (assistant director), Kevin Walsh (assistant director), Scott Borre, Rebecca Eyler, Bradley Roach, Tina Torabi, and Jessica Waselkow.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates.
Listen to our Podcasts and read The Watchblog.
Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

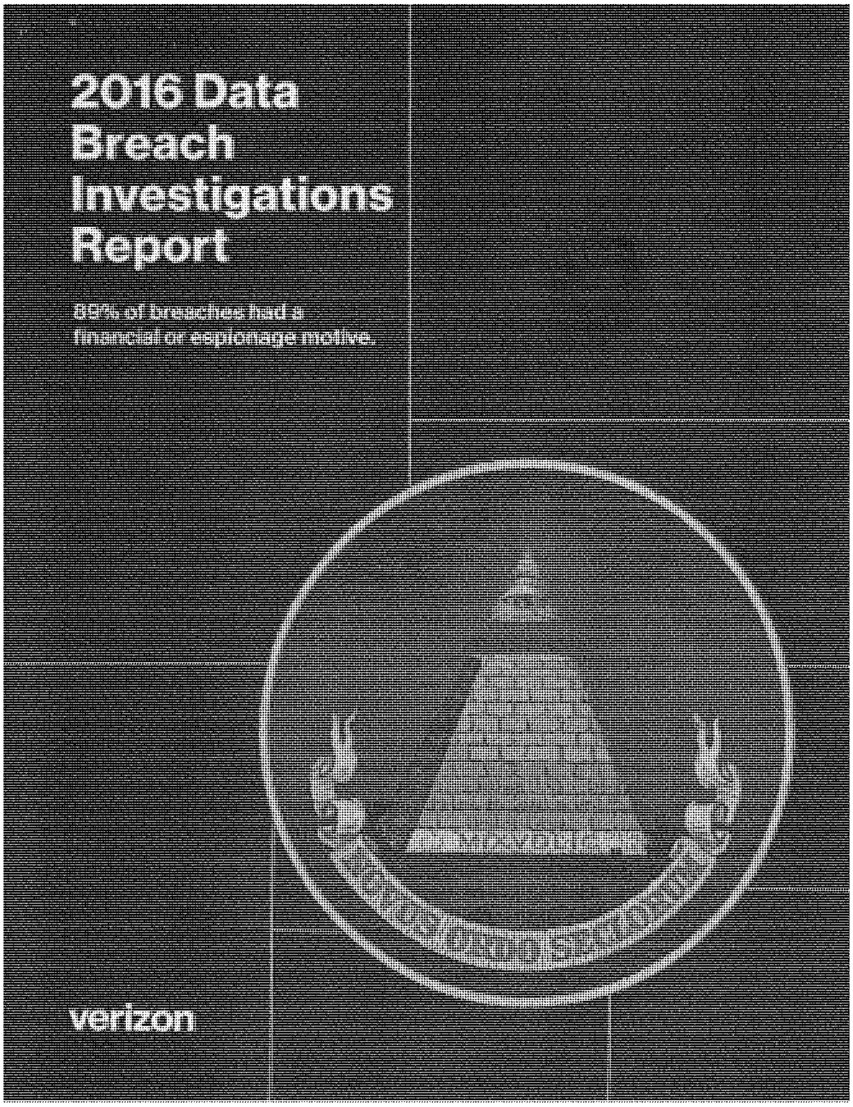
Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper.



2016 Data Breach Investigations Report

89% of breaches had a financial or espionage motive.

verizon

2016 DBIR Contributors

(See Appendix B for a detailed list.)

Akamai

AFP

Deloitte.

CERT | Software Engineering Institute Carnegie Mellon

CERT.PL>_

APWG

DFDR CONSULTING

G-C PARTNERS

CIRCL Computer Incident Response Center Luxembourg

Council on CyberSecurity Le Conseil de la CyberSécurité

CENTER FOR CYBERSIKKERHED

WhiteHat SECURITY

REN-ISAC

wombat security technologies

CERT-UK

OWL One World Labs

KASPERSKY lab

kenna

Check Point SOFTWARE TECHNOLOGIES LTD

Guidance SOFTWARE

EnCase

IRISS Irish Reporting and Information Security Service

RA RiskAnalytics

CISCO

Mishcon de Reya

Center for Internet Security

TRESPASS

ARBOR The Security Division of NETSCOUT

IMPERVA

paloalto NETWORKS

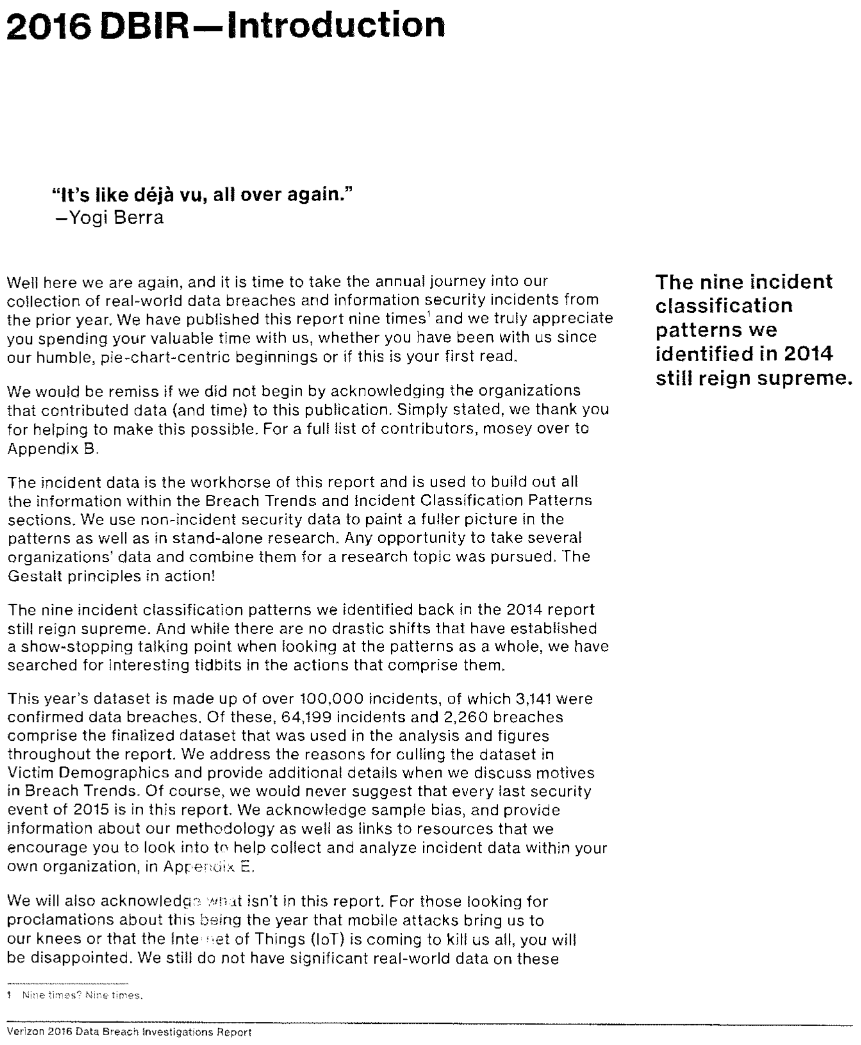
intel Security

CHAMPLAIN COLLEGE | LCDI Leahy Center for Digital Investigation

QUALYS CONTINUOUS SECURITY

Verizon 2016 Data Breach Investigations Report ii

Table of Contents



2016 DBIR—Introduction

"It's like déjà vu, all over again."
—Yogi Berra

Well here we are again, and it is time to take the annual journey into our collection of real-world data breaches and information security incidents from the prior year. We have published this report nine times[1] and we truly appreciate you spending your valuable time with us, whether you have been with us since our humble, pie-chart-centric beginnings or if this is your first read.

The nine incident classification patterns we identified in 2014 still reign supreme.

We would be remiss if we did not begin by acknowledging the organizations that contributed data (and time) to this publication. Simply stated, we thank you for helping to make this possible. For a full list of contributors, mosey over to Appendix B.

The incident data is the workhorse of this report and is used to build out all the information within the Breach Trends and Incident Classification Patterns sections. We use non-incident security data to paint a fuller picture in the patterns as well as in stand-alone research. Any opportunity to take several organizations' data and combine them for a research topic was pursued. The Gestalt principles in action!

The nine incident classification patterns we identified back in the 2014 report still reign supreme. And while there are no drastic shifts that have established a show-stopping talking point when looking at the patterns as a whole, we have searched for interesting tidbits in the actions that comprise them.

This year's dataset is made up of over 100,000 incidents, of which 3,141 were confirmed data breaches. Of these, 64,199 incidents and 2,260 breaches comprise the finalized dataset that was used in the analysis and figures throughout the report. We address the reasons for culling the dataset in Victim Demographics and provide additional details when we discuss motives in Breach Trends. Of course, we would never suggest that every last security event of 2015 is in this report. We acknowledge sample bias, and provide information about our methodology as well as links to resources that we encourage you to look into to help collect and analyze incident data within your own organization, in Appendix E.

We will also acknowledge what isn't in this report. For those looking for proclamations about this being the year that mobile attacks bring us to our knees or that the Internet of Things (IoT) is coming to kill us all, you will be disappointed. We still do not have significant real-world data on these

[1] Nine times? Nine times.

technologies as the vector of attack on organizations.[2] If you feel we are in error, put down the torches and pitchforks and share any breach data that you have. We are always looking for avenues to shine lights into areas in which we may not have sufficient illumination. Also, their absence is not a suggestion to ignore these areas in your risk management decision-making.

The report is designed so you can enjoy it like a prog-rock concept album, from beginning to end, or feel free to bounce around (the room). Enjoy the Breach Trends section for all your figure and chart needs. Get some knowledge on a few of the concepts that stretch across several patterns in our Points of Focus section and for those who want more factoids, pop over to the appendices and give our Taupe Book section a look.

[2] Yes, we are aware of the xCode hack, but without confirmed organizations that suffered an attribute loss it will not be an influencer of this report.

Victim demographics

Before we get into the adversaries behind the incidents and breaches that both underpin this report and keep information security professionals busy, let's acknowledge who is on the receiving end of these attacks. The 2016 report features incidents affecting organizations in 82 countries and across a myriad of industries.

No locale, industry or organization is bulletproof when it comes to the compromise of data.

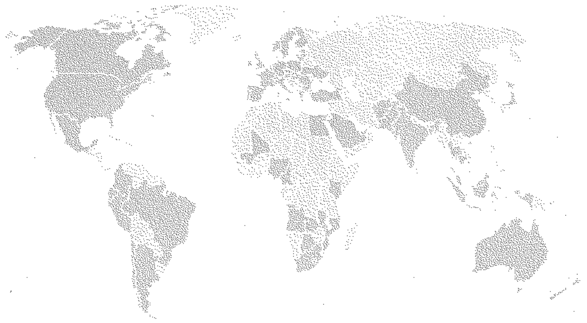


Figure 1.

Countries represented in combined caseload.

No locale, industry or organization is bulletproof when it comes to the compromise of data. Some are notably more represented than others and this is not an indictment that the public sector is any less secure than any other industry. As with prior years, the numbers that follow are heavily influenced by US agency reporting requirements, which open up the fire hose of minor security incidents. Tables 1 and 2 show the number of incidents and breaches by victim industry and size. You may have noticed that the totals in Tables 1 and 2 feature fewer incidents and breaches than the previously advertised 100,000 and 3,141. None are typos—there are a couple of filters applied to the original total. We excluded incidents involving devices repurposed as infrastructure to be used against another target (more on this in the Secondary Motive sidebar in Breach Trends). We also had numerous incidents that failed the "You must be this detailed to enjoy this ride" test.[3]

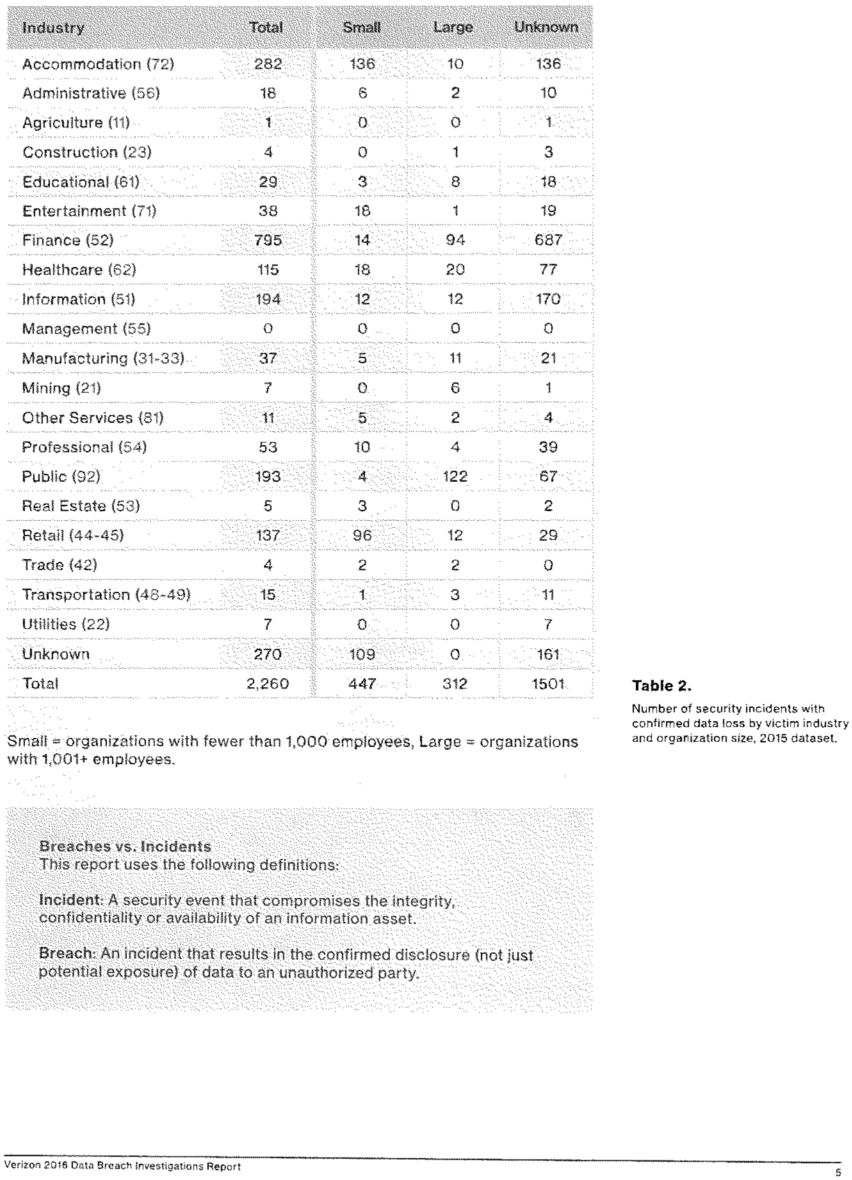
[3] Complexity and completeness scoring is discussed in Appendix E: Methodology and VERIS resources.

When we zoom in on just confirmed breaches, the numbers are less astronomical and we see industries such as Accommodation and Retail accounting for a more significant percentage of breaches (as opposed to incidents). This is unsurprising as they process information which is highly desirable to financially motivated criminals.

Industry	Total	Small	Large	Unknown
Accommodation (72)	362	140	79	143
Administrative (56)	44	6	3	35
Agriculture (11)	4	1	0	3
Construction (23)	9	0	4	5
Educational (61)	254	16	29	209
Entertainment (71)	2,707	18	1	2,688
Finance (52)	1,368	29	131	1,208
Healthcare (62)	166	21	25	120
Information (51)	1,028	18	38	972
Management (55)	1	0	1	0
Manufacturing (31-33)	171	7	61	103
Mining (21)	11	1	7	3
Other Services (81)	17	5	3	9
Professional (54)	916	24	9	883
Public (92)	47,237	6	46,973	258
Real Estate (53)	11	3	4	4
Retail (44-45)	159	102	20	37
Trade (42)	15	3	7	5
Transportation (48-49)	31	1	6	24
Utilities (22)	24	0	3	21
Unknown	9,453	113	1	9,339
Total	64,199	521	47,408	16,270

Table 1.

Number of security incidents by victim industry and organization size, 2015 dataset.



Industry	Total	Small	Large	Unknown
Accommodation (72)	282	136	10	136
Administrative (56)	18	6	2	10
Agriculture (11)	1	0	0	1
Construction (23)	4	0	1	3
Educational (61)	29	3	8	18
Entertainment (71)	38	18	1	19
Finance (52)	795	14	94	687
Healthcare (62)	115	18	20	77
Information (51)	194	12	12	170
Management (55)	0	0	0	0
Manufacturing (31-33)	37	5	11	21
Mining (21)	7	0	6	1
Other Services (81)	11	5	2	4
Professional (54)	53	10	4	39
Public (92)	193	4	122	67
Real Estate (53)	5	3	0	2
Retail (44-45)	137	96	12	29
Trade (42)	4	2	2	0
Transportation (48-49)	15	1	3	11
Utilities (22)	7	0	0	7
Unknown	270	109	0	161
Total	2,260	447	312	1501

Small = organizations with fewer than 1,000 employees, Large = organizations with 1,001+ employees.

Table 2.

Number of security incidents with confirmed data loss by victim industry and organization size, 2015 dataset.

Breaches vs. Incidents
This report uses the following definitions:

Incident: A security event that compromises the integrity, confidentiality or availability of an information asset.

Breach: An incident that results in the confirmed disclosure (not just potential exposure) of data to an unauthorized party.

Breach trends

Playing a part on the blue team in information security can, to a very small degree, be compared to the lot of a hapless soldier. The soldier is told to guard a certain hill and to keep it at all costs. However, he is not told who his enemy may be, what they look like, where they are coming from, or when (or how) they are likely to strike. To ride this analogous horse a bit further, the soldier is given a hand-me-down rifle with only a few rounds of ammunition to fulfill his task. It seems a bit unfair really—even the American Revolution got Paul Revere.

With that in mind, we hope that this section and the facts and figures contained in it will go some way toward making you better prepared than our friend mentioned above. After all, "forewarned is forearmed."

Be prepared: forewarned is forearmed.

A brief primer on VERIS
This section, and many that follow, are based on the Vocabulary for Event Recording and Incident Sharing, or VERIS for short. VERIS is a framework to record and share your security events, incidents and breaches in a repeatable manner. It asks the question, what threat Actor took what Action on what Asset compromising what Attribute? We commonly refer to those as the 4As. In addition to the 4As, it captures timeline, victim demographics, discovery method, impact data and much more.

There are a lot of tools available for VERIS. Methods for creating, importing and analyzing the data are all freely available. More on that in Appendix E: Methodology and VERIS resources.

For those who have read the DBIR before, Figure 2 will come as no surprise. Again, the Actors in breaches are predominantly external. While this goes against InfoSec folklore, the story the data consistently tells is that, when it comes to data disclosure, the attacker is not coming from inside the house. And let's face it, no matter how big your house may be there are more folks outside it than there are inside it.

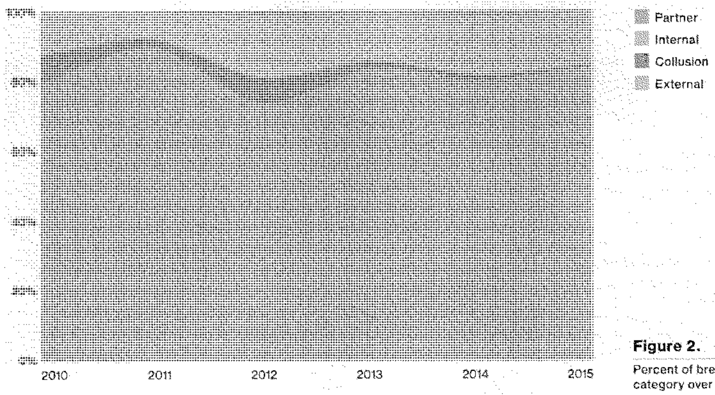


Figure 2.
Percent of breaches per threat actor category over time, (n=8,158)

Why are these people attacking me?
So why do the Actors do what they do? Money, loot, cash, filthy lucre, greed ... get the idea? In fact, it can be money even when it's not money (see Secondary Motive sidebar for more). In the 2013 DBIR it appeared that perhaps the reigning lothario of "financial gain" was in danger of being cast aside in favor of "espionage." Could such a thing come to pass? No, not really.

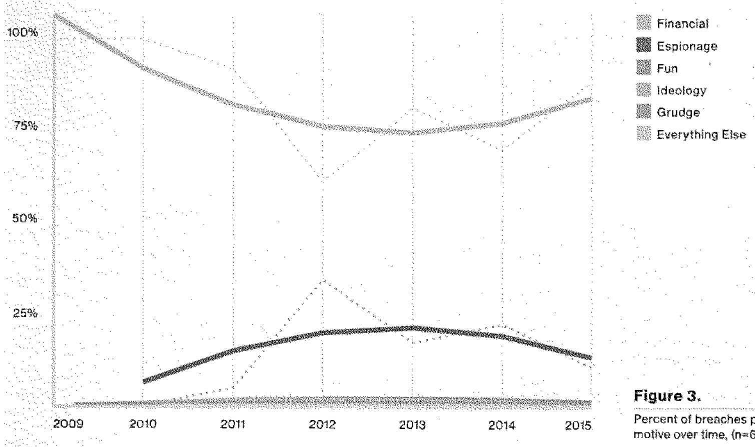


Figure 3.
Percent of breaches per threat actor motive over time, (n=6,762)

There was never any real danger of the financial motive losing its prominence, as even at its peak, espionage remained a far distant second. As illustrated by Figure 3, breaches with a financial motive dominate everything else, including espionage and fun.

Secondary motive
Many of the attacks discussed in this report have what we call a 'secondary motive', which we define as when the motive of the incident is to 'aid in a different attack'. We filter these out of the report because it would overshadow everything else if we didn't. One example is where the bad guy compromises a web server to repurpose it to his own uses (e.g., hosting malicious files or using it in a spam or DoS botnet). Even criminals need infrastructure. "It is a far, far better thing" that someone else manages it for free, rather than having to pay for it yourself. We had thousands of these incidents, as well as poorly configured NTP and DNS servers, leveraged to launch reflective DoS attacks.

Pistols at dawn, or knives at noon?
Now that we know at least a very little bit more about who's coming after us, the next logical question is: how are they armed? As a glance at Figures 4 and 5 can show you, it is often with phishing, which leads to other events that are not going to make your day. We also see the calling card of Point-of-Sale (POS) attacks. No need to go get in the weeds on this here, as these topics will reappear quite a bit in the pages to follow.

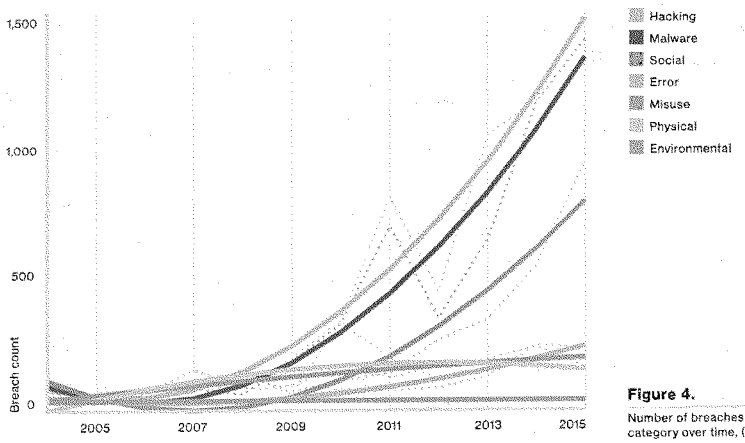


Figure 4.
Number of breaches per threat action category over time, (n=9,009)

Now, to be fair to the other hardworking threat action types in our list, phishing (and the higher level threat action category of Social) was given a leg up this year by the 'Dridex' campaign. We had several contributors who combined to provide a great amount of insight into that naughtiness and this skewed the results somewhat.

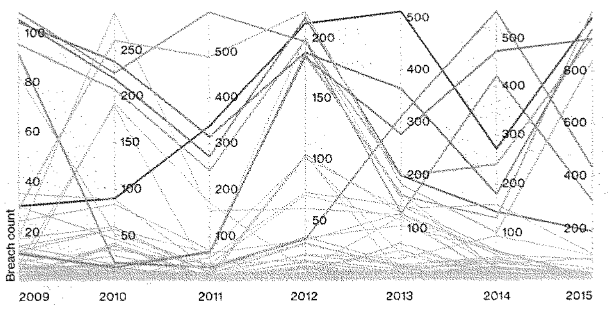


Figure 5.

Threat action varieties in breaches over time, (n=7,717)

Nevertheless, at this point, we think both Phishing and Point-of-Sale could safely say, in their best Ron Burgundy voice, "You might have heard of me, I'm kind of a big deal." Due to this rock-star status, we're going to dig a little deeper into POS attacks later in the Patterns section and also in the Post-Compromise Fraud write-up. Likewise, we discuss phishing in greater detail in the Phishing section and Cyber-espionage pattern. We even have a section on credentials this year. Credentials have made numerous cameo appearances in this report for years, but never before have they had a speaking part. (Always a bridesmaid, never a bride.)

The many facets of assets

Guess what? When the bad guys' actions are centered around phishing and POS devices, the asset varieties displayed in Figure 6 reflect this. That lovely "Person" line trending up is due to the human asset falling victim to phishing attacks[4]. The "User device" line upward trend is based on desktops being infected with malware, as well as POS terminals getting popped.

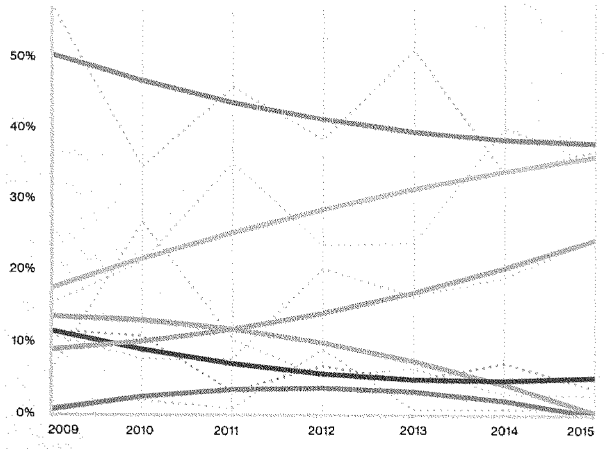


Figure 6.

Percent of breaches per asset category over time, (n=7,736)

[4] In VERIS we model this stage of the attack as a loss of integrity based on the influencing of human behavior.

Mick was wrong—time is not on our side.
Rome wasn't built in a day, but data breaches frequently were. Figure 7 illustrates how quickly the threat Actor gets in and out of your network. The large spikes, however, are driven by very specific threats. The compromise time of minutes, while depressing to look at, is actually another reflection of the ubiquitous 'Dridex' breaches in this year's dataset. As previously alluded to, these cases begin with a phish, featuring an attachment whose mission in its malware life is to steal credentials. If you have legit creds, it doesn't take a very long time to unlock the door, walk in and help yourself to what's in the fridge. Conversely, the exfiltration time being so weighted in the 'days' category is heavily representative of attacks against POS devices where malware is dropped to capture, package and execute scheduled exports.

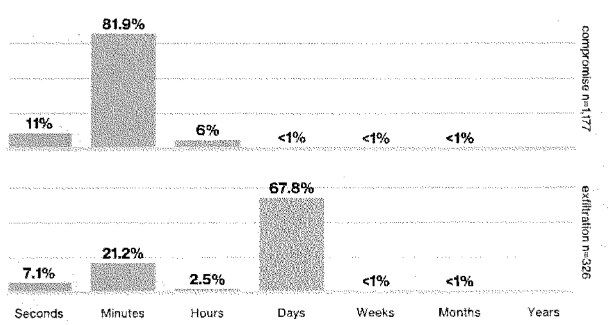


Figure 7.
Time to compromise and exfiltration.

Bad news travels fast, with one exception.
We like this next graph—one line goes one way and the other line goes the other way. Actually we would like it even more if the lines took different paths. The bad news is, the detection deficit in Figure 8 is getting worse.

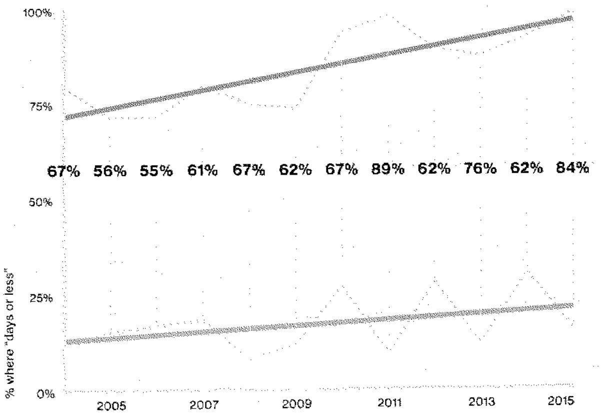


Figure 8.
Percent of breaches where time to compromise (green)/time to discovery (blue) was days or less

In the 2015 report, we mentioned that there was some improvement in discovery in the 'days or less' category, however, that improvement was short-lived. We also pointed out that we would need more than one year's data to verify that as a definite trend and sadly we did not get that verification. Moreover, readers with excellent memories will notice that the deficit in 2014 grew from last year's report. Data for the year-to-year graphs is filtered by incident year (i.e., when the compromise occurred). We continue to add incidents and breaches to prior calendar years post-report to enrich our data. Also, some breaches will occur late in the year and are discovered the next year.

To add another ray to this sunbeam, attackers are getting even quicker at compromising their victims. When you review the leading threat actions again, this really won't come as a surprise. The phishing scenario is going to work quickly, with the dropping of malware via malicious attachments occurring within seconds. Physical compromises of ATMs and gas pumps also happen in seconds. In the majority of confirmed data breaches, the modus operandi of nation-states as well as financially motivated attackers is to establish control via malware and, when successful, it is lightning fast. As this figure is for confirmed breaches only, it makes sense that the time to compromise is almost always days or less (if not minutes or less). If—and some have called "if" the biggest word in the language—there's any good news, it's that the number of breaches staying open months or more continues to decline slightly.

The time to compromise is almost always days or less, if not minutes or less.

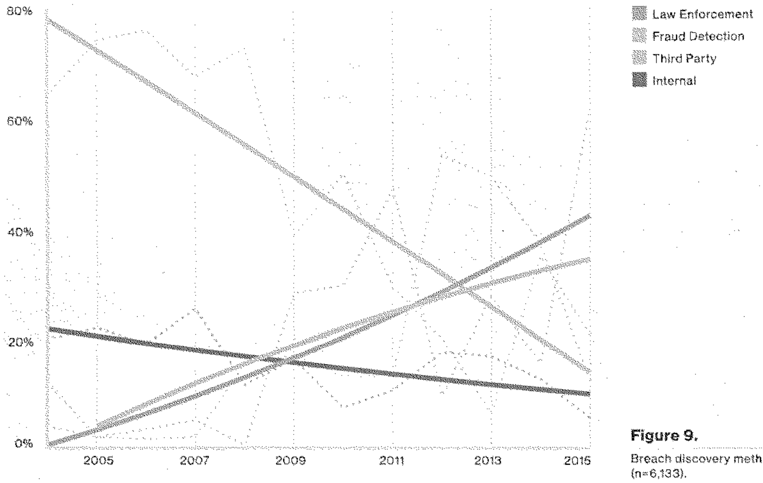


Figure 9.
Breach discovery methods over time, (n=6,133).

When it comes to external[5] breach discovery, fraud detection and law enforcement notification are battling it out like the Celtics and Lakers in the '80s. Figure 9 shows that law enforcement will raise the banner for 2015, due (again) to a botnet takedown and the subsequent notifications to members of the botnet. All in all, external notification is up. And when you have to wait on external detection to tell you you're popped, it's probably too late to keep the horses in the barn.

[5] External is everything but internal detection and when a partner supplies a monitoring or AV service.

Points of focus

One last thing before we get to the patterns. There are a couple of topics that are omnipresent in many of the patterns that we use to classify incidents. While they will receive credit where credit is due, in the pattern sections, we feel that we also need to put the spotlight on them here.

We have numerous breaches where we can infer that some Common Vulnerabilities and Exposures (CVE) were used in order for the attack to advance. Hey, we're looking at you, drive-by downloads! Unfortunately, we don't have a tremendous amount of CVE data in our corpus, either because it was not measured or was unable to be identified. This lack of detail makes us an embarrassment of sad pandas. (Yes, we wanted to say "sleuth", but apparently we can't. Look it up.) Luckily we have contributors in the vulnerability space that can lighten our mood.

Phishing has continued to trend upward (like spawning salmon?) and is found in the most opportunistic attacks as well as the sophisticated nation state tomfoolery. We feature a section where we dive into the human element a bit deeper, with some data on our innate need to click stuff.

Lastly, we strike a deceased equine a bit more with a section on credentials (of the static variety). Don't get us wrong–passwords are great, kind of like salt. Wonderful as an addition to something else, but you wouldn't consume it on its own.

We don't have a tremendous amount of CVE data because it wasn't measured or was unable to be identified.

Vulnerabilities

At a glance

Description	A look into software vulnerabilities, whether we are making any progress in addressing them and ways to improve.
Contributors	Kenna Security (formerly Risk I/O) collaborated with us again to leverage their vulnerability and exploitation data. We also utilized vulnerability scan data provided by Beyond Trust, Qualys and Tripwire in support of this section.
Key findings	Older vulnerabilities are still heavily targeted; a methodical patch approach that emphasizes consistency and coverage is more important than expedient patching.

New vulnerabilities come out every day.

Methodology

The visualizations and statements regarding rates of exploitation in this section are underpinned by vulnerability exploitation data provided by Kenna Security. This dataset spans millions of successful real-world exploitations, and is derived from hunting down exploitation signatures in security information and event management (SIEM) logs and correlating those with vulnerability scan data to find pairings that would be indicative of a successful exploitation.

The tortoise and the hare

Vulnerability management has been a Sisyphean endeavor for decades. Attacks come in millions, exploits are automated and every enterprise is subject to the wrath of the quick-to-catch-on hacker. What's worse, new vulnerabilities come out every day. Since the first DBIR, we've been advocating the turtle's approach to vulnerability management (slow and steady wins the race).

This year we revisit this data to see whether the trends hold, but in typical DBIR fashion, we dig a little deeper, to look at not just how attackers are interacting with vulnerabilities (exploitation), but also how well and how fast enterprises are executing remediation. If we can measure both of these routinely, then we can provide much-needed answers about how the tortoise won the race—and so learn how to close the gap between attackers and enterprises.

Slow and steady–but how slow?

This year we take a different approach to measuring the time from publication to exploitation. Figure 10 is a box plot, which plots the time between publication and the first observed successful exploit by vendors.[6] We can see that Adobe vulnerabilities are exploited quickly, while Mozilla vulnerabilities take much longer to exploit after disclosure. Half of all exploitations happen between 10 and 100 days after the vulnerability is published, with the median around 30 days. This provides us with some general guidelines on which software vulnerabilities to prioritize along with some guidance on time-to-patch targets.

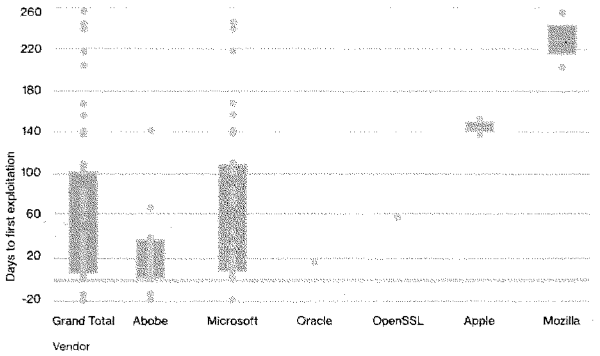


Figure 10.
Time to first-known exploitation by vulnerability category.

Treading water

Figure 11 shows the number of vulnerabilities opened each week minus the number of vulnerabilities (aka "vulns") closed, scaled by the number of assets in the dataset during each week of 2015. When the line is above zero, it means that more vulns are being opened than closed (new vulns disclosed, more

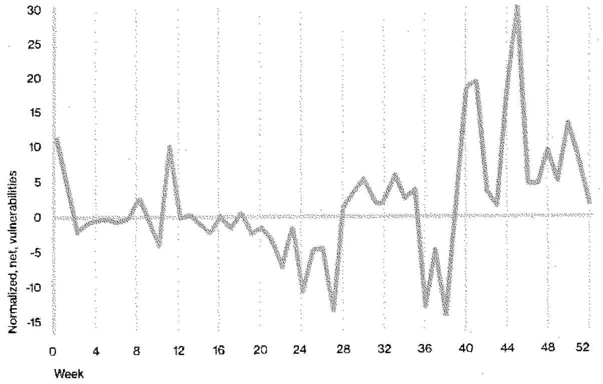


Figure 11.
Delta of number of vulnerabilities opened each week and number closed.

[6] The blue boxes in Figure 10 represent 50% of the values for a given category and the gray line within the box is the median value. The dots represent individual values.

machines entering the environment, new software installed). When it's below zero, remediation efforts are driving down vulnerability counts faster than new vulns are entering the enterprise.

Basically, we confirmed across multiple datasets that we are treading water—we aren't sinking in new vulnerabilities, but we're also not swimming to the land of instantaneous remediation and vuln-free assets. However, all that patching is for naught if we're not patching the right things. If we're going to tread, let's tread wisely.

All that patching is for naught if we're not patching the right things.

What should we mitigate? Hacker economics.
So what are the right things? The 2015 DBIR gave us an idea and since then, not much has changed.

Revisiting last year's trends, we find that the two golden rules of vulnerabilities still hold.

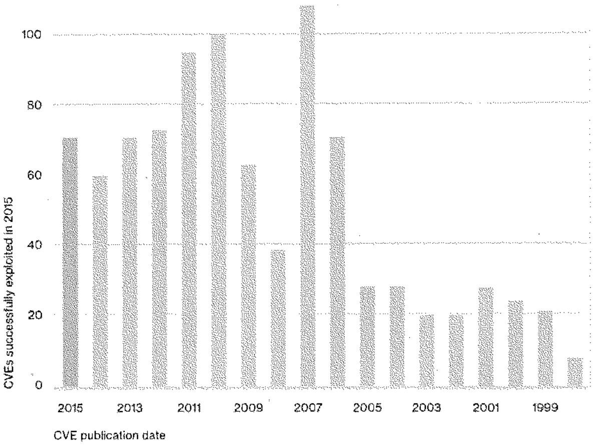


Figure 12.
Count of CVEs exploited in 2015 by CVE publication date.

First, Figure 12 arranges CVEs according to publication year and gives a count of CVEs for each year. While 2015 was no chump when it came to successfully exploited CVEs, the tally of really old CVEs which still get exploited in 2015 suggests that the oldies are still goodies. Hackers use what works and what works doesn't seem to change all that often.[7] Secondly, attackers automate certain weaponized vulnerabilities and spray and pray them across the internet, sometimes yielding incredible success. The distribution is very similar to last year, with the top 10 vulnerabilities accounting for 85% of successful exploit traffic.[8] While being aware of and fixing these mega-vulns is a solid first step, don't forget that the other 15% consists of over 900 CVEs, which are also being actively exploited in the wild.

[7] Astute and frequent readers of the DBIR will notice one more gem in this chart—last year, the numbers of published CVEs exploited were lower across the board—and this year, we have more and better data. Those newly exploited CVEs however, are mostly—and consistently—older than one year.

[8] CVE-2001-0876, CVE-2011-0877, CVE-2002-0953, CVE-2001-0680, CVE-2012-1054, CVE-2015-0204, CVE-2015-1637, CVE-2003-0818, CVE-2002-0126, CVE-1999-1058.

Can't solve everything

In Figure 13, we see that during 2015, vulnerabilities published in 2015 and 2014 were being patched. After that though, the vulnerabilities begin to drop off and really hit a steady state. This gets at a core and often ignored vulnerability management constraint—sometimes you just can't fix a vulnerability—be it because of a business process, a lack of a patch, or incompatibilities. At that point, for whatever reason, you may have to live with those residual vulnerabilities. It's important to realize that mitigation is often just as useful as remediation—and sometimes it's your only option.

Mitigation is often just as useful as remediation—and sometimes your only option.

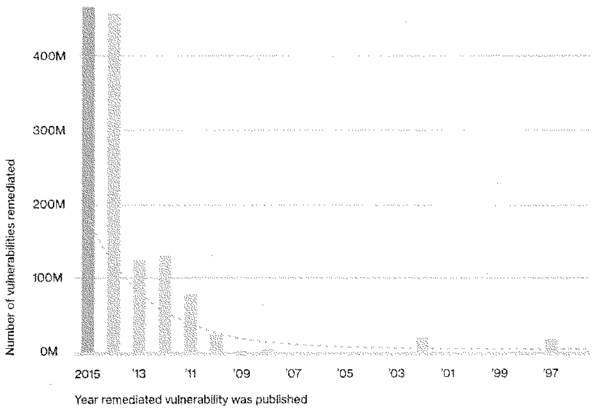


Figure 13.
Closure rate of CVEs by CVE publication date.

Recommended controls

Knowledge is power.

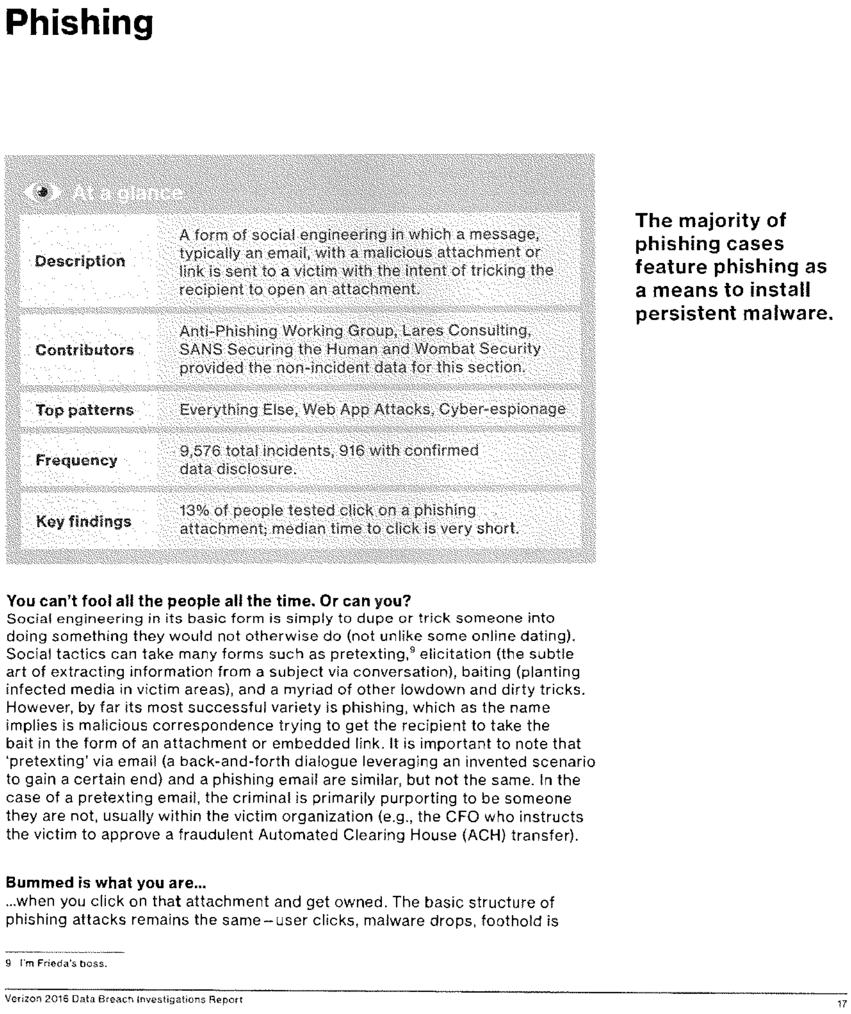
Establish a process for vulnerability remediation that targets vulnerabilities which attackers are exploiting in the wild, followed by vulnerabilities with known exploits or proof-of-concept code.

Have a Plan B.

If you have a system that cannot be patched or receive the latest-and-greatest software update, identify it, and apply other risk mitigations in the form of configuration changes or isolation. Discuss a plan on how the device(s) could be replaced without causing severe business disruption.

At your service

Vulnerability scanning is also useful in identifying new devices and new services. Review scan-to-scan changes as another control to identify unknown devices and deviations from standard configurations.



Phishing

At a glance

Description	A form of social engineering in which a message, typically an email, with a malicious attachment or link is sent to a victim with the intent of tricking the recipient to open an attachment.
Contributors	Anti-Phishing Working Group, Lares Consulting, SANS Securing the Human and Wombat Security provided the non-incident data for this section.
Top patterns	Everything Else, Web App Attacks, Cyber-espionage
Frequency	9,576 total incidents, 916 with confirmed data disclosure.
Key findings	13% of people tested click on a phishing attachment; median time to click is very short.

The majority of phishing cases feature phishing as a means to install persistent malware.

You can't fool all the people all the time. Or can you?

Social engineering in its basic form is simply to dupe or trick someone into doing something they would not otherwise do (not unlike some online dating). Social tactics can take many forms such as pretexting,[9] elicitation (the subtle art of extracting information from a subject via conversation), baiting (planting infected media in victim areas), and a myriad of other lowdown and dirty tricks. However, by far its most successful variety is phishing, which as the name implies is malicious correspondence trying to get the recipient to take the bait in the form of an attachment or embedded link. It is important to note that 'pretexting' via email (a back-and-forth dialogue leveraging an invented scenario to gain a certain end) and a phishing email are similar, but not the same. In the case of a pretexting email, the criminal is primarily purporting to be someone they are not, usually within the victim organization (e.g., the CFO who instructs the victim to approve a fraudulent Automated Clearing House (ACH) transfer).

Bummed is what you are...

...when you click on that attachment and get owned. The basic structure of phishing attacks remains the same—user clicks, malware drops, foothold is

[9] I'm Frieda's boss.

gained. There are still cases where the phishing email leads users to phony sites, which are used to capture user input, but the majority of phishing cases in our data feature phishing as a means to install persistent malware. The victim opens the email, sees the attachment that contains the malware du jour and says "That file looks good, I'll have that". What happens next is dictated by the end goal of the phisher.

"What we have here is a failure to communicate."

Apparently, the communication between the criminal and the victim is much more effective than the communication between employees and security staff. We combined over eight million results of sanctioned phishing tests in 2015 from multiple security awareness vendors aiming to fix just that. Figure 14 is jam-packed with information. In this year's dataset, 30% of phishing messages were opened by the target across all campaigns.[10] "But wait, there's more!" (in our best infomercial voice) About 12% went on to click the malicious attachment or link and thus enabled the attack to succeed. That indicates a significant rise from last year's report in the number of folks who opened the email (23% in the 2014 dataset) and a minimal increase in the number who clicked on the attachment (11% in the 2014 dataset). The median time for the first user of a phishing campaign to open the malicious email is 1 minute, 40 seconds. The median time to the first click on the attachment was 3 minutes, 45 seconds, thus proving that most people are clearly more on top of their email than I am.

The main perpetrators for phishing attacks are organized crime syndicates and state-affiliated actors.

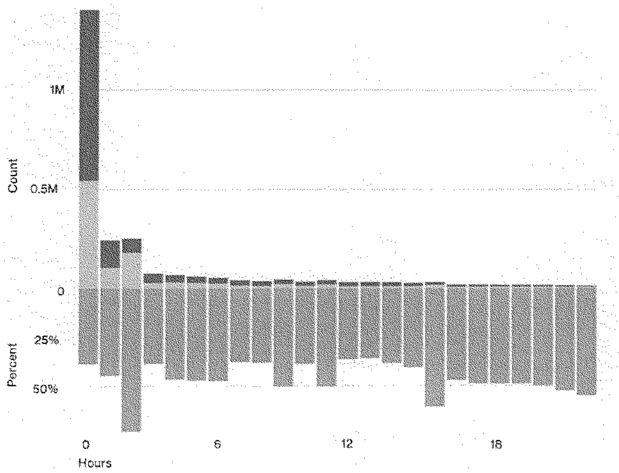


Figure 14.
Number of phishing emails opened and clicked in first 24 hours and percent of opened emails that were clicked

However, before we drag these individuals outside and collectively stone them, keep in mind that the main perpetrators for these types of attacks are organized crime syndicates (89%) and state-affiliated Actors (9%) who can put some thought into the ruse they use (yeah, I know). In roughly 636,000 sanctioned phishing emails, we captured whether the email was reported. Approximately 3% of targeted individuals alerted management of a possible phishing email. We did not verify by what means the email was reported, or whether it was because they were savvy enough to avoid the trap or because they only realized it once they had fallen in themselves.

[10] Granted this could be affected by preview pane opening of emails or people not loading images in emails.

As an aside, the smaller proportion of nation-state Actors in this year's data is due to a large contribution from a particular contributor who saw a great deal of 'Dridex' campaigns which skewed the data toward organized crime. We should not conclude from this that certain groups from East Asia have had a crisis of conscience and mended their wicked ways.

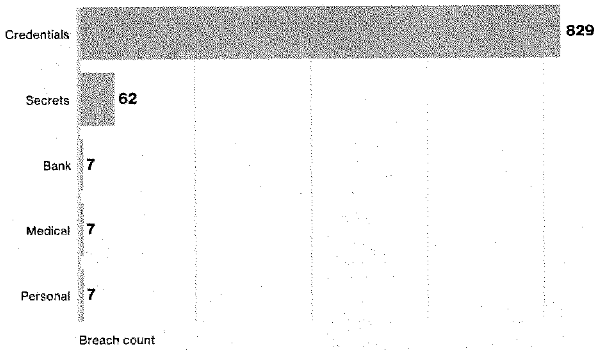


Figure 15.

Top five data varieties breached by phishing attacks. (n=905)

What do the attackers ultimately steal? A heck of a lot of credentials (mostly due to the large amount of opportunistic banking Trojans—beware of Greeks bearing gifts), but also trade secrets.

Recommended controls

Filter it! Filter it real good!
"An ounce of prevention is worth a pound of cure." It was good advice when Ben said it and so it remains. The first opportunity to defend against email-borne threats is (thankfully) before a human can interact with it. Email filtering is your buddy in this fight and you need to have an understanding of your current solution, and test its implementation.

Protect the rest of your network from compromised desktops and laptops by segmenting the network and implementing strong authentication.

Talk amongst yourselves (I'm verklempt)!
Provide employees with awareness training and information so they can tell if there is something 'phishy' (couldn't resist) going on. Also, provide them with a means for reporting these events. We recommend a button on their taskbar, but whatever works for you.

One click does not a catastrophe make.
So, it snuck past your email filters and someone went clicky-clicky. There is still ample opportunity to limit the impact. Assuming the organization's "seekrit stuff" isn't resident on the initial foothold, make it hard to pivot from the user device to other assets in the organization. Protect the rest of your network from compromised desktops and laptops by segmenting the network and implementing strong authentication between the user networks and anything of importance. Static passwords are adorable, but sophisticated attackers don't just bypass them, they utilize them to advance their attack.

Keep your eye on the ball.
You increase your chances of catching signs that you have fallen victim to a phishing attack if you monitor outbound traffic for suspicious connections and potential exfiltration of data to remote hosts.

Credentials

At a glance

Description	Use of stolen credentials and other hacking and malware actions targeting traditional username and password authentication are prevalent across numerous patterns.
Top patterns	Web App Attacks, POS Intrusions
Frequency	1,429 incidents with confirmed data disclosure.
Key findings	Static credentials continue to be targeted by several of the top hacking action varieties and malware functionalities.

63% of confirmed data breaches involved weak, default or stolen passwords.

We're not mad, just disappointed.
The use of stolen, weak or default credentials in breaches is not new, is not bleeding edge, is not glamorous, but boy howdy it works. Static authentication mechanisms have been attacked for as long as we can remember. Password guessing from an InfoSec perspective has been around at least as long as the Morris worm, and has evolved to prominent malware families like Dyre and Zeus that are designed to (among other bad things) capture keystrokes from an infected device. All those efforts to get users to use special characters, upper/lower case numbers and minimum lengths are nullified by this ubiquitous malware functionality.

The capture and/or reuse of credentials is used in numerous incident classification patterns. It is used in highly targeted attacks as well as in opportunistic malware infections. It is in the standard toolkit of organized criminal groups and state-affiliated attackers alike. Even fraud committed with stolen payment card data often relies on the static Card Verification Value (CVV) information on the magnetic stripe.[11]

We are realists here, we know that implementation of multi-factor authentication is not easy. We know that a standard username and password combo may very well be enough to protect your fantasy football league. We also know that implementation of stronger authentication mechanisms is a bar

[11] More on this in the Post-Compromise Fraud appendix.

raise, not a panacea. Even with all of that, 63%[12] of confirmed data breaches involved leveraging weak/default/stolen passwords. This statistic drives our recommendation that this is a bar worth raising. Figure 16 shows the most common threat action varieties associated with attacks involving legitimate credentials. The obvious action of the use of stolen credentials is numero uno, but we see some other common actions used in conjunction, including C2 malware, exporting of data, phishing and keyloggers.

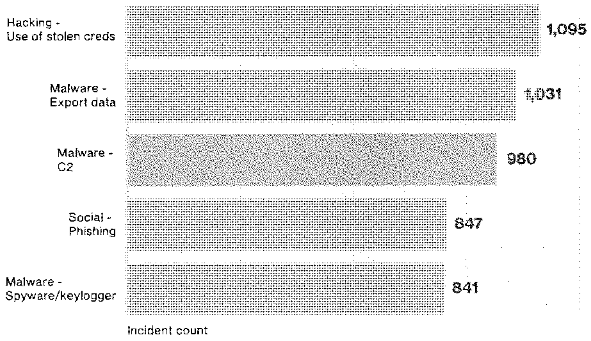


Figure 16.

Top threat action varieties within incidents involving credentials. (n=1,462)

[12] We combined all incidents with confirmed data disclosure AND use of stolen creds OR brute force OR password dumpers OR a data variety of credentials.

Incident classification patterns

What began with a muttered complaint of "ugh, another one of these" during data conversion a couple of years ago grew into a shift in how we present our core results and analysis. The nine incident classification patterns were born of recurring combinations of the who (Actors), what (assets), how (actions) and why (motive) among other incident characteristics.

In the 2014 report, we found that over 90% of breaches fell into one of the nine buckets and this year's dataset is no different. We hope that by discussing security incidents, both for this year and historically, and using these clusters as the foundation, we can allow security folks to gain the most from the entire (huge) dataset. Understanding that you don't have to necessarily worry about 2,260 different breach possibilities, but only a select number of nine patterns (depending on your industry) makes the life of a CISO less of a daily Kobayashi Maru.

Before we dive deeper into changes over time and the individual patterns (and don't fret, we will), let's take a moment and look at the incident and breach breakouts for 2015 in Figures 17 and 18.

The nine classification patterns were born of recurring combinations of the who, what, how and why.

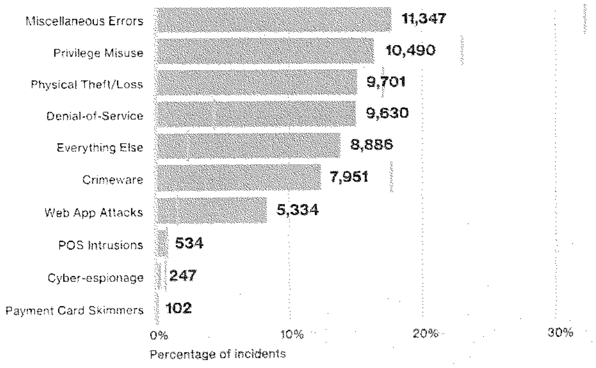


Figure 17.

Percentage (blue bar), and count of incidents per pattern. The gray line represents the percentage of incidents from the 2015 DBIR. (n=64,199)

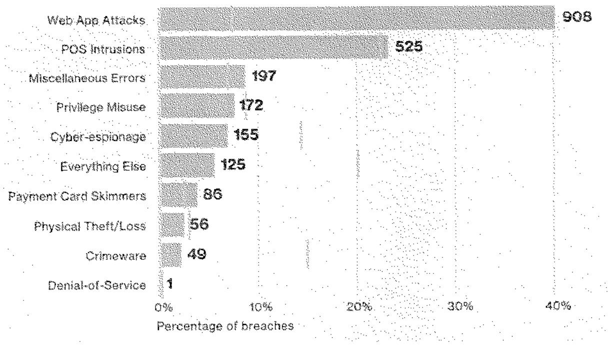


Figure 18.

Percentage (blue bar), and count of breaches per pattern. The gray line represents the percentage of breaches from the 2015 DBIR. (n=2,260)

Much to the chagrin of Jerry Lee Lewis, there was not a whole lot of moving and shaking going on in the pattern rankings compared to last year and looking at all incidents, only one pattern moved in the pecking order. Crimeware was the third most common pattern last year and has moved to sixth. The reason is the filter on the secondary motive we discussed in the Breach Trends section. Thousands of incidents where we know a device was participating in a denial-of-service (DoS) bot (but nothing else) were not sent to /dev/null per se, but you won't find them here.[13]

The fact is that our dataset is constantly evolving with contributors joining (yay) and others not able to participate for a year. Many of our contributors have a certain specialty or discipline that results in their data being associated with a certain victim industry, or threat Actor type, or country ... you get the picture. Because of this fact, the ebbs and flows in the patterns from year to year are attributed more to changes in our data than changes in the threat landscape. Bad guy trends would likely be best gleaned from the threat action variety level within a pattern and again, the deeper dives are coming. Having said all of that, Figures 19 and 20 represent the obligatory "trend" graphs.

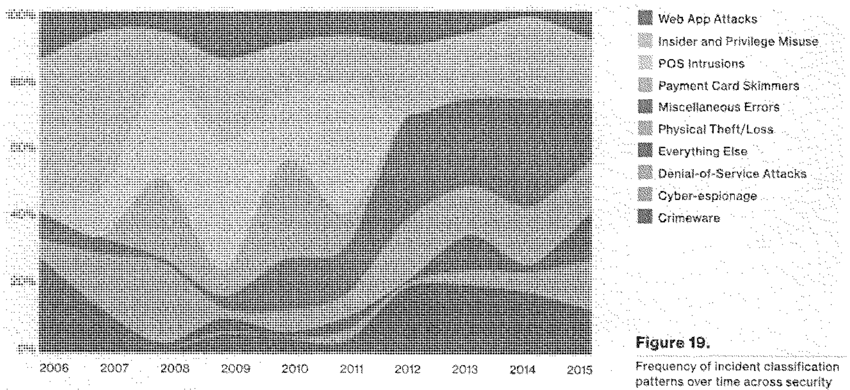


Figure 19.

Frequency of incident classification patterns over time across security incidents.

[13] There are thousands of compromised web servers used as phishing sites that did not make the cut either. No information on how the server was compromised, or if it was owned or maintained by an organization, was available.

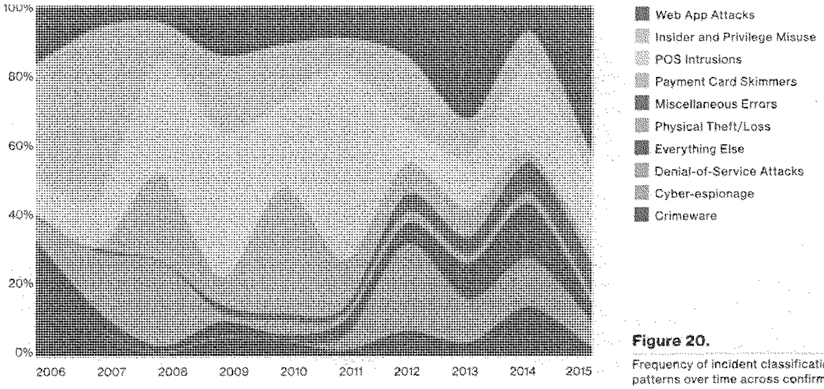


Figure 20.

Frequency of incident classification patterns over time across confirmed data breaches.

OK, in lieu of worrying about how patterns rank overall compared to each other, let's get to the good stuff. The best way to use the patterns is to understand the applicability of each of them to your organization. The following charts show the frequency of each of the patterns relative to each industry. In other words, it shows for all the incidents (Figure 21) and breaches (Figure 22) within your industry, those patterns which were common and those which didn't make an appearance. We have included the incident and breach totals again as some of the combinations are a small percentage, but still represent a significant number of events. We use the North American Industry Classification System (NAICS) to classify the victim industry—go to the NAICS website[14] if you're unsure where your organization fits. Of course if you are an E Corp-like conglomerate, you can have business units that fall into several industry categories.

Figure 21.

Incident patterns by industry minimum 25 incidents

Crimeware	Cyber-espionage	Denial of Service	Everything Else	Stolen Assets	Misc. Errors	Card Skimmers	Point of Sale	Privilege Misuse	Web Apps	
<1%	<1%	20%	1%	1%	1%	<1%	74%	2%	1%	Accommodation (72), n=362
		56%	4%		2%		4%	22%	11%	Administrative (56), n=44
2%	2%	81%	2%	3%	4%			1%	5%	Educational (61), n=254
		99%		<1%			1%		1%	Entertainment (71), n=2,707
2%	<1%	34%	5%	<1%	1%	6%	<1%	3%	48%	Finance (52), n=1,368
4%	2%		11%	32%	18%		5%	23%	4%	Healthcare (62), n=166
4%	3%	46%	21%	<1%	11%		<1%	2%	12%	Information (51)n, 1,028
5%	16%	33%	33%		1%		1%	6%	6%	Manufacturing (31-33), n=171
1%	2%	90%	2%	1%	1%			2%	1%	Professional (54), n=916
16%	<1%	1%	17%	20%	24%		<1%	22%	<1%	Public (92), n=47,237
1%	<1%	45%	2%		1%	3%	32%	1%	13%	Retail (44-45), n=370
10%	16%	26%			6%			6%	35%	Transportation (48-49), n=31

[14] Census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012

From an incident standpoint, Denial-of-Service stands out like "a zoot suit at a Quaker funeral". This is partly due to the fact that DoS attacks are in fact, happening all the time—remember all those popped boxes in the DoS botnets we filtered out? Another reality is that the other patterns that are more commonly classified as incidents as opposed to confirmed data breaches (Crimeware, Insider and Privilege Misuse, and Physical Theft and Loss) are mostly provided by the public sector and healthcare. Those are the top three incident patterns and we are confident that in the real world they are taking some of that market share from DoS in other industries.

Crimeware	Cyber-espionage	Denial of Service	Everything Else	Stolen Assets	Misc. Errors	Card Skimmers	Point of Sale	Privilege Misuse	Web Apps	
			1%	<1%	1%	<1%	95%	1%	1%	Accommodation (72), n=282
	7%		17%	17%	27%			3%	30%	Educational (61), n=29
				3%			47%		50%	Entertainment (71), n=38
1%	<1%	<1%	2%	<1%	2%	9%		4%	82%	Finance (52), n=795
3%	3%		11%	19%	22%		7%	32%	3%	Healthcare (62), n=115
1%	3%		4%		25%		1%	11%	57%	Information (51), n=194
3%	47%		3%				3%	24%	21%	Manufacturing (31-33), n=37
4%	19%		25%	4%	15%			21%	13%	Professional (54), n=53
12%	16%		4%	9%	37%			13%	9%	Public (92), n=193
1%	1%		4%		1%	3%	64%	2%	26%	Retail (44-45), n=182

Figure 22.

Incident patterns by industry minimum 25 incidents (only confirmed data breaches)

The most interesting discovery in the breach patterns to industry matrix was the rise of Web App Attacks across the board, but especially for financial services organizations (up from 31% in the 2015 DBIR). The next item that raised an eyebrow or two (or perhaps a unibrow) was the decline (down from 36% last year) in Crimeware, also in Finance. Is there anything to this? Actually, yes. This year, again thanks to the organizations involved in the Dridex takedown, we have even more data involving the reuse of stolen credentials. This caused the spike in the Web App Attack pattern and if we removed these breaches, the numbers would be more in line with 2014. On the flip side, in 2014 we received more data on malware infections within organizations, leading to breaches that landed in our Crimeware bucket. Is Crimeware not playing as big a role in breaches? The perspective of the reporting contributor has a lot to do with the pattern breakdowns as well. Using the banking Trojan example:

Event 1: Organization A is infected with a Zeus variant via a drive-by download

Event 2: Malware has a keylogging functionality that captures banking credentials

Event 3: Malware exports captured data to command and control (C2) server

Intermission music

Event 4: Credentials are used to log into Organization B web server

Event 5: Fraudulent transaction is initiated

Organization B may be quick to say "We didn't have a malware incident" and if events 4–5 are provided to us, the incident would find a good home in the Web App Attacks section. But if we received data from Organization A and only events 1–3 are documented, it now becomes a newly minted Crimeware breach.

It is important to realize that there are interrelations between the incident patterns that aren't always evident. Crimeware in one organization leads to DoS against another; or to fraudulent transactions on another's application. Remember we're all in this together: the security ecosystem, Kumbaya and trust falls folks...

Web App Attacks

At a glance

Description	Any incident in which a web application was the vector of attack. This includes exploits of code-level vulnerabilities in the application as well as thwarting authentication mechanisms.
Top industries	Finance, Information, Retail
Frequency	5,334 total incidents (19,389 additional with secondary motivation), 908 with confirmed data disclosure.
Key findings	The breaches within this pattern are heavily influenced by information gathered by contributors involved in the Dridex botnet takedown. Hundreds of breaches involving social attacks on customers, followed by the Dridex malware and subsequent use of credentials captured by keyloggers, dominate the actions. Defacements are still commonplace and CMS plugins are also a fruitful attack point.

The great complexity of the infrastructure makes web application servers a target for attackers.

When Clippit was king

Websites aren't what they used to be, with a background of a tiled cloud image, the company name proudly displayed center top in Comic Sans and with identical animated gifs on either side. Combined with a healthy dose of ALL CAPS, <blink> tags and, of course, a site counter at the bottom with numbers that had just the right touch of drop shadow. 1997 was a simpler time. Now organizations have less ugly (typically), less static and more business-critical websites promoting their operations, conducting ecommerce and hooking into backend databases. Users are not merely reading a homepage and clicking on a couple of links to basic information about store hours, but are increasingly more interactive and issue various types of inputs to be read and acted upon by the web infrastructure. The greater complexity, including the web application code and underlying business logic, and their potential as a vector[15] to sensitive data in storage, or in process, makes web application servers an obvious target for attackers.

[15] They are likely/hopefully one of the only services that are internet accessible for an organization.

For starters, not all website compromises are targeted affairs. We had almost 20,000 incidents of websites that were popped used to either host malware, participate in distributed denial-of-service (DDoS) attacks or repurposed as a phishing site. We have no idea as to the method of compromise, nor the victim demographics and thus these instances of secondary motivation have been culled from the information that follows. About half of the incidents that remain were website defacements and the data we have on those was not enough to establish whether the motive was ideology, a personal grudge, or just for fun—so we combined them in Figure 23 below. Typically the hacking actions used to compromise were not known either, but in case you thought defacements, like the blink element, were an obnoxious thing of the past, think again.[16]

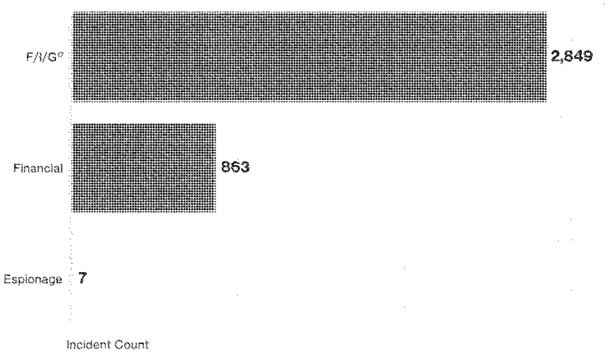


Figure 23.

External Actor motives within Web App Attack incidents, (n=3,720)

When we filter down into confirmed data disclosure, the financial motive flexes its muscle with 95% of breaches associated with criminals all about the cheddar.

95% of confirmed web app breaches were financially motivated.

Eco-friendly hacking—reusing and recycling passwords
When looking at the threat actions in Figure 24, a pattern within the pattern smacks us in the face with a glove and demands satisfaction. The top six actions narrate the story of the Dridex campaign better than Morgan Freeman combined with Sir David Attenborough ever could. These breaches, uncovered through the forensic analysis performed on several C2 servers tell the tale of phish customer > C2 > Drop Keylogger > Export captured data > Use stolen credentials.[18] Even with a particular spree inflating these numbers, the top six looked very similar to last year, albeit in a different order, and with phishing making an appearance in the top actions this year.

There are other stories beyond the botnet though. We wanted to know what other data points the use of stolen credentials was associated with when that spree was removed from the data. Phishing still showed a strong association in the pattern, but also mail servers. While masked at first in our data by the botnet, social engineering to acquire web-based email credentials

[16] If you are not familiar with the blink element, just Google "blink tag". We're sorry in advance.
[17] F/I/G is the combination of Fun, Ideology, or Grudge
[18] If "get funky" was a VERIS enumeration, it would surely be an extension of this attack chain.

was uncovered when peeling back the layers of the Web App onion. And they probably don't even have the black "I read your email" T-shirt to brag about their bounty.

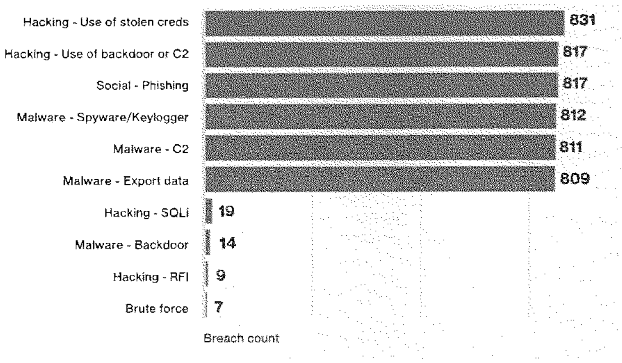


Figure 24.
Top 10 Threat action varieties within Web App Attack breaches, (n=879)

Wendell Wilkins injects web shells into the Web App.
We have seen content management systems (CMS) as the vector for installation of web shells,[19] which are also classified as a backdoor in our framework. Either exploiting a remote file inclusion (RFI) vulnerability, or abusing an insecure upload functionality, the web shells are injected and used as the gateway to additional mayhem. In financially motivated attacks against ecommerce servers, web shells are used to access the payment application code, which is then modified with a new feature that will capture the user input (think payment card number and CVV) for future pickup. As with prior years, this is backed up by other studies.[20] And it wouldn't be a proper DBIR if we didn't raise a glass to one of the elder statesmen of web application hacking, SQL injection (SQLi). It, like other vulnerabilities associated with web applications, stems from a lack of input validation allowing Actors to pass SQL commands via the web application and to the database. Lastly we want to thank AsTech Consulting, Imperva, and WhiteHat Security for scan data and mind melds around web application security.

In attacks against ecommerce servers, web shells are used to access the payment application code and capture user input.

[19] US-Cert.gov/ncas/alerts/TA15-314A
[20] Imperva's 2015 WAAR showed a strong correlation between RFI and Content Management Systems.

Recommended controls

Factor, meet factor.
Like that song you can't get out of your head. Here is another shot across the bow of single-factor, password-based authentication for anything of criticality. If you are securing a web application, don't base the integrity of authentication on the assumption that your customers won't get owned with keylogging malware. They do and will.

I value your input, I just don't trust it.
Validate inputs, whether it is ensuring that the image upload functionality makes sure that it is actually an image and not a web shell, or that users can't pass commands to the database via the customer name field.[21]

Unplug.
Worrying about OS and core application code is hard enough, but third-party plugins are also gray-hair-inducing. Establish a patch process for CMS platforms and third-party plugins.

[21] Still great: XKCD.com/327/

Point-of-Sale Intrusions

Point of sale devices continue to be a reliable source for stolen payment card data.

At a glance

Description	Remote attacks against the environments where card-present retail transactions are conducted. POS terminals and POS controllers are the targeted assets. Physical tampering of PED[24] pads or swapping out devices is covered in the Payment Card Skimmers section.
Top industries	Accommodation and Food Services, Retail
Frequency	534 total incidents, 525 with confirmed data disclosure.
Key findings	Headline-grabbing remote payment card breaches have shifted from large retailers in 2014 to hotel chains in 2015. Use of stolen credentials to access POS environments is significant. Command and control functionalities are being reported at a much higher rate than in years past, although this may be in part due to an underrepresentation of C2 functionalities as opposed to a 2015 trend. RAM scraping continues to be omnipresent in 2015, but keylogging malware has a significant role in many POS attacks, being a common method of capturing valid credentials to be used against POS assets. Continuing the trend of the last several years, the sprees (single threat Actor, many victims) represented in this data are a byproduct of successful attacks against POS vendors and cannot be attributed to automated attacks targeting poorly configured, internet-facing POS devices.

The well, revisited

It should be no surprise to anyone that this pattern is alive and well in the 2015 dataset. There are still folks out there seeking to get paid and looking to stolen payment card data as the means to meet their greedy objectives.

22 Personal Identification Number (PIN) Entry Device

Point-of-sale devices continue to be a reliable source for this data, notably the POS terminals that directly consume magnetic stripe information from customers, or POS controllers that typically act as an aggregator of transactional data from the terminals in a server-to-client relationship.

In small businesses, the POS environment may have a population of one, with a lone computer processing payments and communicating out to the payment processor. This device might also (unfortunately) be used for checking personal email, social media breaks and other interwebby activities that introduce more risk to the POS application which is all alone, with no anti-virus or host-based firewall to talk to.

Four or five years ago, our findings were dominated by POS breaches—simplistic and automated in nature and making full use of known default vendor credentials. We lovingly called these POS Smash and Grabs, and this attack method was one that we saw over and over again and helped drive us to the development of incident classification patterns. The gist of these, if this is your first DBIR rodeo, is: 1) POS server is visible to the entire internet, 2) POS has default login, 3) Bad guy leverages 1) and 2) to install malware and 4) Malware grabs the payment card data as it is processed. This scenario was, and still is, a small business problem. It did, however, offer some insight into what was to come for larger organizations.

The 2015 DBIR detailed the rise of larger organizations suffering POS breaches and their representation in this pattern. While 1) and 2) were not present in these breaches, raising that fruit a little higher from the ground, there are some definite similarities. Both the smash and grabs and large organization breaches took advantage of static, single-factor authentication. Attackers have had to up their game a bit, having to do some work to compromise valid and assumed-to-be non-default, credentials to access the environments. Moreover, they have issued the stolen credentials from a foothold on the network as opposed to directly from the internet.

Attackers have had to up their game to compromise valid credentials and access the environments.

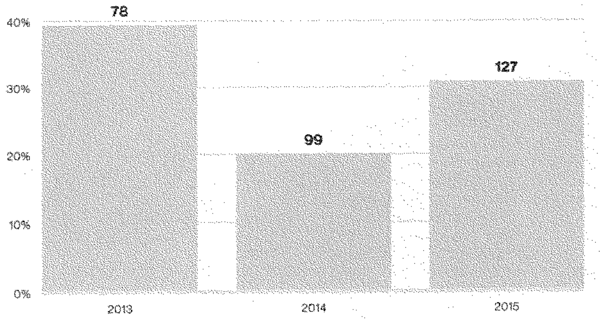


Figure 25.
Three-year chart of % and number of breaches using stolen credentials within POS Intrusions, (n=1,103)

Figure 25 shows the prevalence of stolen passwords in the POS Intrusion pattern. Brute force is still relevant, but we hope it will continue to decline as small and medium businesses move away from passwords that could be guessed by a rhesus monkey of average intelligence.

Vendor as a vector

The vector associated with the hacking actions tells an interesting story as well. Ninety-seven percent of breaches featuring use of stolen credentials also had a vector of Partner. This is selected when the Actor uses legitimate partner access in the hacking action. This year continued the trend of the criminal sprees in our data being associated with attacks against POS vendors followed by using their access into their customer base.[23] Bill Gates once said "Your most unhappy customers are your greatest source of learning." With all of their customers equally unhappy, the amount of learning some POS vendors have acquired must have been like Neo's martial arts training.[24]

97% of breaches featuring stolen credentials leveraged legitimate partner access.

The other similarity of large and small organizations is that malware is the workhorse of POS breaches. Figure 26 shows the most common malware functionalities. We have seen the evolution from "off-the-shelf" keyloggers, to memory scraping malware (RAM scrapers), to POS-specific RAM scrapers with names like BlackPOS and PoSeidon (in case you weren't sure what they were designed to attack). Exfiltration has evolved from static code within the malware to FTP data to a single destination, to utilization of a C2 infrastructure to ship the captured data out.

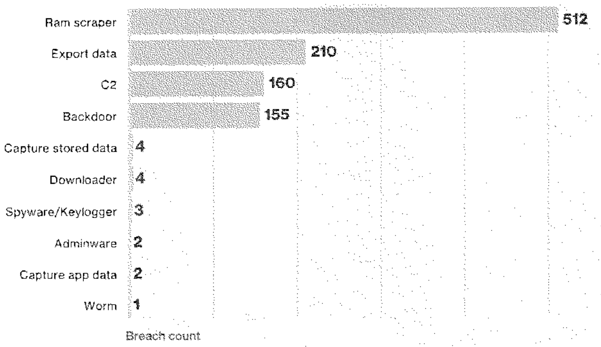


Figure 26.
Malware varieties within POS Intrusion breaches, (n=521)

Both C2 and Backdoor are more prevalent this year than in years past. The reality is that POS malware families are typically multifunctional and some of the most notorious (Dexter, vSkimmer, Alina, Backoff, JackPOS ...) have command and control/backdoor capabilities. In many cases, it is easier to prove the use of one functionality (the one that stole the data) than others (C2 beaconing). Many of the POS Intrusion incidents did not have the evidentiary logs needed to validate outbound communications. Long story short, the spike in C2 and Backdoor may very well be a product of better windows into the entire behavior of the malware.

[23] The actions used in this scenario are examined more closely in the Wrap Up section as it features combinations of many of the top threat action varieties that are also found in other patterns.
[24] "I know kung fu."

Recommended controls

Not trying to give you static, but...
Static single authentication is a weakness that is used in spades by the attackers. If possible, improve this with a second factor such as a hardware token or mobile app, and monitor login activity with an eye out for unusual patterns. Have a conversation with your vendors and ensure that they are using strong authentication to access your POS environment.

Who can it be, knocking at my door?
Find out what monitoring options are available for your POS environment and validate their implementation. Track remote logins and verify any and all that are against the norm.

Segmentation, seriously
Separate the POS environment from the corporate LAN and ensure that it is not visible to the entire internet.

Insider and Privilege Misuse

The Privilege Misuse pattern is one of the few that includes collusion between internal and external Actors.

At a glance

Description	All incidents tagged with the action category of Misuse—any unapproved or malicious use of organizational resources—fall within this pattern. This is mainly insider-only misuse, but outsiders (due to collusion) and partners (because they are granted privileges) show up as well.
Top industries	Public, Healthcare, Finance
Frequency	10,489 total incidents, 172 with confirmed data disclosure.
Key findings	They're behind your firewall, getting all up in your data. They are often end users and they are comfortable exfiltrating data out in the open on the corporate LAN. Insider incidents are the hardest (and take the longest) to detect. Of all the incidents, these insider misuse cases are the most likely to take months or years to discover.

The disgruntled insider—we all have an idea in our minds of what this person looks like. Perhaps it is the software developer who is frustrated with management; maybe it is the healthcare worker who has been recruited by organized crime; or maybe it is that guy in the basement grieving the loss of his red stapler. Regardless of what they look like, the fact is they are inside our carefully constructed defenses and they are wreaking havoc with our data.

The Insider and Privilege Misuse pattern is one of the few that sees collusion between internal and external (or even partner) Actors. Figure 27 shows the percentage of these breaches where multiple Actors are present.

These are most frequently an external/internal pairing, but ruling out partners as potential colluders is a mistake. The break from the norm that we saw was the rise in misuse breaches tied to external Actors only. This was normally solely associated with TGYFBFTDHRA,[25] but this year we had cases where

[25] That guy you fired but forgot to disable his remote access.

instead of organized crime soliciting insiders to provide banking information, they went to the customer. It was actually external > external collusion to commit fraud.

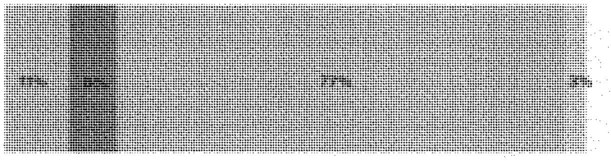


Figure 27.
Percent of breaches per threat Actor category within Insider and Privilege Misuse, (n=172)

The butler did it.
Back to the insiders—who are they? When their roles were classified in the incident, almost one third were found to be end users who have access to sensitive data as a requirement to do their jobs. Only a small percentage (14%) are in leadership roles (executive or other management), or in roles with elevated access privilege jobs such as system administrators or developers (14%). The moral of this story is to worry less about job titles and more about the level of access that every Joe or Jane has (and your ability to monitor them). At the end of the day, keep up a healthy level of suspicion toward all employees. While we would like to think they will never give you up, let you down, run around or desert you, we simply can't (tell a lie, and hurt you).

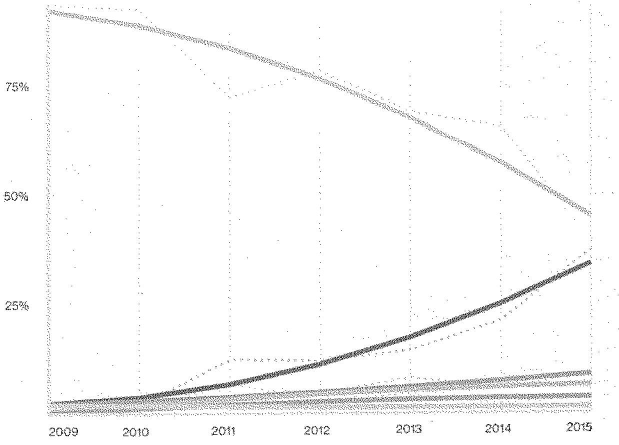


Figure 28.
Actor motive over time within Insider and Privilege Misuse, (n=715)

The why and how
What motivates them? Most frequently it is the potential for financial gain (34%), although the espionage motivation (25%) continues to be associated with these breaches. Figure 28 shows how the motivation of these Actors

has changed since 2009. It is interesting to see the potential convergence of the financial motivation and the espionage motivation. While this also reflects the change in the dataset as we progress over time, the rise of the espionage-motivated insider should give organizations reason to consider implementing processes to detect when exiting employees may have taken valuable data with them.

Figure 29 lists the top varieties of Misuse within the Insider and Privilege Misuse pattern. When the nature of their actions is known, the general privilege abuse is always at the top of the list. This is merely using access to gain information for alternative and unsanctioned uses. Data mishandling follows and typically involves mailing sensitive information or loading to a sharing service. Many times this is not done with malicious intent, but for a convenience factor. Use of unapproved hardware and software are the third and fourth most common varieties of misuse. The unapproved hardware is usually either a USB drive (used to store information to be used later, like, when employed at another company kind of later) or a hand-held skimmer that we have seen food servers use to capture diners' payment card data.

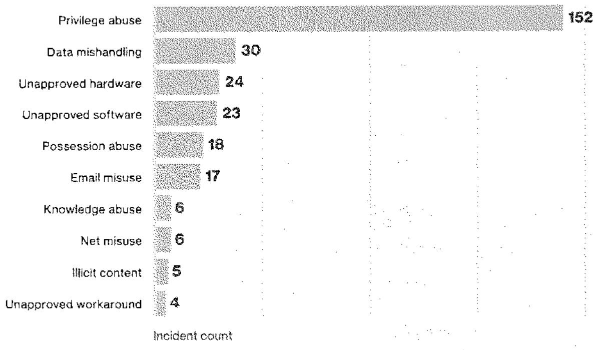


Figure 29.

Top Misuse action varieties within Insider and Privilege Misuse, (n=230)

The actions of insiders are among the most difficult to detect and the discovery timeline (Figure 30) illustrates this point. In our graphic we show the majority of these incidents are taking months or longer to discover. In fact, when we looked at the overall DBIR dataset, we found that the incidents that take the longest to discover were these inside jobs. The shift from days to months led us to look at what was different. We found that there were more cases where bank employees provided info that was used for fraud–and was discovered quicker–in years prior. For organizations that will not have fraud detection in their arsenal, the shift is likely more representative of their world.

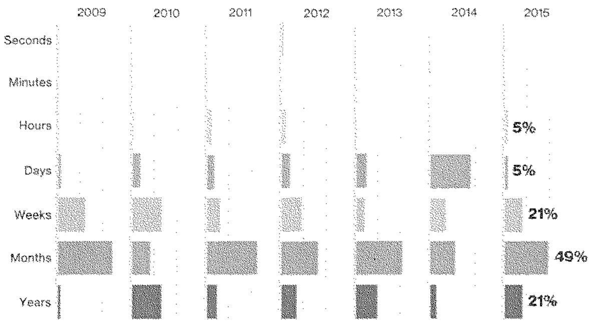


Figure 30.

Discovery timeline within Insider and Privilege Misuse over time, (n=358)

Recommended controls

The evil within

So love your employees, bond at the company retreat, bring in bagels on Friday, but monitor the heck out of their authorized daily activity, especially ones with access to monetizable data (financial account information, personally identifiable information (PII), payment cards, medical records).

USB wary

Our dataset included numerous instances of audits being performed after an employee had left, which uncovered evidence of a USB drive used to transfer data prior to their departure. It makes sense to take measures to identify use of these portable drives sooner rather than later.

Keep one eye on your data and the other on your employees!

You cannot effectively protect your data if you do not know where it resides. Likewise, it does you little good to know where it is but then pay no attention to who has access to it. Make sure that you are aware of exactly where your data is and be careful who you give privileges to and to what degree. It makes sense to give the valet attendant your keys to park your car, but not to hand over your credit cards as well.

You can't effectively protect your data if you don't know where it resides.

Tougher penalties for data breaches

Almost without exception, every international fraud and business crime case that Mishcon de Reya LLP has advised on in the past 12 months involved the use of computer equipment and electronic data. For a company that falls victim to cybercrime, there are immediate financial ramifications from loss of revenue while systems are down, the unlawful exploitation of valuable data that has been stolen, or possible claims faced from the queue of litigants seeking compensation. Additionally, there can be a broader impact on customer trust and confidence following an incident that can lead to reputational damage that is more difficult to quantify.

Yet, there is huge inconsistency and discrepancy in the way that governments are tackling this problem. Many believe that the legislation is out of date with technology and too weak to combat the problem with any meaningful sanction. There is widespread confusion and enhanced regulatory risk as businesses are forced to comply with radically different laws as their data passes from one country to the next.

In the US, there are a multitude of privacy and data security laws but no specific and comprehensive federal law, and no official national authority responsible for enforcing it. As a member of the European Union, the UK implemented the European Union's 1995 Data Protection Directive 95/46/EC with the Data Protection Act 1998. The Information Commissioner's Office is responsible for enforcing it and upholding information rights, but the ICO is championing tougher sanctions, including prison sentences rather than fines, to deter theft and trading of personal data. At the moment, there is no mandatory reporting obligation in the UK under the data protection legislation and the toughest penalty that the ICO can impose is a £500,000 fine (about $700,000) for the most serious of data breaches. As such, the legislation lacks the necessary teeth to properly deter misuse of personal data.

While there is other criminal legislation law enforcement can use to combat cybercrime more broadly, the authorities in the UK and elsewhere face difficult and expensive jurisdiction hurdles as offences routinely cross borders, requiring authorities to cooperate internationally to investigate acts, then extradite and prosecute criminals. With huge volumes of encrypted data, proxy servers masking true IP addresses, secure VPNs and anonymous currency exchanges used by criminals, many authorities are falling at the first hurdle in terms of finding the necessary evidence to support a prosecution. Unfortunately, there is still a long way to go before the scale and rate of cyberattacks is brought under control by effective legislation.

Hugo Plowman and Rob Wynn Jones, Partners – Mishcon de Reya LLP

Miscellaneous Errors

At a glance

Description	Incidents where unintentional actions directly compromised a security attribute of an information asset. This does not include lost devices, which are grouped with theft instead.
Top Industries	Public, Information, Healthcare
Frequency	11,347 total incidents, 197 with confirmed data disclosure.
Key findings	Misdelivery of information both in paper and digital form remains the most prevalent variety of error.

The most common error of losing stuff is so common, it was deemed worthy of its own pattern.

People aren't perfect.
With all of the hubris and bravado in the InfoSec world, one proclamation we usually don't hear is "Our employees NEVER make mistakes." Well, because they do. Everyone does and this is the section where we talk about breaches caused by the people saying "Oops, my bad". An important distinction that will be familiar to those with strong VERIS-fu is that we take a very narrow approach to the Miscellaneous Errors action category. If you got hacked due to the lack of any patch process or validation, then that is not an error. The action or inaction was not a direct cause of the data loss (the bad guy still had to get his hack on). To ensure that every incident we come across isn't rubber-stamped as an error due to less-than-perfect security practices, we limit its use to only when the action is the direct cause of attribute loss. And because the most common error of losing stuff is so common, it was deemed worthy of its own pattern along with stolen assets on page 43. As in prior reports, due to the influx of thousands upon thousands of misdelivery incidents from the public sector[26] that tried to steal the show, we have removed them in the interest of finding actionable tidbits of information that would never have a voice otherwise.

Data errors reduce productivity (DERP).
Traditionally, this pattern has been dominated by the Trio of Trouble: Misdelivery, Publishing and Disposal errors and they make their annual appearance in Figure 31. Last year we grew our corpus to include data that

[26] Public sector misdelivery incidents was. (n=10,094)

shed light on availability issues caused by non-malicious spikes in traffic. Those capacity shortage errors lead the way this year, followed by worker bees either sending emails or documents to the wrong recipients. Classified as Misdelivery errors, these events have seen many a person curse the existence of autocomplete in their Outlook To: field.

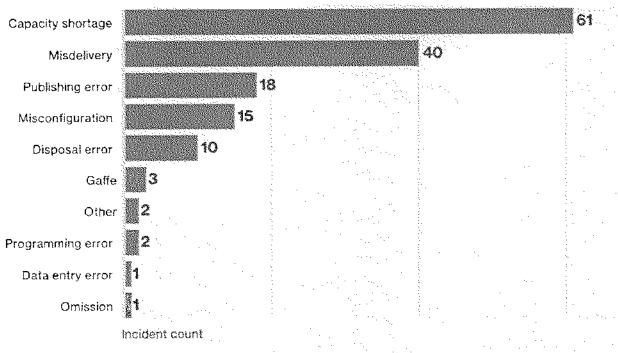


Figure 31.
Top 10 threat action varieties within Miscellaneous Errors, excluding Public, (n=153)

Publishing information where an unintended audience (e.g., the entire internet) is able to view it remains in the top five. As does misconfiguration—mistyping a firewall rule allowing access to a sensitive file server from all internal networks instead of a specific pool of hosts would be a fine example.

Rounding out the top five is disposal errors. These are primarily documents, which is concerning, since that data is in human-readable format—look Ma, no controls! While not as common in our dataset this year, proper wiping of hard drives on decommissioned devices must also be standard operating procedure for organizations.

A note on data disclosure—for the VERIS field name data_disclosure to be "Yes," there must be some indication that data was actually viewed or accessed by an unauthorized individual. The following are example scenarios and guidance on how this variable is set:

- Unencrypted stolen or lost device: Potentially
- Encrypted stolen or lost device: No
- Improperly disposed documents or devices: Potentially
- Accidentally publishing private data to a public website (no evidence that anyone viewed it): Potentially
- Misaddressed envelope that was never traced or recovered: Potentially
- Misaddressed envelope that was opened by the incorrect recipient: Yes
- Scenarios not marked No or Potentially will change to Yes if discovered by an outside party. For instance, if an external party notifies the victim of a publishing error, the data is, by definition, disclosed.

When errors lead to data spills, it is still more common to find out from the customers affected by the mistake. One or several of the recipients of someone else's PII or medical information will reach back out to the organization to clue them into the off-by-one error. Figure 32 shows the top discovery methods for breaches in the Miscellaneous Error pattern.

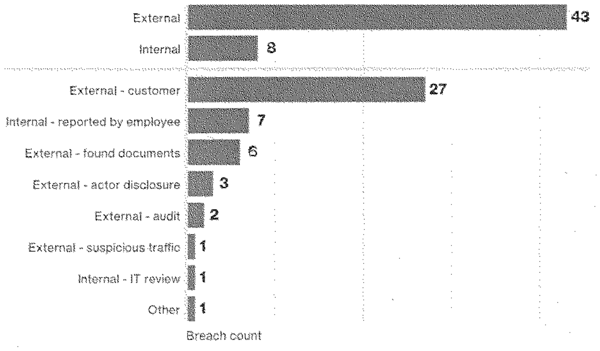


Figure 32.
Discovery methods of breaches within Miscellaneous Error excluding Public. (n=52)

Recommended Controls

There is perhaps an element of absurdity in recommending controls for the Error section. One can't really say "don't screw up again", or "pay attention to what you are doing for Pete's sake". Nevertheless, there are some common sense practices that can be implemented to help keep errors to a minimum. After all, with all the crooks trying to ruin us, the least we can do is try not to help them.

Learn from your mistakes!
Keeping a record of common errors that have plagued your organization can be used for something other than to mock fellow employees at the company Christmas party. Collecting this information can be used to implement new training materials for security awareness. Did Jim in accounting cc: everyone in to his latest rant again? Talk about it. Just don't mention Jim by name. Incorporate frequent "Oops moments" into security training.

Ensure that all assets go through a rigorous check by the IT department before they can be decommissioned or disposed of.

"I'm the map, I'm the map, I'm the map, I'm the map, I'm the map!"
Now that you are keeping a record of wrongs (love may not do it, but wise IT departments do), use that data to map the most common errors to effective controls that can help to minimize the frequency with which they occur, and mitigate the damage they do when they do take place.

Stop trash talking!
When assets are ready for disposal, make sure that there is a documented procedure for wiping all assets before they are trashed or resold. Ensure that any and all assets go through a rigorous process of check and recheck by the IT department before they can be decommissioned and disposed of. Our dataset is rife with examples of assets being sold to a third party while chock-full of PII and other sensitive data.

Physical Theft and Loss

At a glance

Description	Pretty much what it sounds like—any incident where an information asset went missing, whether through misplacement or malice.
Top industries	Public, Healthcare
Frequency	9,701 total incidents, 56 with confirmed data disclosure.
Key findings	When we look at all incidents, laptops are the top asset affected by this pattern. However, for confirmed breaches, it is the documents, with their lack of controls, which result in the most confirmed disclosures. Lost assets were over 100 times more prevalent than theft.

For non-encrypted devices, the determination of a breach can be tough, given that you no longer have custody.

Humans, what are you gonna do?
If you have young children, the next time you are in their school take a gander at the horror show known as Lost and Found. You will see what appears to be at least 2.5 articles of clothing per student shoved in a bin and left there long enough to form a single brick of coats, hats, gloves and unidentifiable pieces of fabric that entered—but like Charlie on the MTA—never returned home. People lose things all the time—this is not new or particularly newsworthy. It is, however, a real-world pain in the neck for organizations that are at best replacing Scooter's laptop, or at worse scrambling around to figure out if there was PII on the device and whether encryption had been implemented. And if the fallibility of Scooter weren't enough, there are still people that want something and don't wanna pay for it. So to sum this pattern up in haiku form:

Employees lose things
Bad guys also steal your stuff
Full disk encryption

Same old story, same old song and dance
We defined more specific guidelines on data disclosure in the sidebar featured in the Miscellaneous Error pattern. For non-encrypted devices, the

determination of a breach can be tough, given that you no longer have custody of the computer in question. Is the data on that system at risk? Certainly, since it is trivial to bypass the sole control—the password. Still, we cannot by our definition, in most cases of lost computing devices, label them as a confirmed data breach. This discrepancy between the number of confirmed breaches and the number of incidents in this pattern shows that there is quite a bit more data in the at-risk category than the number of confirmed breaches implies.

Based on all the incidents in this pattern, laptops are the most common target. However, when we narrowed our research to confirmed breaches, documents are in the lead due to the ability to infer that the finder or thief can read the language in which the information is written.

Physical theft is a problem that we have seen time and again, and these incidents most commonly occur in the victim's own work area (39%) or from the personal vehicle of the employee (33.9%). That said, these items are being lost far more often than they are being stolen. In this year's data, an asset is lost over 100 times more frequently than it is stolen. At the end of the day, the impact is the same—the laptop is gone and likely wasn't turned into Lost and Found.

In this year's data, an asset is lost over 100 times more frequently than it is stolen.

Recommended controls

Just do it.
Full disk encryption on all mobile devices and removable media—make it part of the standard build.

Changes in attitudes
Keep hope alive that security and situational awareness will become ingrained in your users. Include physical security of corporate assets as part of their orientation and ongoing training. Reiterate that cars are not an appropriate place to leave laptops. Cars have windows which thieves have proven that they can not only see through, but also break to get what they want.

Dead trees
Rein in the paper as much as feasible given your business. Establish data classification and make it a policy violation, with potential consequences, to print and transport sensitive data. Consider tokenizing to replace sensitive information with an alternate unique identifier when printed copies are required.

Crimeware

At a glance

Description	Any incident involving malware that did not fit into a more specific pattern. The majority of the incidents that comprise this pattern are opportunistic in nature and have a financial motivation behind them. This pattern frequently affects consumers and is where "typical" malware infections will land.
Top industries	Public, Information, Finance
Frequency	7,951 total incidents (6,858 additional with secondary motivations), 49 with confirmed data disclosure.
Key findings	The Crimeware pattern continues to be driven by external organized criminal groups that are financially motivated. Establishment of control over a device using C2 malware followed by ransomware, then the targeting of credentials or enrollment into a botnet accounts for the majority of the incidents.

Typically, these are high-frequency, low-impact annoyances that will not receive a full forensics investigation.

Since the expansion of our data contributors and the advent of the patterns, Crimeware has historically been generous in the number of cases, but not so rich in detail. The majority of the incidents found in this neck of the woods come (in bulk) from CERT/CSIRT organizations, who receive them from a wide variety of organizations. These are typically high-frequency, low-impact annoyances that will not receive a full forensics investigation and/or be documented and categorized. We focus on the smaller subset of incidents where the fidelity is higher and use those as predictors into the nature of the rest. This year we also will be delving into malware data received from our security vendor contributors (many thanks to Cylance, Fortinet, ICSA Labs, Palo Alto Networks and Tenable) to shed some light on certain areas.

When the functionality of the malware was known, C2, ransomware, spyware/keylogger, and backdoor and export data were the top five functionalities (see Figure 33). Notably absent is malware designed to DoS another target—these were culled with the secondary motive filter discussed on page 8. Over

6,800 instances of identified devices launching traffic at unknown victims would have dominated the numbers in such a way that it would deter from the usability of the data.

Ransomware, in the number two spot, realized the biggest jump in our data and this will continue to be an element that we track. In case you missed it, ransomware is malware that encrypts files resident on the infected device and, in worst cases, attached file shares. Extortion demands follow, leveraging the need for availability of the data. This is cut from the same cloth as denial-of-service extortion, but typically is opportunistic in nature and affects organizations and consumers alike.

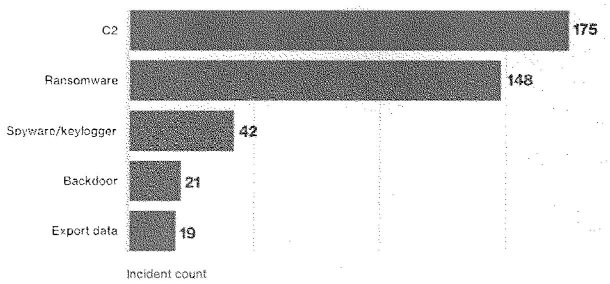


Figure 33.

Top five malware varieties within Crimeware, (n=382)

The rest of the top five draw out a very familiar pattern involving banking Trojans. The criminal groups behind these families of malware know that you need to control your infected minions (C2/backdoor), and you need to capture (keylogger) and send (export data) the banking credential information—so these are the tools of the trade. These functionalities are top-heavy this year, but are by no means new or indicative of an upward trend.

Generally speaking, there are three major avenues for crimeware installation, either via emails with malicious attachments, websites serving up drive-by downloads with each visit, or a hybrid of the two—emails with links to pages with, you guessed it, drive-by code installs.

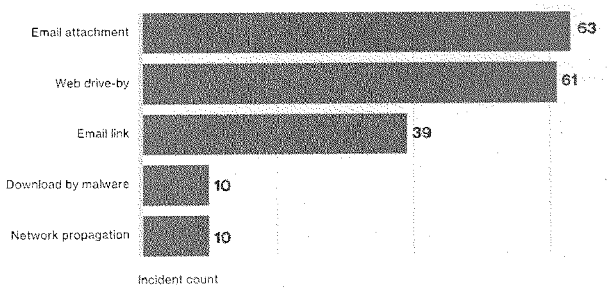


Figure 34.

Top five malware vectors within Crimeware, (n=135)

Do you want ransomware? Because that's how you get ransomware!
We stated earlier that because run-of-the-mill malware does not always merit incident responders rappelling in through skylights and cloning drives, it is a bit light on details. We did however receive a group of ransomware cases where the vector was known (hooray!) and what was specifically exploited (Flash). Even better was that we had the version of Flash exploited and the current Flash version. We thought, "This could be interesting—how bad can people be at updating Flash?" The answer is, very bad. This is a small sample size, but the results were still eye-opening. We aren't putting this here to ring the shame bell at anyone, but Figure 35 shows that over one half of these browsers were rocking Flash versions that were over a year older than the current revision. The speed of Lewis Hamilton was not required for the majority of these drive-by downloads; the pace of a horse-drawn carriage would have done just fine. It should be noted that some organizations with more togetherness in their act also fell victim, with one having a version that was current and another only two weeks older than the latest iteration.

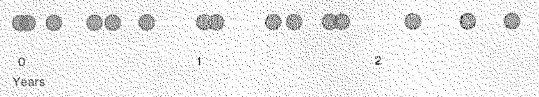


Figure 35.
Time from release date of exploited Flash version to release date of current version at time of exploitation (n=15)

We look to non-incident data for the rest of this section to provide some more malware information. We first wanted to reaffirm what we found last year regarding the uniqueness of hashes.

To hash or not to hash? Let's not.
Last year we burst many a bubble by calling out that a unique hash does not mean you have been targeted by an ultra-sophisticated group of nation state malware ninjas.

This year, we compared hashes out of a total of 40 million records of malware from several contributors and noticed that again there was little overlap across organizations. When investigating for commonalities, we saw that about 20,000 MD5 hashes existed across multiple organizations out of almost 3.8 million unique hashes.

We then looked at how long hashes were used for. Drumroll please… not long.

And poof, he's gone.
We then looked at how long hashes were used for. Drumroll please … not long. When looking at the difference between when a hash was first seen versus when it was last seen, we saw that the count of hashes over this time difference was very much long-tailed (see Figure 36 below). The vast majority were used for a very short period of time and then dropped off the face of the network.

Analysis of one of our larger datasets showed that 99% of malware hashes are seen for only 58 seconds or less. In fact, most malware was seen only once. This reflects how quickly hackers are modifying their code to avoid detection.

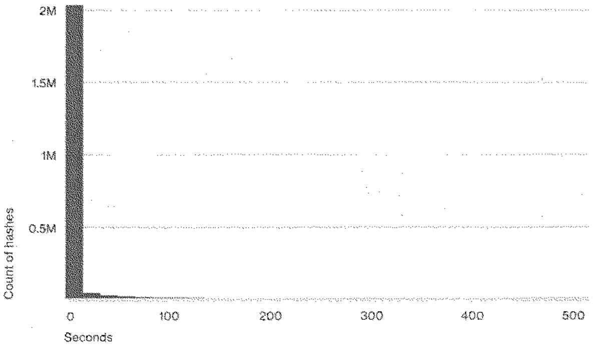


Figure 36.
Count of hashes by lifespan in seconds. (n=2.3 million)

Recommended controls

Where be me eye patch, matey?
We know that malware droppers, in many cases, succeed by exploiting known vulnerabilities, so utilize those patches that your vendors release for your OS, applications (cough, browsers, cough) and security tools.

The lifespan of malware hashes is short and not so sweet.

Exes, stop calling!
Defending against malicious executables ranges from not allowing programs to run scripts/macros (e.g., document-based programs) to having your email server strip/remove executables or other file extensions as attachments in emails. Less is more in this scenario, as you will be reducing the attack surface.

Don't monkey around.
Don't be like the three wise monkeys here. See, listen and discuss. As suggested in last year's report, capture malware analysis data in your own environment; actually look into the different families of malware in your own organization and, if at all possible, the entry point.

Payment Card Skimmers

At a glance

Description	All incidents in which a skimming device was physically implanted (tampering) on an asset that reads magnetic stripe data from a payment card (e.g., ATMs, gas pumps, POS terminals, etc.).
Top industries	Finance, Retail
Frequency	102 total incidents, 86 with confirmed data disclosure.
Key findings	There continues to be little variation in this pattern. Actors from Eastern Europe favor this attack type, with ATMs the target of choice and the discovery method remains largely external.

70% of Payment card skimming incidents in our dataset can be blamed on criminal organizations.

"Third verse, same as the first"
In a world full of chaos and change, it is a comfort to know that you can rely on certain things to stay relatively constant. For instance, your bread will always fall buttered-side down, your distance from a bathroom will remain in direct proportion to the urgency of your need for one and skimming won't really change much from year to year. That is probably because the crooks were raised in the "If it ain't broke, don't fix it" school. Payment card skimming remains one of the most lucrative and easy to pull off crimes, both for organized criminals and the occasional independent pilferer (he's just a poor boy, from a poor family).

Due to the fact that these incidents come mainly from US-based law enforcement, our data is almost entirely US-centric with regard to victim location. However, since the bulk of it can be blamed on criminal organizations (approximately 70%), we can sometimes ascertain which countries those organizations are tied to. Figure 37 shows that just as in years past, Eastern Europe—namely Romania and Bulgaria—accounts for the bulk of the attacks in which a known organization can be identified.

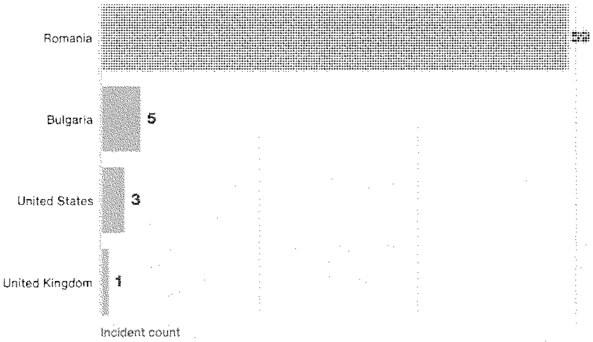


Figure 37.
Actor country within Card Skimmers, (n=68)

Also reflecting past trends, the vast majority of breaches in this category were related to ATMs (94%), with gas pump terminals coming in second (5%) and PIN entry devices (PEDs) barely making an appearance (1%). The physical action of 'surveillance' was selected in over 90% of cases—this is due to the installation of pinhole cameras designed to capture PIN codes on the devices in question. As in prior years, the skimmers can be, and often are, constructed with extreme precision and great detail and are difficult, if not impossible, to detect with the naked eye (or for that matter, even with eyes that are fully clothed in contacts or spectacles). This may account for the fact that discovery as displayed in Figure 38 is almost all external, and mostly via fraud detection utilizing algorithms and Common Point of Purchase (CPP) mechanisms.

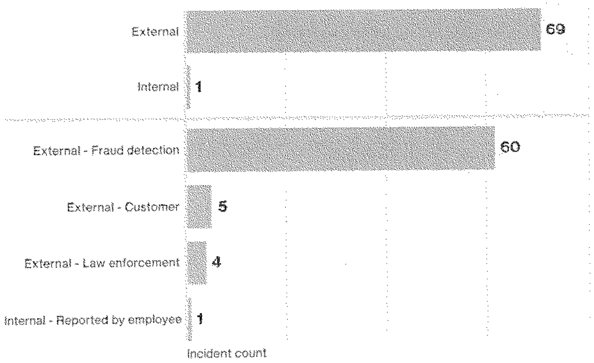


Figure 38.
Discovery methods within Card Skimmers, (n=70)

"And finally... some bad news"
With regard to discovery timelines, we discussed last year that detection times were getting better, and were leaning heavily toward the 'days' category rather than 'weeks' or 'months'. This year, we do not see that shift continuing. On the contrary, discovery times are firmly entrenched in the 'weeks' this year.
There is a dramatic decline in internal discovery and a corresponding increase in discovery by fraud detection in our dataset this year. It is not clear whether the employees of victim organizations all need a better prescription vision plan, or whether it is simply that those victims who discover the tampering themselves quickly remove the devices without reporting it to law enforcement (or not to the agencies that partner in this research). Naturally, it is quicker to discover skimming-related theft when you see it with your own eyes than it is to wait for signs of CPP to appear, so the relative change in each category would make sense.

There is a dramatic decline in internal discovery and a corresponding increase in discovery by fraud detection.

Recommended controls

Merchants

- Purchase tamper-resistant terminals: Certain designs are more susceptible to tampering than others. Some models of ATMs are designed with this in mind. Look to those when purchasing new equipment.
- Use tamper-evident controls: When possible, do things that will help to make it clearer when tampering occurs. For instance, apply stickers over the door of the terminals and monitor video footage of the ATMs and gas pumps to see if anyone has tampered with the equipment.
- Time for a checkup: Establish a process to check the physical integrity of ATMs. Employees can be trained on how to spot evidence of tampering and seek it out as a scheduled task.

Consumers

- Guard your PIN: When entering your PIN, cover your hand so that any pinhole camera can't see what you are entering.
- Trust your gut: If you think that something looks odd or out of place, don't use it. While it is increasingly difficult to find signs of tampering, it is not impossible. If you think a device may have been tampered with, move on to another location, after reporting to the merchant or bank staff.

Cyber-espionage

At a glance

Description	Incidents in this pattern include unauthorized network or system access linked to state-affiliated Actors and/or exhibiting the motive of espionage.
Top Industries	Public, Information, Manufacturing
Frequency	247 total incidents, 155 with confirmed data disclosure.
Key findings	Espionage begins with the same threat actions as many other patterns to gain access, but will deviate as needed once the initial compromise occurs.

The Actors are predominantly state-affiliated groups. Competitors and nation states are also mixing it up.

Espionage, cyber-espionage

Unlike Bond movies, Cyber-espionage has a glaring lack of machine-gun umbrellas, henchmen with razor-rimmed hats and tear-gas-laden briefcases.

It does, however, have a diverse victim demographic, and while the villains may not be exfiltrating data to an underground fortress disguised as a volcano, they are certainly more skilled and patient than your script kiddies. If you want to dig into some dossiers, see the research studies by some DBIR contributors and others wearing the white hats in the Cyber-espionage Research sidebar.

First, let's define the pattern for you. Cyber-espionage features external threat Actors infiltrating victim networks seeking sensitive internal data and trade secrets. Incidents where an employee steals the customer database and sets up his own lemonade stand will fall into the Privilege Misuse pattern. The Actors are predominantly state-affiliated groups, although organized criminal groups, competitors and nation states are also mixing it up. Figure 39 shows the top victim demographics are the same popular targets as last year: Government, Manufacturing, followed by Professional and Information services. Beyond the top four, we have a smattering of other industries that show that <obvious>if you have something someone can use to their advantage, you are a potential target of Cyber-espionage</obvious>.

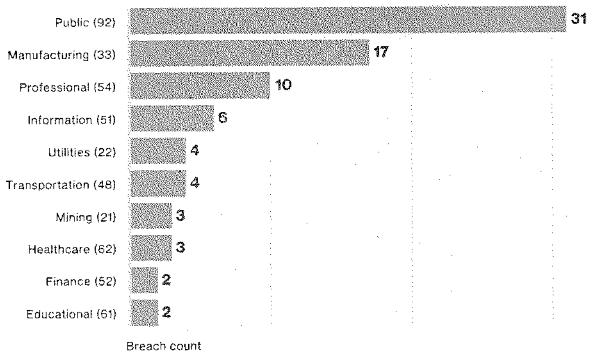


Figure 39.
Number of breaches by victim industry within Cyber-espionage. Numbers within parentheses are the industry NAICS codes. (n=86)

Insist to persist

We will admit here and now that our view into the specific tactics of these adversaries is front-loaded and focuses on the tactics used to gain the foothold. Many of these breaches begin with the tried and true mirepoix of phishing, dropping some backdoor and/or C2 malware, and then using that malware for the entry point. Phishing, as a leading action, provides a number of advantages over many other exploit approaches. The time to compromise can be extremely quick and it provides a mechanism for attackers to target specific people in an organization. And by using a service that is necessary for business communication to the internet, it allows an attacker to bypass many security devices and gain a foothold on an endpoint in the organization from a remote attack.

When phishing isn't the vector for the persistent malware installation, the browser is. Drive-by downloads leveraging browser or common plug-in vulnerabilities are utilized to accomplish the same mission—compromise a desktop on the corporate LAN and go from there. While targeting specific individuals may not be as feasible, the targeting of specific sites that are likely to be visited by certain sectors is. Strategic web compromises allow the adversary to leverage a vector more associated with opportunistic Crimeware to begin their assault.

Phishing, as a leading action of cyber-espionage, provides a number of advantages—the time to compromise can be extremely quick and attackers can target specific people.

After the initial access is established, what happens next is dependent on the location of the data and the obstacles that the adversary must overcome to reach the finish line. It goes without saying that the obstacles in your internal environment should resemble a Warrior Dash more than a kid's potato sack race, but more on that later. Looking at Figure 40, we can infer a bit more of the storyline via the combination of footprinting of the network and utilizing stolen credentials for advancing the attack. While we don't have the specifics on what methods were used to acquire credentials, there are a lot of breaches with unspecified malware and if we were to bet on it, keyloggers and password dumpers would be our educated guesses on the tools selected for that stage of the game.

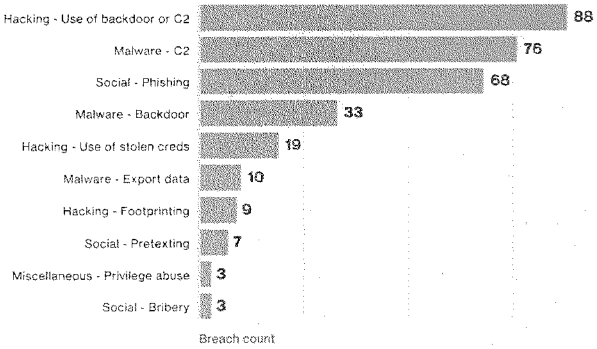


Figure 40.
Top threat action varieties within Cyber-espionage, (n=154)

That's my ex, Phil.
Trade secrets, aka proprietary information, are the most common data variety captured in Cyber-espionage breaches, present in over 90% of cases. Also represented are data types that help map out a path (configuration information gleaned from footprinting and fingerprinting the environment) and provide a means to move around in the network (credentials).

90% of Cyber-espionage breaches capture trade secrets or proprietary information.

Recommended controls

Cyber-espionage Actors put on their pants the same way we all do. It's just that after their pants are on, they persistently and patiently compromise terabytes of data. In the DBIR, we've seen that the threat Actors will start with simpler tools and techniques before moving on to more sophisticated attacks. For this reason, basic protections are still critical to guard against these types of threats, in addition to specialized protection.

Endpoint protection

Malicious software was involved in 90% of our Cyber-espionage incidents this year. Whether it's delivered via email, a web drive-by, or direct/remote installation, protecting the endpoint is critical. To secure the endpoint you should:

- Make browser and plug-in updates "your jam"
- Use and update anti-virus (AV)
- Use Data Execution Prevention (DEP)
- Use Endpoint Threat Detection and Response (ETDR)

Email protection
As phishing remains a dominant Cyber-espionage attack vector, protecting this means of communication is critical. To protect against email-based attacks, implement defenses that incorporate:

- Spam protection
- Block lists
- Header analysis
- Static/Dynamic email attachment and URL analysis
- Reporting procedures for suspected phishing attempts

Network protection
Protecting the network is critical to securing your internal systems, even if a foothold has been established. To defend the network, work to:

- Use two-factor authentication
- Segment the network
- Block C2 communications and remediate compromises

Monitoring/Logging
Internal monitoring of networks, devices and applications is necessary to learn the lessons from all these hacks. At a minimum, work to implement:

- Account monitoring
- Audit log monitoring
- Network/IDS monitoring

Cyber-espionage research published in 2015/Q1 2016
The DBIR focuses on overall trends and statistics related to Cyber-espionage incidents and breaches. Several organizations that have contributed to this publication over the years have done some writing of their own and published in-depth research and analysis on the Actors that are on the hunt for intellectual property.

- APT28 (FireEye)
- APT30 (FireEye)
- Duqu Threat Actor (Kaspersky)
- Morpho Group (McAfee)
- Various Actors/Campaigns (Kaspersky)
- Project CameraShy (Threat Connect)
- Various Actors/Campaigns (CrowdStrike)

Denial-of-Service Attacks

At a glance

Description	Any attack intended to compromise the availability of networks and systems. Includes both network and application attacks designed to overwhelm systems, resulting in performance degradation or interruption of service.
Top industries	Gaming, Information Technology & IT Services, Financial
Frequency	9,630 total incidents, 1 with confirmed data disclosure.
Key findings	Attacks are either large in magnitude or they are long in duration but they are typically not both, and many are neither.

To prevent losing fidelity in the data, we used a hybrid of naming conventions utilized by our contributors and the NAICS categories.

Time for a break from NAICS

This isn't a forever thing, but we are using a hybrid of the naming conventions utilized by our data sharing contributors and the high-level NAICS categories. We are doing this, not out of laziness, but because when we looked to do the mapping from our data sharing contributors naming conventions to NAICS, we were worried about losing fidelity in the data. Many of the affected companies are gambling sites, as an example. We would lose a lot of the industry demographic information if we classified them as an internet entertainment or game site, or likewise as a casino. No framework is perfect[27] and we felt that blending the two classifications for this particular section made sense.

In a Galaxy Far, Far Away ...

Back when we first added this section in 2014's DBIR, we noted the evolution of this pattern dating back prior to 2012 and the new waves of DoS attacks peeking out from the horizon.

Rarer are the days where the DDoS bot recruitment pool is limited to our parents' 15 year-old home desktop—the one that haunts all your family visits like Banquo's ghost, breathing its foul contagion on all who dare attempt to

[27] No, not even VERIS.

patch it. As the attackers' botnets popped their steroids for a beefier blow, the attackers began to realize their creativity and scope should not be so limited. This epiphany has resulted in script injections into browser sessions, distributed reflective DoS attacks, as well as the infancy of temporal lensing[28] (which sends packets via different paths with a focus on time so that they arrive simultaneously in order to overwhelm the target system). Not only are these attacks increasing in scope, but also in number. We received the gory details of DDoS attacks (e.g. bytes and packets per second, duration) from Akamai Networks, Arbor Networks, and Verizon DoS Defense. We will get into magnitude and duration in a little bit but first, let's examine density.

As provided in the last two reports, Figure 41 shows two density plots of bandwidth and packets in DoS attacks, respectively. In this year's dataset, we see that the means of bytes per second versus packets per second were 5.51Gbps and 1.89Mpps respectively.

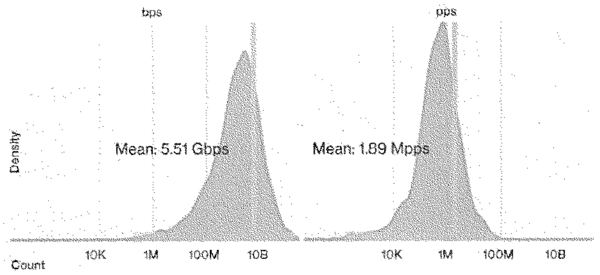


Figure 41.
Denial-of-Service attack bandwidth and packet count levels, (n=10,808)

Try this on for size.
Our analysis showed that attacks are either large in magnitude (i.e. packets per second), or they are long in duration, but they are typically not both, and frequently neither as depicted in Figure 42. Larger-sized attacks pull away from the origin and yet remain parallel to the y-axis. Thus, the data revealed predictability of whether the attack would be either a thundering exclamation or a conversation that seems to never end, by just looking at the very beginning of the attack.

DoS attacks are either large in magnitude or they are long in duration, but typically not both.

[28] EECS.Berkeley.edu/Pubs/TechRpts/2014/EECS-2014-129.pdf

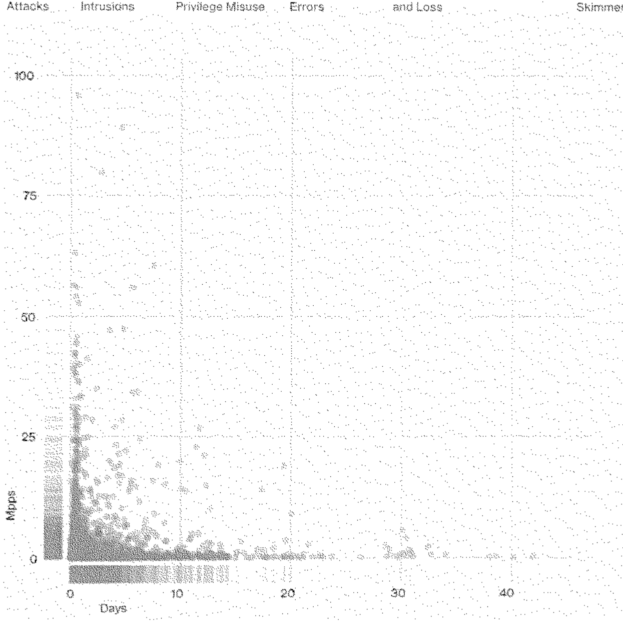


Figure 42.

Packets per second and duration of DDoS attacks, (n=5,800)

With density, magnitude and duration out of the way, let's finally look at enumeration of packets per second (pps) by industry and a caveat that comes with it. We compared the max and median number of pps per industry and as expected, they varied quite a bit. For example, although one of our large datasets showed that Media had the highest number (222 million pps) throughout this year's data, it doesn't necessarily mean (no pun intended) that it is the industry you'd expect to run out the door with their pants on fire every time. To see this, just look at Figure 43 that reflects the median number of pps for Media (approximately 600,000). Another such case includes High Tech Consulting, where the max pps was around 214 million, yet the median was around 540,000. In general, we don't always want to look at the max as it may only point to a single event, not all events throughout the entire year, hence we need to consider the median.

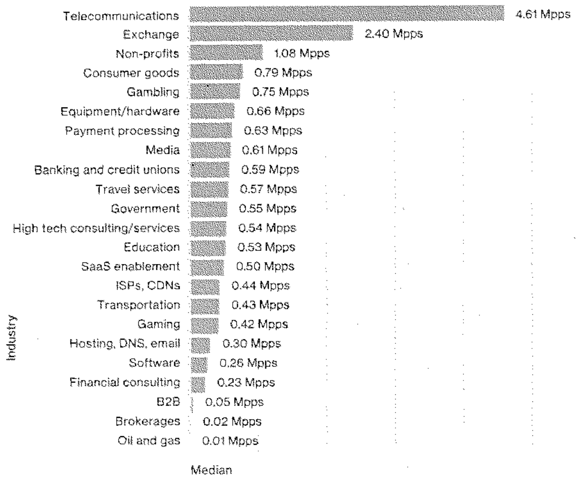


Figure 43.

Median DDoS packet count, in millions of packets per second, by industry. (n=5,800)

To sum up, "They start wanting me to care more, and I just don't" works for good ol' Han, but unfortunately we cannot live by his motivational motto when it comes to DoS. Not only is it one of the most popular attack types out there, but the rise to dominance of DoS is forcing attackers to join the dark side in droves; it may be time for Han, and the rest of us, to have an abrupt paradigm shift.

Recommended controls

Fear not the lone wolf.

Isolate key assets to help prevent your devices from being used to launch attacks. For instance, enforce the principle of least privilege, close any ports that are not necessary and—bottom line—if you don't need it, turn it off. Also, prepare your den for potential attacks. Patch your servers/services, use your IDS/IPS to identify and block bad traffic, use your firewalls to help filter, and have a response plan ready.

Walking around with your head in the clouds

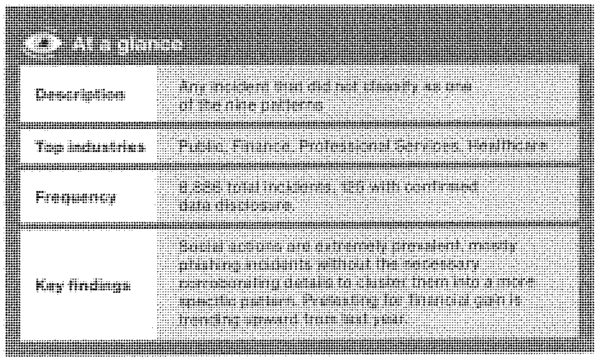
It makes sense as the peak size, complexity and frequency of DoS attacks continue to evolve and rise, that cloud service providers must have solutions in place in order to protect the availability of their services and infrastructure.

Understand the capabilities of your defenses.

Have a solid understanding of your DDoS mitigation service-level agreements. Make sure that your own DoS response procedures are built around existing denial of service protections and your operations teams are trained on how to best engage and leverage these services if and when they become more than just a 'piece of mind' control.

As DoS attacks continue to evolve, cloud service providers must have solutions in place to protect their infrastructure.

Everything Else



At a glance

Description	Any incident that did not classify as one of the nine patterns
Top industries	Public, Finance, Professional Services, Healthcare
Frequency	8,226 total incidents, 126 with confirmed data disclosure.
Key findings	Social actions are extremely prevalent, mostly phishing incidents without the necessary corroborating details to cluster them into a more specific pattern. Pretexting for financial gain is trending upward from last year.

By far, the biggest source of incidents in this pattern is phishing attacks where not much else is known.

If the other patterns are the hip bars in the Gulch, Everything Else is more like the local hangout off of Belcourt. Just like in 2014, the Everything Else pattern isn't a subset of unique, never-seen-before events, but some select groups that like hanging out away from the main drag.

Sorry, VIPs only

There are two reasons why an incident would not be on the guest list, thus causing the bouncers, in the form of clustering analysis, to keep them behind the velvet rope and outside of the nine clubs. The first is that there simply was not enough information provided about the incident to associate it with a pattern. By far the biggest source of incidents in the Everything Else pattern is phishing attacks where not much else is known. A large number of them come from a pair of Computer Security Incident Response Team (CSIRTS), but ten additional different data contributors reported phishing attacks that fell into this pattern. We won't dwell on phishing in general since there's already a section for that, but it is interesting to note why these end up here and are not bounced via the complexity filter we discuss in Appendix E: Methodology and VERIS Resources. Merely knowing phishing was involved gives us a fair amount of details—we know a human asset is targeted, we know a threat action, we know the vector is email, and we know or infer an integrity loss due to the altering of human behavior. So there is a lot we know, but it's what we don't know that lands it here.

The second reason that incidents hang their hat here, is that they are actually different from the norm. One scenario we are seeing more of is financial pretexting, sometimes called 'CEO Fraud'. This involves old-fashioned social engineering of employees with the authorization to move money. Emails purportedly from the CEO or other head honcho provide instruction to transfer funds to an entity, with a seemingly valid reason provided. These may also be blended with other forms of communication, but you get the gist of it. 'Twas not the CEO behind that email and somebody who believed they were following legitimate instructions is not having a very good day. As our dataset continues to get a better view into this corner of cybercrime it may be time for this to move out of the indie scene and become more mainstream.

We encourage organizations to collect as many details as possible for data breaches and many of these breaches will get "on the list."

You know we like Everything Else, so let's talk about everything else in Everything Else.

Outside of the aforementioned social actions, and focusing on confirmed breaches, we have a significant number of hacking events, but without knowledge of the specific varieties used by the adversary. We can see in Figure 44 that it represents a large number of breaches.

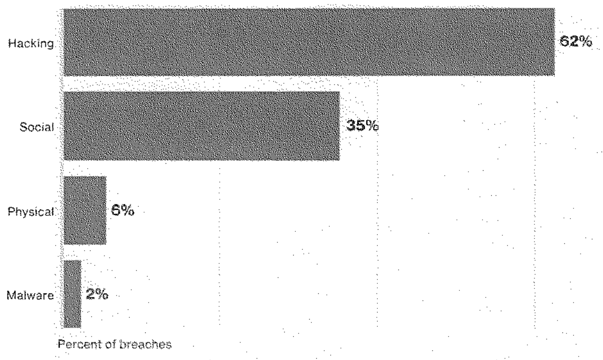


Figure 44.

Threat actions within Everything Else breaches, (n=125)

As we stated earlier, it is the missing pieces of the puzzle that are the cause of these "hacks" ending up on the back pages of patterns sections. As always, we encourage organizations to collect as many details as possible for data breaches and hopefully incident reporting detail will improve and many of these breaches will get "on the list".

Wrap up

First off, thank you for making it this far! We hope you have enjoyed the long, strange trip through this year's data and found some insights and/or figures that you can leverage as you fight your battles against adversaries and internal contrarians in need of some evangelization. To recap, we talked through some points of focus that would be a core component in several of the incident classification patterns that followed.

The focus on credentials and phishing in particular, show that actions taken by the adversary are not exclusive to a single pattern—anything but.

Actions taken by the adversary are not exclusive to a single pattern.

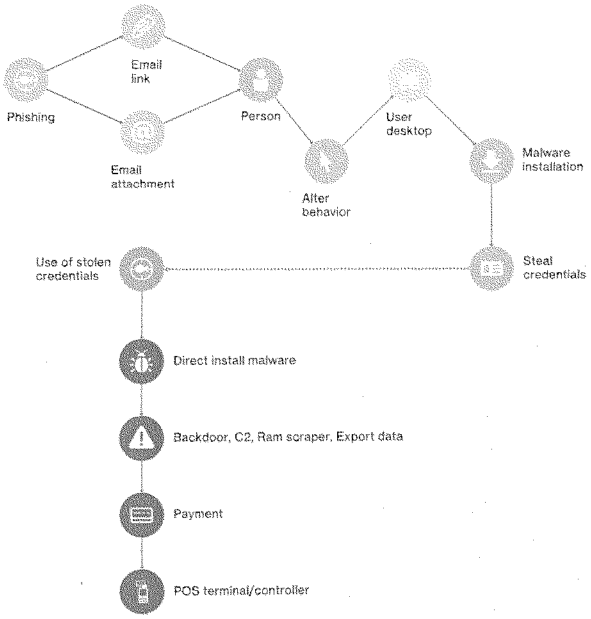


Figure 45.
Birth and rebirth of a data breach.

And while we tend to stray from focusing on particular trees in the data breach forest, the scenario depicted in Figure 45 is interesting to walk though as it features many of the most common threat actions, vectors and assets from our corpus. What you are looking at is a progression of a breach involving the targeting of a POS vendor and subsequent collection of sensitive data used against a second group of victims. The birth and rebirth of a breach is established above.

The attack begins with a targeted phishing campaign against the vendor. The person on the other end interacts with the email (clicks) and malware installation on the user device occurs. While the end of this story is stolen payment cards, those who aren't flipping their collective wigs trying to comply with PCI should still pay close attention. Up to this point we could be talking about the beginnings of a state-affiliated Cyber-espionage breach, or even a totally opportunistic Crimeware attack. Once the initial access has been established the attacker's motivation influences which street they choose to drive down.

In the above case the foothold is used to harvest credentials to be used against B2B customers. We can even infer some likely suspects as far as malware varieties here, notably some level of control and access (backdoor/C2) and a means to establish the first confirmed data disclosure (keylogger).

So for the adversary, great success. User duped, device compromised, data captured—time to yell "Yabba dabba doo" and slide down the dinosaur tail to signify the end of another productive work day? Not quite.

The breach is reborn as an attack on the customer using the stolen credentials against a static authentication factor. With the second network compromised, malware is installed directly (after system access). Malware functionalities of scraping RAM and exporting data, as well as establishment of control and persistence, make their appearance. They combine to capture, package and exfiltrate payment card data, thus completing the breach.

Having an understanding of how patterns can complement each other and share portions of event chains can help direct your efforts as to what to prioritize your limited resources against. That is, knowing the processes used by the Actors, the tools (Actions) to accomplish their goals and how many of these patterns begin with the same or similar bag of tricks.

Having an understanding of how patterns complement each other can help direct your efforts as to what to prioritize your limited resources against.

Varieties of impact

Paying the well-dressed pipers

Last year we analyzed impact data associated with cyber insurance claims leading to two main conclusions. First, record loss is not a simple linear relationship; the first few records breached cost significantly more per record than the 100,000th. Second, there's a lot we don't understand about the cost of breaches. In fact, half of why one breach costs one amount and another costs another amount is not known. (The other half is due to the number of records breached.) A year later and we are still looking for the meaning of life and a better predictor of bottom line impact to organizations that suffer a security incident.

We decided against attempting to build a better mousetrap this year. With limited tangible, hard data available on the cost of breaches, that exercise was not going to be a dragon we attempted to slay. Instead we dug into actual cyber insurance payout data again contributed by NetDiligence and looked into other characteristics that could be interesting and actionable. We poked around with the data varieties involved in the dataset and found that PCI breaches had a much higher median of documented record loss than personal health information (PHI) or PII.

PCI breaches had a much higher median of documented record loss than PHI or PII.

Data Type	Percent of Incidents	Median
PCI	27%	53,100
PHI	11%	1,000
PII	48%	761
Non-card Financial	5%	55

Table 3.
Median records breached by data type

Without more knowledge about the representation of insurance clients we choose not to make broad statements about frequency of data variety. However, we did find some interesting results when we looked into what we call data loss varieties. Take a peek below:

Forensics (like freedom) isn't free.
Not a box plot grokker?[29] Don't let Figure 46 intimidate you. The short explanation is that it shows that the majority of the insurance payouts go toward costs within the phase of breach recovery associated with determining just which creek you are up and your current paddle supply. Legal guidance during the crisis management phase and forensics investigations are where the majority of the cash is going. These cost categories are followed by breach notification and credit monitoring, because sending flowers to your customer base just isn't going to cut it.

Legal guidance during the crisis management phase and forensics investigations is where the majority of the cash is going.

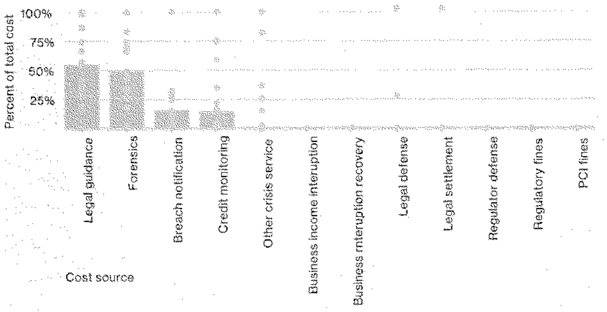


Figure 46.
Breakout of cyber insurance payouts by type of cost, (n=41)

If you look at all the different cost categories, they are ordered from first to last. The first phase includes up-front costs which are incurred when you think you have suffered a loss, and are receiving third-party guidance and investigative services to determine what happened and establishing how bad it was. This is followed by reluctant acceptance and trying to save as much face as possible with the customers affected. Then come the long-term costs involving legal representation, settlements and fines, which would occur after the story of your breach is coming to the epilogue. It should be noted that while our glimpse into the cyber insurance world is enlightening, it also requires some additional context. It's important to understand what might not be covered by insurance. Many cyber insurance policies do not include coverage for remediation costs or judgments to pay punitive damages – each being potentially expensive on their own. In many jurisdictions, punitive damages are not even legally insurable. And these costs are not nearly as common, in comparison with the more upfront costs.

Attorneys and investigators don't charge by the record breached, but typically on an hourly basis whether for a fixed number established by a pre-existing retainer, or on demand. Develop relationships before their services are required and align your ducks, so in case these services are required, you have processes in place to quickly provide the level of access and information needed to kick things off properly. You want to try to ensure hours aren't spent looking for a network diagram or SLAs while suits are in a conference room looking at their mobile phones.

[29] The line is the median – half the costs were below the line and half were above. One fourth of all breaches were between the line and the top of the box and another fourth in the bottom part of the box. The rest of the breaches were outside of the box. It's an easy way to see a range of where most breaches fall.

Appendix A: Post-compromise fraud

Whatcha doin' in these waters?

If cybercriminals were anglers, they would not be practicing "catch and release." No, when they hook a live one, that bad boy is going into a cooler. With the help of Intel Security, this section will discuss what the threat Actors do with all the data they compromise once they land it, in particular:

- Analysis of the monetization of stolen data
- A look into the market(s) for compromised records

Methods of monetization

There are seemingly endless types of stolen data available for sale from an equally endless variety of sources. However, this document is not "War and Peace," so we will attempt to shorten and simplify our analysis by limiting the scope to the data types that are easily understood and where a significant volume of stolen data is available through reasonably well-understood marketplaces. The following broad categories are presented but we recognize that this list is anything but exhaustive:

- Payment card information
- Financial account information
- Personal information (PII)

Other data types such as intellectual property or access to enterprise systems can also be stolen and monetized, and often are. However, while we commonly see services related to the theft of a variety of data, transactional details are not commonly seen on the open market and it is therefore difficult to quantify its market value. Some data may be more valuable to keep rather than re-sell on the markets. It is probable that those who steal IP are actually using it themselves to create a better widget without the laborious and costly R & D otherwise required. So, we will focus on the areas where we do have sufficient visibility—the categories mentioned above.

There are seemingly endless types of stolen data available for sale from an equally endless variety of sources.

Payment card monetization

There are multiple methods by which stolen cards are obtained and cashed out. Furthermore, there are several factors that influence how compromised payment card data will be used for financial gain once it is purloined. A few of those are listed here:

- The actions taken by the criminal to acquire the data and to what type of asset. How data is stolen will often influence what information in addition to the primary account number (PAN) is captured. We will use the pertinent incident classification patterns where possible to better explain the attack methods.

- How many payment records are captured in a breach or a spree of breaches.
- The threat Actor behind the breach. (Are they a one-man wolf pack, or an organized criminal group?)

The initial decision made by the threat Actor is whether to sell the data they have acquired, or to engage in the post-compromise fraud themselves. In large breaches with record losses in the millions, it may be advantageous to act as a wholesaler and sell in bulk to intermediaries who will ultimately initiate the fraudulent transactions. The "This little piggy went to market" section below digs deeper into the black market for stolen data.

Methods available to monetize stolen payment card information (like the Wonder Twins) can take many forms. We can, however, begin with a simplistic breakout of possible fraud mechanisms into two distinct and commonly used categorizations, card-present and card not-present fraud.

Bueller, Bueller ... Bueller?
We will start with card not-present (CNP) fraud. Obviously, this fraud is associated with purchases made either online or over the phone. At first thought, it seems like this would be a desirable fraud action to take. It can be done remotely with no need to physically travel to a store and show your face. But there is a catch. Namely, the lack of the 3 or 4 digit number on the physical cards, known as the Card Verification Value (CVV2). The CVV2 code is a required field on the vast majority of ecommerce sites. In a blatant demonstration of pure pigheaded obstinacy, the issuing banks do not place the CVV2 code on the magnetic stripe of the card, thereby forcing criminals to actually work for their money. Therefore, the necessary piece of information to perpetrate CNP transactions is typically gathered in attacks against legitimate CNP transactions. The two main patterns associated with capturing CNP data are:

Profiting from stolen card not-present (CNP) transactional data is similar to old school fencing of stolen goods.

Crimeware installed on consumer devices with spyware or form grabber functionalities to capture (client-side) the PAN+Expiration+ CVV2 combo which are needed in addition to billing information to "prove" possession of the physical card.

Web App Attacks leading to compromise of the payment application and subsequent code modification to collect and exfiltrate the same information.

Profiting from stolen CNP transactional data is similar to old school fencing of stolen goods. Think of goodfellas handing out cartons of cigarettes off the back of a truck at a "discounted" price. CNP orders for goods or services are placed online and then delivered through a network of intermediaries to obfuscate the true recipient of the shipment. At the end of the shipping chain the goods are delivered to warehouses where the goods are then sold through local websites.

Present and accounted for!
POS Intrusions and Payment Card Skimmers: Two great tastes that go great together—91% of payment card breaches fall into these two patterns. Both patterns feature specific assets that are targeted due to their role in processing payment card information and both involve card-present transactional data. And the data captured in a card-present transaction is highly likely to be reused in card-present fraud. Some of you at this point are noticing a lack of Chip and PIN mentions, and we will get to that in a bit, we promise.

Both of these attacks, if successful—and let's be real, they frequently are—result in the compromise of magnetic stripe information and are detailed more thoroughly in their respective sections. Let's focus on the stripes, shall we? That bold black stripe on the back of your card holds some key pieces of information: the PAN, expiration date and discretionary data (most notably the CVV) that was designed to help establish "proof" that the physical card is legitimate.

The CVV protects against cloning the payment cards of the people that take pictures of their debit cards and post them on Twitter, so I guess that's a win.[30] But since the common attacks are grabbing all the static magnetic stripe data, the utility of CVV (not CVV2 which is used in CNP transactions) is lessened. This is where the Europay, MasterCard and Visa (EMV) standard—via Chip and PIN—comes into play, using a one-time security code to establish the authenticity of the physical card instead of the static CVV.

ATM skimming operations also target the users' PINs. Combining this key piece of information with the mag stripe allows for quick cash-outs in areas where Chip and PIN protection has not been fully implemented such as in the USA, South America and Asia.

To recap: CNP fraud most often leverages peeking in on legitimate CNP transactions. Card-present fraud stems from stealing info from card-present transactions. The CVV and CVV2 numbers help to prevent the cross-pollination of fraud, but neither are a powerful force field against stealing payment info and getting paid.

Banking data monetization
As consumers began to access financial information online, cybercriminals targeted the theft of both login credentials and ultimately the money in the accounts. Financial account login credentials can be used to exfiltrate money through transfers via online banking applications. Phishing and malware can team up to capture account and routing numbers to commit ACH Fraud. The Crimeware pattern makes another appearance in the form of banking Trojans (e.g., Zeus, Dyre and Dridex) that have evolved to efficiently target static and thus reusable banking information. Privilege Misuse by banking employees is another pattern that leads to banking data loss. Simply put, employees have access to this data, and often use it for their own gain solely or in collusion with external criminal groups.

In cases of Privilege Misuse, employees have access to data and use it for their own gain or in collusion with criminals.

Personal information monetization
Personal data, aka PII, is the other data type that is often associated with financial fraud. The term "identity theft" is no longer an alien concept to most people and there are numerous ways for adversaries to use PII. Opening up new lines of credit and filing fake tax returns are common fraud methods. PII can also be used to craft better pretexts to be used in a variety of social engineering attacks. Many disclosures of PII fall into the Miscellaneous Error pattern, as well as Insider and Privilege Misuse and Physical Theft and Loss.

This little piggy went to market.
The most obvious type of stolen data that is monetized in high volumes is that for payment cards. In a fall 2015 McAfee Labs publication, The Hidden Data Economy[31], the following prices were identified as average selling prices for stolen cards:

Payment Card Number with CVV2	United States	United Kingdom	Canada	Australia	European Union
PCI	$5-$8	$20-$25	$20-$25	$21-$25	$25-$30
PHI	$15	$25	$25	$25	$30
PII	$15	$30	$30	$30	$35
Non-card Financial	$30	$35	$40	$40	$45

Table 4.
Estimated per card prices, in US$, for stolen payment card data (Visa, Mastercard, Amex, Discover).
Source: McAfee Labs

[30] @NeedADebitCard
[31] McAfee.com/us/resources/reports/rp-hidden-data-economy.pdf

The challenge with such pricing is that there are multiple variants that are only touched on in the table above. Variants include such things as geography, whether a PIN number is included, the available balance, validity rates, what additional data is provided and, of course, the seller.

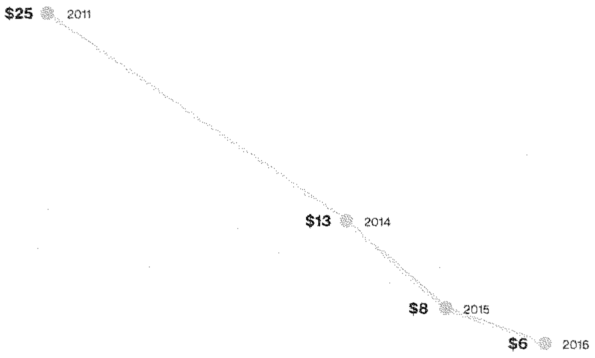


Figure 47.

Price per payment card record over time (USD). Source: Intel Security

It is difficult to establish marketplace trend information over time because there are so many purchase options available. Above is a best effort graph (Figure 47) showing the pricing changes for a "bare-bones" model of a stolen US-based payment card.

Like any market, the market for stolen payment cards is subject to supply and demand. Large-haul payment card breaches were non-existent in the 2011 DBIR and we were concerned over the small record count (approximately 4 million records, down from 144 million the prior year) in our 2011 DBIR data. We confirmed the lack of known high record count breaches for that year. And the market data above points to a low supply, raising the cost, which supports that finding. Following the retail mega-breaches in 2014, we saw that there was an overabundance of cardholder data that influenced a drop of about 50% from prices just three years earlier. As we fast forward into 2016, we continue to see a steady yearly decline. With supply through the roof, sellers of stolen cards began differentiating based on other criteria to prop up prices. We discovered that the criminals were selling by geography (e.g. city) and by validity rate, immediately following large breaches. Clearly, knowing the location where cards can be used without suspicion and the likelihood that the cards are valid, provide significant value to buyers. Today buyers can specify certain countries or card types for extra cost (we have seen an $8 upcharge for this). Costs are significantly higher with additional cardholder information (PII) such as billing address and social security number. Overall, however, the trend over the past four years has been a general decline in the prices charged.

Sellers of stolen cards began differentiating, basing their prices on geography or the validity rate of the cards.

There is not much data to establish price trend information for stolen financial account credentials. However, we have found some current pricing information.

For $250, a buyer can acquire access to an account (from a number of major banks) with a balance of $5,000. There is a volume discount here, where $400 provides access to an account with $10,000. This reflects an account balance of between x20–x25 the purchase price.

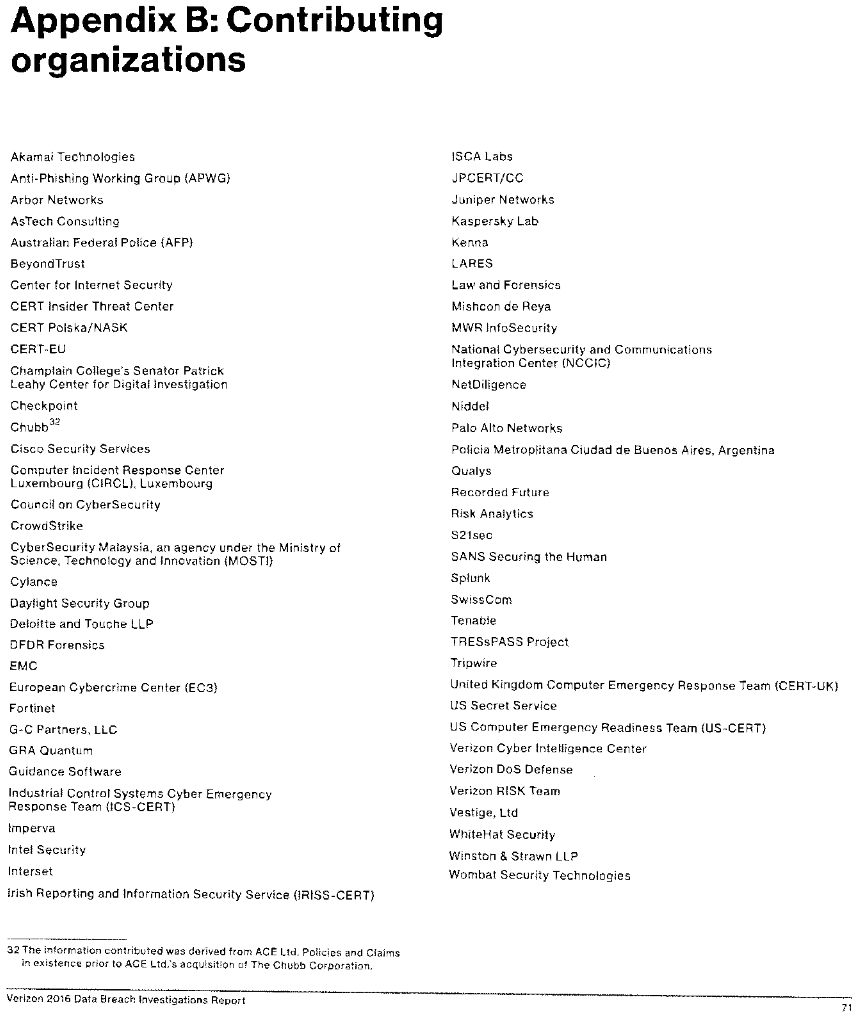
PayPal accounts are also a common target for those who wish to steal financial account login credentials. We have seen markets with even greater discounting, where 60 bucks will get you $4,000 in PayPal credit (x67 the purchase price).

The value of something is what someone is willing to pay for it, and if there is a demand for something there will always be someone willing to supply it in order to obtain a profit. The rules of the market can be perfectly applied to the cybercrime marketplaces. Through the operations coordinated through Europol, we have seen how all kinds of illegal goods are traded through black market digital sites, some on the dark net, taking advantage of the anonymization possibilities given by the technology, and many of them on the open net. There is a clear demand for stolen data and, therefore, there will always be criminals ready to supply and satisfy this demand, especially if we take into account the disproportion between the risk-cost-profit, as data can be easily stolen and transmitted.

The whole internet community, from citizens to companies or governments, is a target for cybercriminals looking for protected data. Private users are victims of phishing/spam campaigns aiming at stealing online banking credentials or sensitive documents. Small, medium and large companies, for which data is one of the most important assets (information on its customers, their market strategy or industrial information) are constantly targeted through sophisticated technical attacks or basic social engineering techniques. As stated in Europol's iOCTA (Internet Organised Crime Threat Assessment) 2015, the media commonly referred to 2014 as the "Year of the data breach." With record numbers of network attacks recorded, this is a constant trend and the future scenario doesn't look any better.

The law enforcement community is constantly fighting against these criminal markets, its administrators and the criminals trading the stolen data. However, only through a coordinated effort involving all the parties involved; law enforcement, private sector, financial institutions, internet security industry, we will be in position to properly tackle this threat.

Fernando Ruiz–Head of Operations–European Cybercrime Centre (EC3)–Europol



Appendix B: Contributing organizations

Akamai Technologies
Anti-Phishing Working Group (APWG)
Arbor Networks
AsTech Consulting
Australian Federal Police (AFP)
BeyondTrust
Center for Internet Security
CERT Insider Threat Center
CERT Polska/NASK
CERT-EU
Champlain College's Senator Patrick Leahy Center for Digital Investigation
Checkpoint
Chubb[32]
Cisco Security Services
Computer Incident Response Center Luxembourg (CIRCL), Luxembourg
Council on CyberSecurity
CrowdStrike
CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation (MOSTI)
Cylance
Daylight Security Group
Deloitte and Touche LLP
DFDR Forensics
EMC
European Cybercrime Center (EC3)
Fortinet
G-C Partners, LLC
GRA Quantum
Guidance Software
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
Imperva
Intel Security
Interset
Irish Reporting and Information Security Service (IRISS-CERT)
ISCA Labs
JPCERT/CC
Juniper Networks
Kaspersky Lab
Kenna
LARES
Law and Forensics
Mishcon de Reya
MWR InfoSecurity
National Cybersecurity and Communications Integration Center (NCCIC)
NetDiligence
Niddel
Palo Alto Networks
Policia Metroplitana Ciudad de Buenos Aires, Argentina
Qualys
Recorded Future
Risk Analytics
S21sec
SANS Securing the Human
Splunk
SwissCom
Tenable
TRESsPASS Project
Tripwire
United Kingdom Computer Emergency Response Team (CERT-UK)
US Secret Service
US Computer Emergency Readiness Team (US-CERT)
Verizon Cyber Intelligence Center
Verizon DoS Defense
Verizon RISK Team
Vestige, Ltd
WhiteHat Security
Winston & Strawn LLP
Wombat Security Technologies

[32] The information contributed was derived from ACE Ltd. Policies and Claims in existence prior to ACE Ltd.'s acquisition of The Chubb Corporation.

Appendix C: The Taupe Book

Prepared based on security incident data collected from all of our contributors, this document pays homage to the Federal Reserve System Beige Book.[33] All statements are written in the parlance of this financial document and are made against a filtered set of data that only includes confirmed malicious data breaches. The Physical Theft and Loss as well as Miscellaneous Errors patterns are not included. This is based on an incident date of 2015, not the year of DBIR publication, although we would expect little-to-moderate fluctuation due to this method.

Organized criminal activity increased due to high levels of botnet activities and stable levels of POS intrusions.

Threat Actor activity

External Actors reported a slight growth in percentage of breaches from last year but not outside of historic norms. Internal Actors realized a similar decline in percentage and count from 2014. Collusion between internal and external Actors is still sluggish since its above average 2012 mark. Diversification of data and less breaches involving solicitation of banking workers has contributed to its decline. Partner Actors have remained flat.

Organized criminal activity reports an overall increase benefiting from high levels of reported botnet activities and stable levels of POS intrusions in 2015. Shifts in data contributions were cited as a cause of a slight decline in state-affiliated Actor prevalence last year.

Activist group activity review showed that breach levels were down and noted a continued moderate shift in focus from SQLi to denial-of-service campaigns.

Threat action trends

Hacking and Malware activity was characterized as growing rapidly and was similar to 2011 numbers. A botnet takedown contributed to this growth as well as an upward trend in the social threat action category. Phishing had a stronger association to known Crimeware breaches in 2015.

Physical actions cited the significant increase of non-law-enforcement data contributors as the principle reason for their decline from 2013 levels. Skimming operations have realized flat to slightly declining activity from 2014.

Conditions for use of stolen credentials and use of backdoor or C2 have continued to show growth in 2015. A partnership of the two varieties in a banking Trojan campaign was cited as a reason for increased activity. Brute force activity continued to be subdued as stolen credentials continued to establish growth in the POS Intrusion market.

[33] FederalReserve.gov/monetarypolicy/beigebook

The continued use of Web App Attacks has allowed SQLi and RFI to report stable activity in 2015. Contacts indicated that spikes in Crimeware breaches have resulted in significant gains in C2 and keylogging data malware functionalities. Data exports via malware also have a positive outlook.

RAM scrapers continue to show significant usage overall, but are showing signs of decreasing activity. The victim population in associated scaled remote attacks on guessable POS credentials is showing signs of overall decline.

Penetration into several incident classification patterns in 2015 is credited for the growth of phishing in the breach dataset. Social threat actions are showing stable growth. Pretexting activity has increased and was seen at a higher percentage than solicitation/bribery—this is a significant change from 2014 and was last seen in 2011. A positive growth in the use of pretexting in financially motivated breaches was reported in 2015 contributing to the rise in activity. This gain was offset by a sluggish performance by the Misuse variety of use of unapproved hardware. Reports suggest that the majority of these breaches involve use of USB drives to steal data and are related to espionage motives. Financially motivated uses of hand-held skimmers have realized a slowdown from 2014, which was stable when compared to 2013.

The majority of use of unapproved hardware in breaches involve use of USB drives to steal data and are motivated by espionage.

Financial, Information and Online Retail industries showed growth in their representation in the report. Accommodation showed moderate activity slightly up from 2014. Public, Retail (not online), Healthcare and Professional Services' presence softened in 2015. This is likely due to changes in the contributing organizations and several breach sprees that influenced numerous 4A (see Breach Trends section for definition) aspects in 2015.

No breaches have been attributed to vermin or any other environmental action, remaining flat.

Appendix D: Attack graphs

The making of an attack graph
So maybe you're wondering where the attack graph came from. It's one of the many things you can do with VERIS.

VERIS breaches have actions which lead to attributes. It's also possible to see where an attribute leads to an action. By taking those individual connections and counting them up, a graph of paths across the attack surface soon forms.

The graph isn't the attacks that happened, but the attacks that could happen. That is exactly what we need to assess our attack surface.

Graphs Attack! Film at 11

In the Breach Trends section, we compared information security defense to being told to defend a hill. Throughout the report you got an idea of what the attack looks like. But what if you had a map of the entire land, with the roads, paths and intersections laid out for you. That'd be a lot easier right? You could plan to defend not just the main paths, but the alternate paths the attackers might take as well. If you did that, you'd be defending your entire attack surface.

That's what attack graphs do. They are road maps that allow you to defend against your entire attack surface, not just paths you've seen. The attack graph at right[34] is the entire attack surface of the 2016 DBIR dataset in a single picture.[35] Try tracing all the paths from the start to the end.[36] And this is a very high-level look—imagine doing it at a more detailed level. Each action or attribute can be broken down into the individual varieties and vectors that exist in VERIS.

Now, when you hear about some specific attack, that's a single path from start to end and in many cases mitigations are planned specific to that single path. Wouldn't it be nice if you didn't have to apply mitigations to one path at a time and could instead mitigate a bunch of paths all at once? Yeah it would.

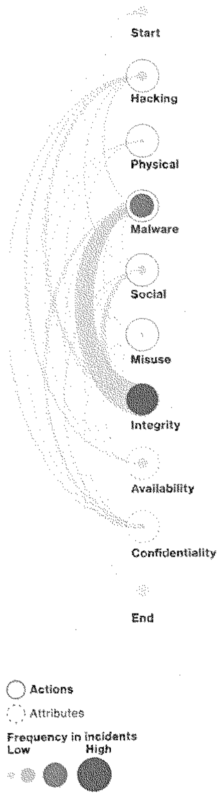


Figure 48.
2016 DBIR attack graph.

[34] Pointing your finger at the DBIR is fun and all, but why not try out the interactive version of the figure? Give it a shot at http://vz-risk.github.io/dbir/2016/52
[35] Do you know how long it took to come up with that figure? Don't even get us started! We tried like a million different things.
[36] The lawyers wanted us to say not to actually trace all the paths. There's so many you'll never finish and, in the interim, your company will fire you, your wife (or husband) will leave you, and your guild members will replace you.

Analyzing your entire attack surface using attack graphs can do that. I'll spare you the math,[37] but attack graphs can help you understand how to address the most likely attack path as well as multiple paths, all at once.

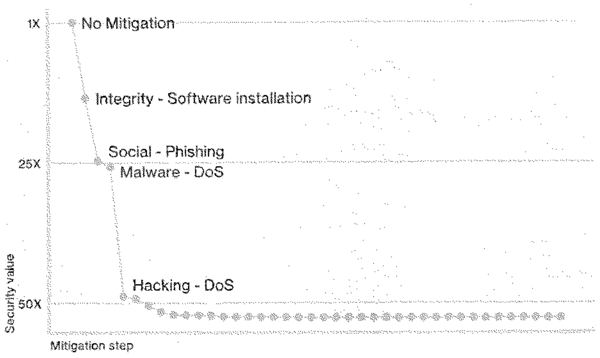


Figure 49.
Relative improvement per mitigation against the most likely paths

For the 2016 DBIR, Figure 49 shows the best areas of focus to address the most likely paths. Unsurprisingly, at this high level, the best thing to do first is prevent software installation. Software installation, which is the loss of integrity when malware is installed, is very prevalent in our incident corpus (but you know this by now). We have also practically harangued you folks on phishing so much that you are considering a pescetarian diet. Phishing, like denial of service has widespread coverage in this year's incident dataset.

I fought the law (of diminishing returns).

After you mitigate the first few things, the effectiveness simply falls off. The reality is there are a couple of highways the attackers like to use. Blocking those slows them down and they absolutely should be an area of focus, but once you get the attackers on the side roads, attempting to block all possible paths (or roads) is a fool's game.

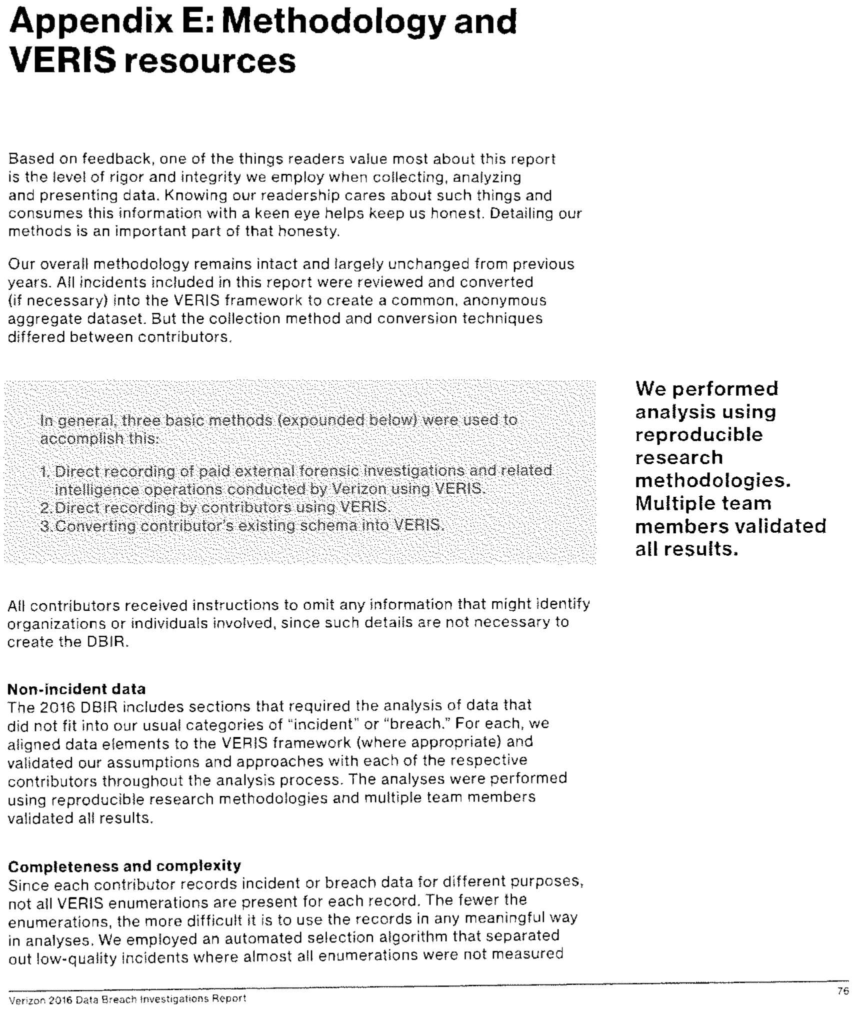
There are a couple of highways the attackers like to use. Blocking those slows them down. Attempting to block all possible paths is a fool's game.

These paths, be it of the highway or side road variety, may vary based on industry (e.g., Misuse is a likelier path for Healthcare than for Retail in our data). Defining the roads most traveled by your likely adversary[38] as well as the ones that lead to the greatest impact to you is key. Else you're trying to solve everyone's InfoSec problems and that's way too much InfoSecs for any one person.

In the end, it's the math that does the work. If you'd rather not math that hard, just try out our handy, dandy web app.[39] Just choose your threat (an industry or pattern), choose what you'd like to protect (confidentiality, integrity, availability, or everything), and the type of analysis you want to do (all potential attackers or just the most likely) and let it do the hard work for you.

In closing, if you are not addressing, to an appropriate level, your entire attack surface, you may be adding locks to a door while a window is left open.

[37] SecurityBlog.VerizonEnterprise.com/?p=6949
[38] You know, like looking at the industry data in the Incident Classification Patterns section of this report.
[39] DBIR-Attack-Graph.Infos.ec/



Appendix E: Methodology and VERIS resources

Based on feedback, one of the things readers value most about this report is the level of rigor and integrity we employ when collecting, analyzing and presenting data. Knowing our readership cares about such things and consumes this information with a keen eye helps keep us honest. Detailing our methods is an important part of that honesty.

Our overall methodology remains intact and largely unchanged from previous years. All incidents included in this report were reviewed and converted (if necessary) into the VERIS framework to create a common, anonymous aggregate dataset. But the collection method and conversion techniques differed between contributors.

In general, three basic methods (expounded below) were used to accomplish this:

1. Direct recording of paid external forensic investigations and related intelligence operations conducted by Verizon using VERIS.
2. Direct recording by contributors using VERIS.
3. Converting contributor's existing schema into VERIS.

We performed analysis using reproducible research methodologies. Multiple team members validated all results.

All contributors received instructions to omit any information that might identify organizations or individuals involved, since such details are not necessary to create the DBIR.

Non-incident data

The 2016 DBIR includes sections that required the analysis of data that did not fit into our usual categories of "incident" or "breach." For each, we aligned data elements to the VERIS framework (where appropriate) and validated our assumptions and approaches with each of the respective contributors throughout the analysis process. The analyses were performed using reproducible research methodologies and multiple team members validated all results.

Completeness and complexity

Since each contributor records incident or breach data for different purposes, not all VERIS enumerations are present for each record. The fewer the enumerations, the more difficult it is to use the records in any meaningful way in analyses. We employed an automated selection algorithm that separated out low-quality incidents where almost all enumerations were not measured from those that would support more informed analyses. The algorithm we used assigned a score to each record based on two main criteria: "completeness" (i.e., "was each core section—Actor, action, assets, attribute, victim, timeline, discovery method, and targeted—filled out") and "complexity" (i.e., "how well was each section populated"). The result is more meaningful, descriptive and actionable findings. Any deviation from this strategy is documented where it occurred in the report.

Another important point is that when looking at the findings, "unknown" is equivalent to "unmeasured." Which is to say that if a record (or collection of records) contains elements that have been marked as "unknown" (whether it is something as basic as the number of records involved in the incident, or as complex as what specific capabilities a piece of malware contained), it means that we cannot make statements about that particular element as it stands in the record. That said, it is important to realize when we have 10,000 cases where the motive of an Actor was "unknown," 500 cases where the motive is "financial gain" and 100 cases where the motive is "fun," readers should not infer that those 10,000 cases are implying anything about the cases where we have measurable values.

When looking at the findings, "unknown" is equivalent to "unmeasured" where we have too little information.

A word on sample bias

While we believe many of the findings presented in this report to be appropriate, generalization, bias and methodological flaws undoubtedly exist. Even though the combined records from all our contributors more closely reflect reality than any of them in isolation, it is still a sample. And although we believe many of the findings presented in this report to be appropriate for generalization (and our confidence in this grows as we gather more data and compare it to that of others), bias undoubtedly exists. Unfortunately, we cannot measure exactly how much bias exists (i.e., in order to give a precise margin of error). We have no way of knowing what proportion of all data breaches are represented because we have no way of knowing the total number of data breaches across all organizations in 2015. Many breaches go unreported (though our sample does contain many of those). Many more are as yet unknown by the victim (and thereby unknown to us).

VERIS resources

VERIS is free to use and we encourage people to integrate it into their existing incident response reporting, or at least kick the tires.

VerisCommunity.net provides general information on the framework with some examples and enumeration listings.

GitHub.com/vz-risk/veris features the full schema as well as access to our database on publicly disclosed breaches, the VERIS Community Database (VCDB).

Splunkbase.Splunk.com/app/2708/ is a community-supported application for Splunk that maps to the incident classification patterns.

Appendix F: Year in review

The year began with the Verizon Cyber Intelligence Center (VCIC) tracking incidents that would emerge as 2015's major risk trends. We were seeking actionable intelligence from the mega-data breach at Sony Pictures Entertainment (SPE) in November 2014. Online wire-transfer provider Xoom was probably the year's first victim of a Business Email Compromise (BEC) to the tune of $31 million. Palo Alto Networks reported Dridex banking Trojans "began 2015 with a bang." Chick-fil-A and OneStopParking were the victims of payment card breaches which hit the headlines. Sadly, headlines on sites like AOL and Huffington Post also led to the year's first major malvertisement campaign with an exploit kit (EK) attacking browsers with unpatched Adobe Flash Player. Later in **January**, Adobe released a new version of Flash Player to mitigate a zero-day vulnerability being exploited in three advertising networks.

On **February** 4, Blue Cross health insurance member-company Anthem announced they were the victims of a data breach along with almost 80 million people. And on February 27, ThreatConnect reported Chinese threat Actor "Deep Panda" was probably Anthem's attacker. Invincea and iSight partners each released intelligence on a Chinese cyber-espionage campaign that occurred in November 2014. Dyre, Vawtrak and Carbanak joined the list of active banking Trojans. Symantec and Microsoft announced the first major malware takedown of 2015 after the seizure of the infrastructure for the Ramnit botnet. With no arrests reported in the takedown, it came as no surprise Dr. Web reported signs of a Ramnit comeback about a month later.

In **March**, Premera, another Blue Cross member, announced a data breach affecting 11 million people. ThreatConnect's intelligence attributed the Premera breach to Deep Panda. The Mandarin Hotel Group reported a payment card data breach. POS vendor NEXTEP also reported a breach. March's takedown of the "Evolution" deep web marketplace included arrests and it stayed down. A day after the Canadian Security Intelligence Service (CSIS) reported Vawtrak was targeting Canadian banks, AVG reported a Vawtrak campaign collecting banking credentials globally.

Early **April** brought reports that threat Actors in China had launched "Great Cannon" DDoS attacks on GitHub, probably targeting censorship-evasion projects, and Great Cannon also attacked anti-censorship organization GreatFire. The Drudge Report was one of the sites serving up malvertisements leading to an EK and the click-fraud Trojan Bedep. Interpol, Microsoft and several security companies collaborated on two takedown operations seizing the infrastructure hosting the Simda and Beebone botnets. Pawn Storm and CozyDuke cyber-espionage campaigns aligned with Russian national security were the focus of several intelligence reports we collected in April. InterContinental Hotel Group, Sally Beauty and FireKeeper's Hotel and Casino joined the list of payment card data breaches in May. Healthcare sector data breaches proliferated with reports from Partners HealthCare, CareFirst Blue

JAN

Xoom

$31 million
business email compromise

FEB

Deep Panda

Likely cause of breach
with 80 million victims

MAR

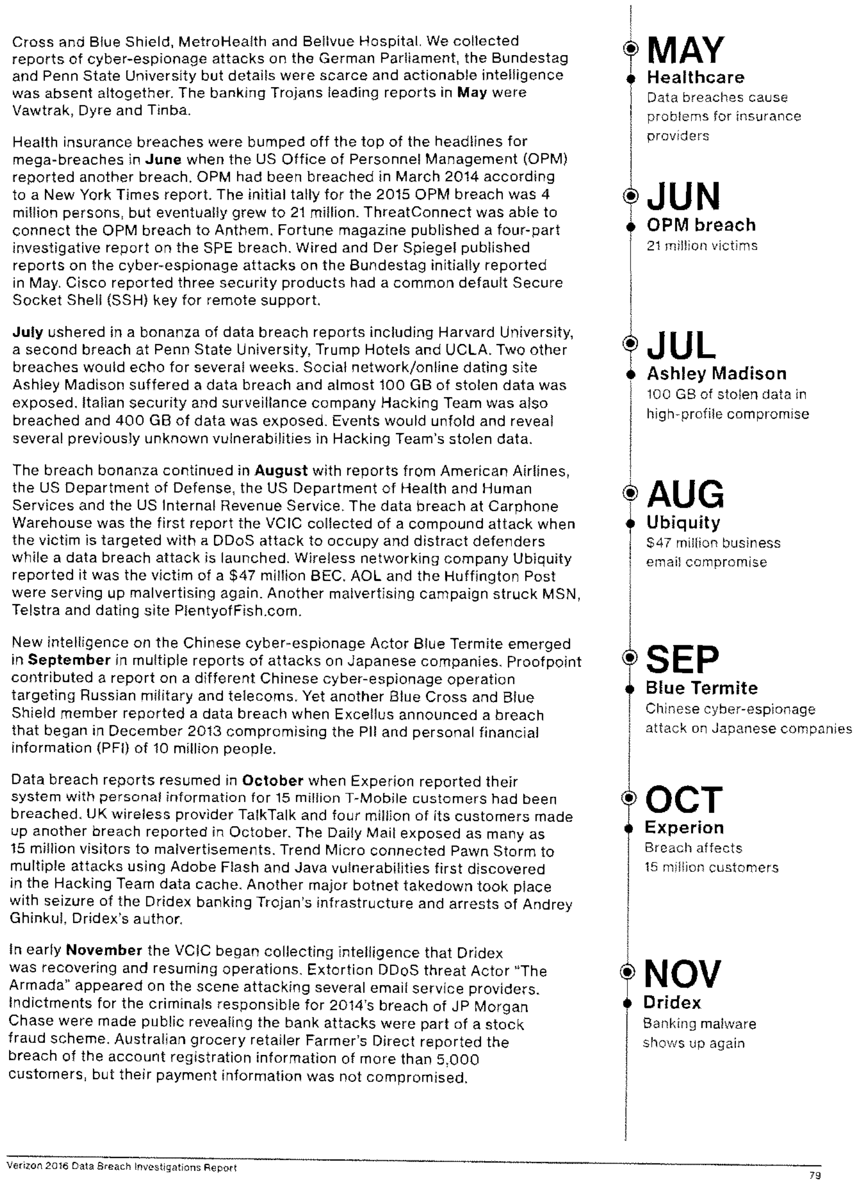
Premera

Data breach affecting
11 million people

APR

Great Cannon

DDoS attacks on
GitHub, GreatFire



Cross and Blue Shield, MetroHealth and Bellvue Hospital. We collected reports of cyber-espionage attacks on the German Parliament, the Bundestag and Penn State University but details were scarce and actionable intelligence was absent altogether. The banking Trojans leading reports in **May** were Vawtrak, Dyre and Tinba.

Health insurance breaches were bumped off the top of the headlines for mega-breaches in **June** when the US Office of Personnel Management (OPM) reported another breach. OPM had been breached in March 2014 according to a New York Times report. The initial tally for the 2015 OPM breach was 4 million persons, but eventually grew to 21 million. ThreatConnect was able to connect the OPM breach to Anthem. Fortune magazine published a four-part investigative report on the SPE breach. Wired and Der Spiegel published reports on the cyber-espionage attacks on the Bundestag initially reported in May. Cisco reported three security products had a common default Secure Socket Shell (SSH) key for remote support.

July ushered in a bonanza of data breach reports including Harvard University, a second breach at Penn State University, Trump Hotels and UCLA. Two other breaches would echo for several weeks. Social network/online dating site Ashley Madison suffered a data breach and almost 100 GB of stolen data was exposed. Italian security and surveillance company Hacking Team was also breached and 400 GB of data was exposed. Events would unfold and reveal several previously unknown vulnerabilities in Hacking Team's stolen data.

The breach bonanza continued in **August** with reports from American Airlines, the US Department of Defense, the US Department of Health and Human Services and the US Internal Revenue Service. The data breach at Carphone Warehouse was the first report the VCIC collected of a compound attack when the victim is targeted with a DDoS attack to occupy and distract defenders while a data breach attack is launched. Wireless networking company Ubiquity reported it was the victim of a $47 million BEC. AOL and the Huffington Post were serving up malvertising again. Another malvertising campaign struck MSN, Telstra and dating site PlentyofFish.com.

New intelligence on the Chinese cyber-espionage Actor Blue Termite emerged in **September** in multiple reports of attacks on Japanese companies. Proofpoint contributed a report on a different Chinese cyber-espionage operation targeting Russian military and telecoms. Yet another Blue Cross and Blue Shield member reported a data breach when Excellus announced a breach that began in December 2013 compromising the PII and personal financial information (PFI) of 10 million people.

Data breach reports resumed in **October** when Experion reported their system with personal information for 15 million T-Mobile customers had been breached. UK wireless provider TalkTalk and four million of its customers made up another breach reported in October. The Daily Mail exposed as many as 15 million visitors to malvertisements. Trend Micro connected Pawn Storm to multiple attacks using Adobe Flash and Java vulnerabilities first discovered in the Hacking Team data cache. Another major botnet takedown took place with seizure of the Dridex banking Trojan's infrastructure and arrests of Andrey Ghinkul, Dridex's author.

In early **November** the VCIC began collecting intelligence that Dridex was recovering and resuming operations. Extortion DDoS threat Actor "The Armada" appeared on the scene attacking several email service providers. Indictments for the criminals responsible for 2014's breach of JP Morgan Chase were made public revealing the bank attacks were part of a stock fraud scheme. Australian grocery retailer Farmer's Direct reported the breach of the account registration information of more than 5,000 customers, but their payment information was not compromised.

MAY
Healthcare
Data breaches cause problems for insurance providers

JUN
OPM breach
21 million victims

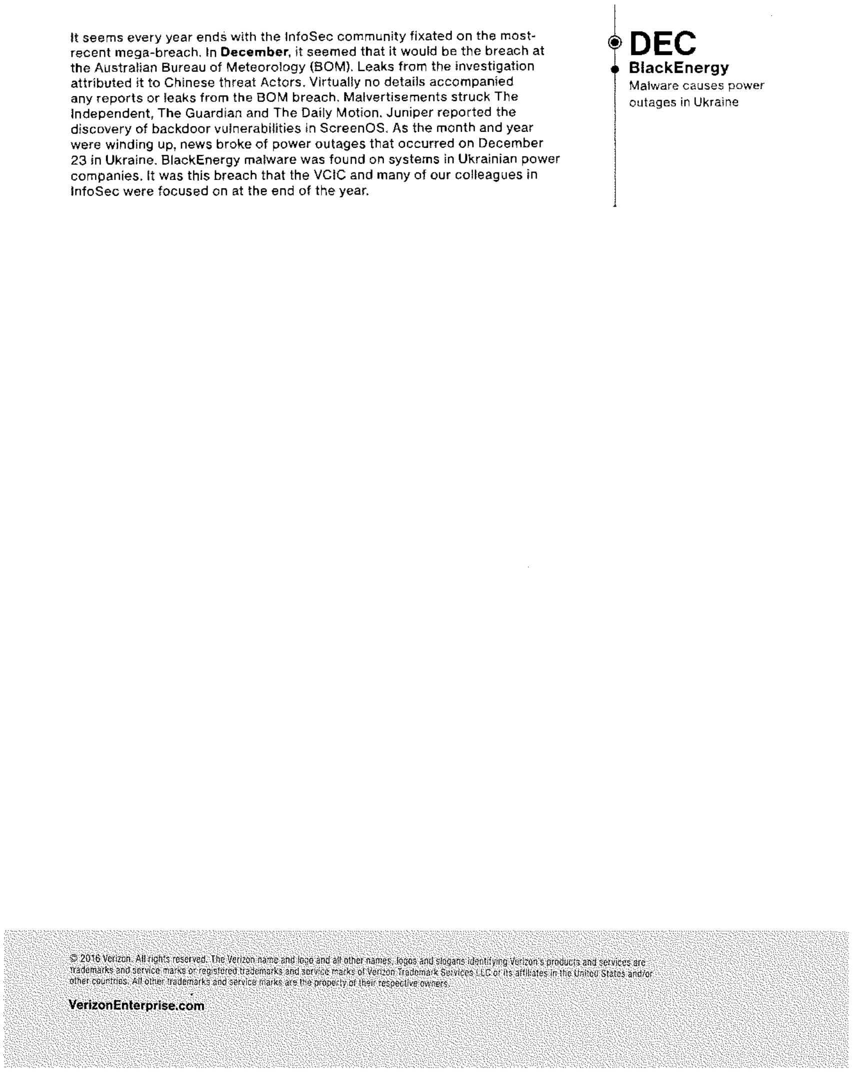
JUL
Ashley Madison
100 GB of stolen data in high-profile compromise

AUG
Ubiquity
$47 million business email compromise

SEP
Blue Termite
Chinese cyber-espionage attack on Japanese companies

OCT
Experion
Breach affects 15 million customers

NOV
Dridex
Banking malware shows up again



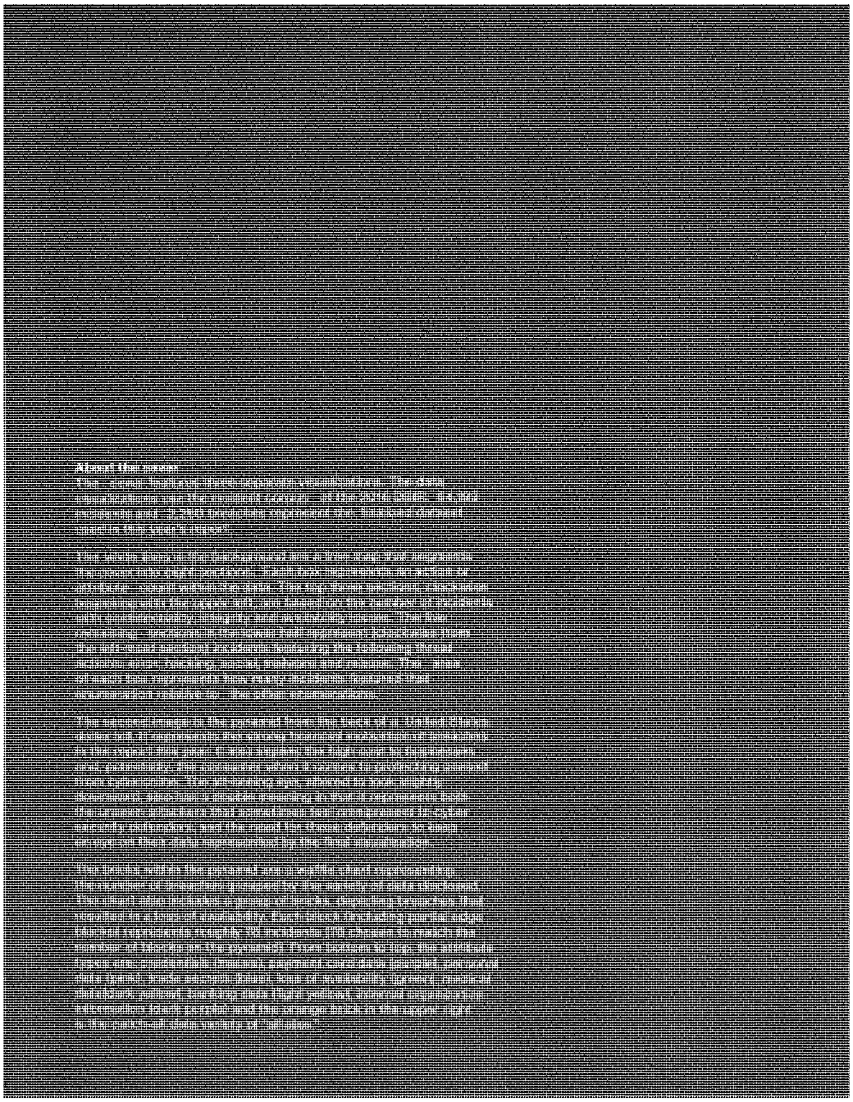
It seems every year ends with the InfoSec community fixated on the most-recent mega-breach. In **December**, it seemed that it would be the breach at the Australian Bureau of Meteorology (BOM). Leaks from the investigation attributed it to Chinese threat Actors. Virtually no details accompanied any reports or leaks from the BOM breach. Malvertisements struck The Independent, The Guardian and The Daily Motion. Juniper reported the discovery of backdoor vulnerabilities in ScreenOS. As the month and year were winding up, news broke of power outages that occurred on December 23 in Ukraine. BlackEnergy malware was found on systems in Ukrainian power companies. It was this breach that the VCIC and many of our colleagues in InfoSec were focused on at the end of the year.

DEC

BlackEnergy

Malware causes power outages in Ukraine

VerizonEnterprise.com



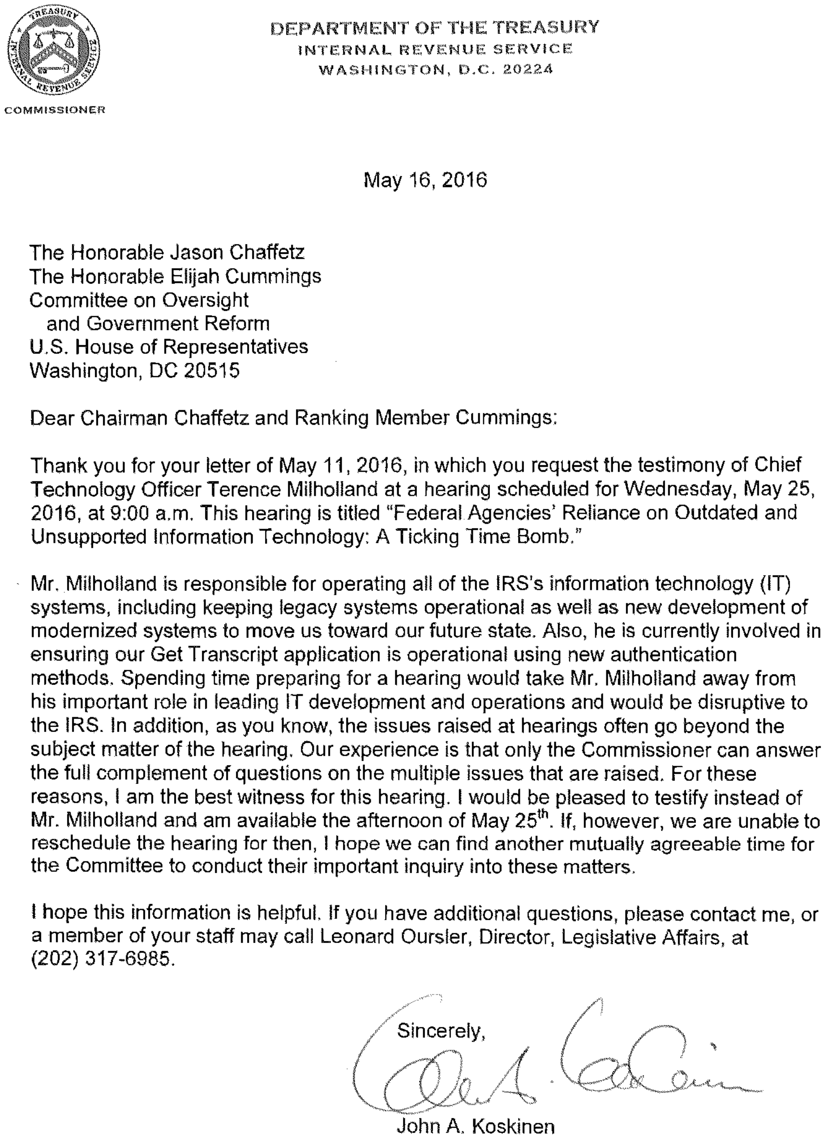
About the cover

The cover features three separate visualizations. The data visualizations use the incident corpus of the 2016 DBIR: 64,199 incidents and 2,260 breaches represent the finalized dataset used in this year's report.

The white lines in the background are a tree map that segments the cover into eight sections. Each box represents an action or attribute count within the data. The top three sections (clockwise beginning with the upper left) are based on the number of incidents with confidentiality, integrity and availability losses. The five remaining sections in the lower half represent (clockwise from the left-most section) incidents featuring the following threat actions: error, hacking, social, malware and misuse. The area of each box represents how many incidents featured that enumeration relative to the other enumerations.

The second image is the pyramid from the back of a United States dollar bill. It represents the secretly intertwined collection of incidents in the report this year. It also implies the high cost to organizations and, potentially, the consumer when it comes to protecting oneself from cybercrime. The all-seeing eye, altered to look slightly downward, also has a double meaning in that it represents both the criminal attackers that sometimes feel omnipresent to cyber security defenders, and the need for these defenders to keep an eye on their data represented by the final visualization.

The blocks within the pyramid are a waffle chart representing the number of incidents grouped by the variety of data disclosed. The chart also includes a group of blocks, depicting breaches that resulted in a loss of availability. Each block (including partial edge blocks) represents roughly 98 incidents (98 chosen to match the number of blocks on the pyramid). From bottom to top, the attribute types are: credentials (maroon), payment card data (purple), personal data (pink), trade secrets (blue), loss of availability (green), medical data (dark yellow), banking data (light yellow), internal organization information (dark purple) and the orange block in the upper right is the catch-all data variety of "other."



COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

May 16, 2016

The Honorable Jason Chaffetz
The Honorable Elijah Cummings
Committee on Oversight
  and Government Reform
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Chaffetz and Ranking Member Cummings:

Thank you for your letter of May 11, 2016, in which you request the testimony of Chief Technology Officer Terence Milholland at a hearing scheduled for Wednesday, May 25, 2016, at 9:00 a.m. This hearing is titled "Federal Agencies' Reliance on Outdated and Unsupported Information Technology: A Ticking Time Bomb."

Mr. Milholland is responsible for operating all of the IRS's information technology (IT) systems, including keeping legacy systems operational as well as new development of modernized systems to move us toward our future state. Also, he is currently involved in ensuring our Get Transcript application is operational using new authentication methods. Spending time preparing for a hearing would take Mr. Milholland away from his important role in leading IT development and operations and would be disruptive to the IRS. In addition, as you know, the issues raised at hearings often go beyond the subject matter of the hearing. Our experience is that only the Commissioner can answer the full complement of questions on the multiple issues that are raised. For these reasons, I am the best witness for this hearing. I would be pleased to testify instead of Mr. Milholland and am available the afternoon of May 25th. If, however, we are unable to reschedule the hearing for then, I hope we can find another mutually agreeable time for the Committee to conduct their important inquiry into these matters.

I hope this information is helpful. If you have additional questions, please contact me, or a member of your staff may call Leonard Oursler, Director, Legislative Affairs, at (202) 317-6985.

Sincerely,

John A. Koskinen