What does the US Department of the Treasury’s Individual Master File (IMF) software—the authoritative data source on American taxpayers—have in common with Apple’s CEO? Like Tim Cook, the IMF will be celebrating its 56th birthday this year, according to a May 2016 US Government Accountability Office (GAO) report on legacy IT investments. The report identified the IMF and its same-aged companion, the Business Master File (which contains the tax information related to individual business-income taxpayers), as the government’s two oldest operating software systems. Indeed, nearly 75 percent of today’s Americans weren’t yet born when the systems went operational. Both are written in assembly code and execute on IBM mainframes—and there are no immediate plans to replace either of them.

The Treasury Department’s elderly software systems are by no means unique. Coming in at 53 years of age are the US Air Force’s Strategic Automated Command and Control System (SACCS), which coordinates the operational functions of US nuclear forces, and the US Department of Veterans Affairs Personnel and Accounting Integrated Data (PAID) system for tracking VA personnel time and attendance. The Air Force system runs on a 1970s-era IBM Series/1 minicomputer and depends on 8-inch floppy disks, while the VA system is written in COBOL and executes on an IBM mainframe. SACCS is slated for an upgrade in 2017, whereas PAID is scheduled to be replaced next year.

The GAO report lists 10 systems that are 39 years old or older (6 are over 50 years old), with half not currently scheduled for either replacement or modernization. In addition, the GAO found that operations and maintenance
(O&M) are absorbing the entire budget of 5,233 of the 7,000 or so IT investments by federal agencies. In total, at least $61.2 billion of the US government’s current $79.4 billion unclassified IT budget is going to O&M. More concerning, the percentage of O&M expenditures has been steadily climbing (due in part to funding constraints) from around 68 percent in fiscal year 2010 to 76 percent in fiscal year 2017, leaving increasingly less funding for IT system modernization or replacement.

The GAO report warns that archaic IT systems pose “a giant problem” in performing the job of government cost-effectively and efficiently, not to mention the threats of operational failure and unauthorized intrusion. For example, in 2015, outdated financial IT systems contributed to at least $136.7 billion in improper federal payments. The actual cost is likely higher, but without the ability to do a complete financial audit, how much higher is uncertain. With federal IT spending expected to remain flat for the next five years, the risks posed by outmoded IT systems will only grow.

**MODERNIZATION OR BUST: COMPETING APPROACHES**

In response to the ticking time bomb of obsolescent IT systems, especially in regard to their cybersecurity vulnerabilities, the Obama administration has proposed creating a $3.1 billion Information Technology Modernization Fund (ITMF)—basically a line of credit—managed by the US General Services Administration (GSA) and provided to government agencies to modernize their IT infrastructure. Upon completing the modernization, the agencies would be required to pay back the funding over time, based upon the garnered savings in O&M expenditures. The administration claims that the ITMF would fund $12–15 billion in modernization projects over the next decade alone.

Initial agencies to receive ITMF funding would be identified by an appointed board of technical and financial experts as those having IT systems most in need of replacement. Agency CIOs could also propose modernization efforts to the board. Another ITMF funding priority would be replacing multiple legacy systems with fewer common platforms that could also be used to facilitate cross-government transition to those same platforms. Furthermore, to encourage use of agile development techniques, ITMF funding could be tied to work products rather than be an annual appropriation.

The ITMF proposal additionally calls for IT experts in acquisition and development to help select and execute modernization efforts, with a publicly accessible online IT dashboard showing the status and progress of each such effort.

While acknowledging possible pushback to elements of the proposal, especially the notion of “borrowing” funding, the administration warns that the status quo is unsustainable—government IT systems can’t be kept on indefinite life support.

As an alternative to the ITMF, a bipartisan group of senators and congresspersons led by Representative Will Hurd (R-Texas) proposed the Modernizing Outdated and Vulnerable Equipment and Information Technology (MOVE IT) Act of 2016. This bill wouldn’t create a central funding pool for legacy IT system modernization but instead would allow each government agency to set up its own working capital fund by reprogramming current O&M funding along with discretionary appropriations. The fund could be used to replace legacy IT systems, transition to cloud computing and innovative platforms or technologies, address security vulnerabilities, or modernize/enhance agency IT activities. Agencies would need to spend the money within three years, and could use any realized savings to replenish their working capital.

Proponents argue that MOVE IT will get more buy-in from agencies, who will retain full control of their IT modernization efforts without GSA involvement. Agencies will also have far more flexibility in funding projects, as they won’t have to wait on yearly congressional appropriations. Moreover, it avoids the tricky issue of what happens if an agency fails to repay an ITMF loan.

Which approach is likely to prevail is unclear at this time. A combination of elements of the two is probable. Whatever approach is adopted, modernizing legacy IT systems is clearly going to be a high governmental priority in the near future.

**THE LEGACY OF LEGACY SYSTEMS: THE MORE THINGS CHANGE …**

Current calls to modernize government IT systems aren’t new. In 1980, a GAO report warned that obsolete computer systems were significantly increasing the cost and lowering the productivity of government operations. It stated that most of the government’s large and medium-size computer systems were no longer fit for purpose, yet few agencies planned to replace them. Even then, less than 5 percent of these systems were under 5 years old, whereas 60 percent were 15 years old or more. Further, agency IT staff spent nearly two-thirds of their time maintaining existing software rather than developing new software. A companion report by then US Comptroller General Elmer Staats succinctly described the situation: “Software maintenance in the Government is now largely undefined, unquantified, and undermanaged.”

---

**EDITORS**

**HAL BERGHEL** University of Nevada, Las Vegas; hlb@computer.org

**ROBERT N. CHARETTE** ITABHI Corp.; rncharette@ieee.org

**JOHN L. KING** University of Michigan; jking@umich.edu
In light of these alarming reports, the newly elected Reagan administration adopted an aggressive IT modernization strategy that continued under the George H.W. Bush and Clinton administrations. However, after more than a dozen years the problem of obsolescent federal IT still hadn’t been resolved and, in many ways, was worse. Efforts to modernize aging computer systems by the Federal Aviation Administration (FAA), Department of Defense (DoD), National Weather Service, and other agencies were in deep trouble or had resulted in costly failures. For example, in 1994, after spending $2.6 billion, the FAA terminated its nearly 15-year attempt to bring the nation’s air-traffic control system out of the vacuum-tube era. 9

That same year, Senator William Cohen (R-ME) authored a widely circulated critique, Computer Chaos: Billions Wasted Buying Federal Computer Systems, in which he stated, “The Federal government continues to operate old, obsolete computer systems while it has wasted billions of dollars in failed computer modernization efforts. … [T]he system is indeed broken and it is time to fix it.” 10 He described in depth the government’s ineffectiveness, if not outright ineptitude, when acquiring, overseeing, and maintaining its IT systems. The report contained eight major recommendations, including emphasizing early oversight and planning; only approving projects of manageable scope, cost, and schedule; and halting existing procurements until the government’s IT acquisition process was improved.

Senator Cohen’s report, along with other ongoing IT project failures like the slow-motion train wreck of the Internal Revenue Service’s $4 billion modernization effort, spurred Congress in 1996 to pass the Clinger–Cohen Act, which sought to reform government IT acquisition and management once and for all. 11,12 The Act had several ambitious goals, such as directing agencies each year for the next five years to achieve at least a 5 percent decrease in O&M costs (in constant fiscal year 1996 dollars) along with a 5 percent increase in operational efficiency through improvements in management. It also elevated CIOs to senior management and directed them to report directly to their top agency administrator in order to give them more input into IT project selection, funding, and deployment.

Unfortunately, but not unexpectedly, the Clinger–Cohen Act’s implementation left something to be desired. For example, overall IT spending including O&M went up, not down, by 9 percent annually by 2006. 13 In addition, by 2011, 15 years after the Act’s passage, only 17 of 30 CIOs were reporting to their agency’s top administrator. 14 Further, cybersecurity threats—something not even highlighted in the Cohen report—became an increasingly troubling O&M concern for agencies.

The Act failed to meet another key objective—reducing large government IT failures. Billions of dollars were wasted on the Census Bureau’s plan to outfit field workers with handheld computers [$2 billion, canceled in 2008], the Army’s software-dependent Future Combat System [$18 billion, canceled in 2009], and the Department of Homeland Security’s SBINet “virtual fence” border control system [$1 billion, canceled in 2011], among other projects. 15–17 In 2013, the disastrous and costly rollout of the HealthCare.gov website, coupled with a number of major cybersecurity incidents including the theft of classified information on the F-35 Joint Strike Fighter and several other weapon systems, accentuated the urgent need to gain control of federal IT systems development, operations, and maintenance. 18,19

In 2014, Congress enacted the Federal Information Technology Acquisition Reform Act (FITARA) in yet another stab at wasteful government IT spending. 20 FITARA aims to enhance (again) the authority and decision-making power of agency CIOs not only in budgeting and acquisition, but in hiring as well. It also attempts to improve the risk management, cost efficiency, and effectiveness of federal IT investments, especially in the areas of datacenter consolidation and hardware, software, and services procurement. To avoid meeting the same fate as the Clinger–Cohen Act, FITARA mandates that agencies rate their progress in meeting the legislation’s requirements.

Although FITARA’s main goal is to improve IT governance, it’s also hoped that CIOs can convince senior decision makers to recognize IT’s central importance to accomplishing their agency’s mission. However, FITARA doesn’t provide any funding to address IT modernization issues, especially in regard to improving cybersecurity or moving to a cloud computing platform—hence the dual ITMF and MOVE IT proposals to upgrade legacy IT systems.

An obvious question is whether the current legislative efforts to modernize federal government IT and reign in O&M costs will succeed when all previous exertions have failed.
For example, Federal CIO Tony Scott claims that agency CIOs will now be held accountable for how well they manage and modernize their agency’s IT, but that seems unlikely given that the average tenure of government CIOs is only two years (versus six in industry).22,23

Many agency executives aren’t too bothered by failure anyway. For example, the Air Force canceled the Expeditionary Combat Support System (ECSS) in 2012 after spending $1 billion and some eight years to deliver a critical logistics system that, the Air Force admitted, didn’t yield “any significant military capability.”24 Asked whether anyone would be demoted or fired, the last general in charge of the project said no one believed that it was necessary.25 Apologies for the wanton waste also don’t seem necessary. An internal Air Force review even went so far as to proclaim that ECSS shouldn’t be seen as a failure but as “the first step to understanding” what needed to be done.26

This “What, me worry?” perspective is reinforced by the pervasive- ness of what NASA Inspector General Paul K. Martin terms “Hubble Psychology,”27 in which project personnel (government workers and contractors alike) expect that “projects that fail to meet cost and schedule goals will receive additional funding and that subsequent scientific and technological success will overshadow any budgetary and schedule problems.”27 A corollary to this optimism bias is that if the project does get canceled, program managers are confident that it’ll be resurrected again sometime in the future. The ECSS project, for example, was the Air Force’s third major failed attempt to deliver a modernized logistics system since the 1980s. One can surmise that learning from past mistakes isn’t a requirement for government IT modernization, claims to the contrary notwithstanding.

Even public scrutiny isn’t much of a deterrent. Since 2009, the US government has made a concerted effort to make the progress of modernization projects more transparent by publishing progress data on an IT dashboard. When the dashboard was rolled out, then Federal CIO Vivek Kundra said that it would enable “better decision-making, giving us the ability to turn around poorly performing projects and to divest from those which no longer make sense,” because agency CIOs would be rating the projects.28

However, as the GAO reported in June of this year, federal agency CIOs are an optimistic bunch who are more likely to believe that their projects are less risky than they really are.29 For instance, the GAO examined 95 IT investments across 15 different agencies and found that 60 of them are at greater risk of failure than was indicated by the CIOs, including 10 rated as low risk that were in fact high risk. On the positive side, 13 projects were rated as being higher risk than the GAO said they should be.

In addition, the GAO found that many agencies didn’t provide timely data for display on the dashboard, making it difficult to track projects’ status. IT modernization efforts can easily be identified as being at medium or even low risk of failure all the way up until the day they’re canceled or, more likely, restarted. For example, the US Social Security Administration (SSA)’s new Disability Case Processing System (DCPS) was officially listed as a low-risk project even though for 5 consecutive years Release 1.0 was projected to be 24–32 months away from completion.30 Not surprisingly, when a working release of DCPS was finally deployed, it fared poorly. After repeated attempts to fix it, the SSA decided in 2015 to write off nearly the entire initial investment of $311 million and start the DCPS project again from scratch at an additional cost of at least $131 million.31 The dashboard also listed ECSS as being a medium-risk project though it was widely acknowledged to be spiraling out of control.

Another recurring and predictable issue involves trust—or, better put, mistrust. An Institute for Defense Analyses (IDA) report on repeated DoD enterprise resource planning (ERP) modernization project failures found that “Program managers are unable to deliver a completely factual version of their status to leadership if it contains any element that could be considered significantly negative. … Program managers fear that an honest delivery of program status will result in cancellation. As a result of this, leadership is unable to be effective in removing obstacles to program success.”32 In fact, the IDA noted, program personnel needed “courage” to deliver bad news to senior agency leadership, as doing so might be career threatening. This phenomenon isn’t confined to the DoD by any means.

Finally, there is a generally negative perception of IT O&M within government. In the words of British technology historian David Edgerton, O&M exists in a “twilight world” even though the machinery of government is fully dependent upon it.33 A 1981 New York Times article on federal IT modernization efforts stated that O&M had all “the appeal of technological janitorial work,”34 and little has changed since then. A recent Partnership for Public Service report found that many federal IT support staff feel “disconnected” from their agency and not regarded as being integral to its success.35

Several decades’ worth of internal and external audits of abortive government IT modernization efforts suggest that trying to legislate away the problem is wishful thinking. As safety expert Sidney Dekker would contend, it’s time to examine the organizational dynamics and behavioral motivations underlying such projects’ “drift into failure.”36 With more than $200 billion to be spent on IT system development, modernization, and enhancement at the federal level and another $150 billion at the state and local levels over the next decade, not to mention hundreds of billions more for O&M on obsolete systems, waiting will be costly. Otherwise, by around 2025 we can expect another round of disheartening reports
and proposed legislative solutions to the same old IT legacy problems.

REFERENCES


space/military/the-us-air-force -explains-its-billion-ecss-bonfire.


ROBERT N. CHARETTE, coeditor of the Aftershock column and founder of ITABHI Corporation, is an internationally acknowledged authority and pioneer in risk management, systems engineering, and the lean development and management of large-scale software-intensive systems. Contact him at rncharette@ieee.com.