

The U.S. Government's IT Fossils

February 2016

Americans won't soon forget the botched launch of Healthcare.gov. The website, intended to support signups for the new Affordable Care Act, came online in October 2013; but it quickly failed as it proved to be incapable of handling the subscription load imposed upon it. Eventually, the website became operational with the help of some bright engineers from Google, Oracle, and other Silicon Valley companies. Originally budgeted for USD \$95 million, the ultimate cost of the website, according to the Office of Inspector General, reached USD \$1.7 billion.



Healthcare.gov is a modern system that now is performing flawlessly. This is not the case with the bulk of government IT systems. Most are decades old and are experiencing an alarming rate of outages.

The Sad State of the U.S. Government's Legacy Systems

The U.S. government operates 28 systems that are at least 25 years old and eleven systems that are more than 35 years old. It spends USD \$60 billion, 75% of its IT budget, each year to keep these systems running. Just finding the skill sets to maintain the systems is becoming increasingly difficult. Less than 25% of college computer-science programs teach old-school skills such as COBOL.

Aging federal IT systems are seen as a security risk. Many of the older systems are impossible to secure against cyberattacks. When the Office of Personnel Management (OPM) was hacked in mid-2014,¹ it took a year to discover the attack. By that time, information on 22 million federal employees and contractors had been stolen. None of the social security numbers stored in the 1980s-era database were encrypted. The storage arrays were too old to support encryption.

U.S. Federal Chief Information Officer Tony Scott has stated that the problem of outdated federal IT systems is a crisis that is bigger than Y2K. In testimony before the U.S. Congress, he asserted that "much of the government runs on very old, outdated technology."

In a survey by Symantic, 70% of federal agencies experienced downtime of thirty minutes or more in the month studied. The breakdown of outage root causes included the following:

- 45% were blamed on network outages or server problems.
- 20% were caused by Internet connectivity loss.
- 13% were the result of natural disasters.
- 7% were due to application errors.
- 6% were caused by human error.

¹ The Government OPM Hack Gets Worse, *Availability Digest*, July 2015.
http://www.availabilitydigest.com/public_articles/1007/OPM_attack_2.pdf

When outages occur, 48% of workers said that they do what they can by telephone. 33% use personal devices. 24% try to find a workaround, such as Google Apps.

When asked to grade their IT departments, workers gave an “A” in 15% of the cases. A “B” was awarded in 49% of the cases, and a “C” grade was given in 27% of the cases.

In 2014, the U.S. Congress passed a sweeping IT acquisition reform bill, the “Federal Information Technology and Acquisition Reform Act.” The bill seeks to dig into the reliance by federal agencies on aging software and archaic hardware.

One agency in particular has become a focus of the act, and that is NASA, the U.S. National Aeronautics and Space Administration. NASA operates 67 systems whose value totals USD \$1.4 billion. Lawmakers have rated NASA with a grade of “F,” just one of three agencies to earn a failing grade. Seeking answers about the age and overall health of NASA’s mission-critical systems, lawmakers asked:

- What are NASA’s top three mission-critical legacy IT systems in need of modernization or replacement and the planned date to switch over from the old technology?
- What are the top five oldest IT hardware systems and software applications used by NASA?
- Do the five oldest systems and applications support any mission-critical programs?
- What are the oldest programming languages, such as COBOL or Fortran, used by NASA?
- How many staff members are available to maintain code in these archaic languages?

Undergoing similar scrutiny under the Act will be several other agencies that have a history of chronic outages. Some examples follow.

The Six-Week Outage of the U.S. Immigration Court System

The U.S. Executive Office for Immigration Review (EOIR) supports 59 immigration courts. These courts decide which foreign-born individuals that have violated immigration laws must be deported and which ones can stay in the U.S.

On April 12, 2014, five servers located in the EOIR headquarters in Falls Church, Virginia, U.S.A. failed. Information provided by EOIR indicated that the five servers needed parts that would not be available until sometime the following month. How could five servers be simultaneously damaged to the extent that parts had to be replaced? Sounds like a power failure gone seriously wrong to us.

In any event, the servers were repaired and returned to service at the end of May 2014. The EOIR immigration courts were without IT services for six weeks.

The immigration court judges do not have court reporters. Rather, all court proceedings are recorded digitally. They are transcribed later only if needed. During the six-week outage, court proceedings were recorded on cassette recorders.

The 260 immigration court judges turned to pencil-and-paper methods for taking notes. This outage slowed an already clogged immigration court system with a backlog of 360,000 cases. EOIR had to prioritize cases to compensate for its reliance on manual processes.

When the EOIR system was restored to service, all of the information captured manually over the previous six weeks had to be entered into the computer system. This process took months before the courts were able to fully return to the use of online court proceedings.

The Multi-Day Outage of the State Department's Visa and Passport System

The U.S. State Department operates the Consular Consolidated Database (CCD). The CCD supports worldwide visa and passport verification operations and allows visas to be printed and passports to be issued.

The CCD contains more than 100 million visa cases and 75 million photographs. It has links to other federal agency security databases, such as those of the FBI (the U.S. Federal Bureau of Investigation), the U.S. Department of Homeland Security, and the U.S. State Department. About 35,000 new visa cases are added to the CCD every day (about twelve million per year). The CCD is one of the largest Oracle-based databases in the world.

On July 19, 2014, the CCD system crashed shortly after maintenance was performed on it. The State Department indicated that the root cause of the outage was a combination of software optimization and hardware compatibility issues. Evidently, the database had not been taken offline during the maintenance operation and was subsequently corrupted as a result of the sudden outage.

It took over a week to repair the database and to bring the system back online. The outage stranded thousands of people worldwide who no longer could complete their visa or passport applications to get into the United States. In most cases, there was little doubt of the traveler's right to enter the United States. However, there was no manual workaround procedure available. Consular officers explained to frustrated travelers that they could not handwrite visas because security measures prevent consular officers from printing visas unless they are approved through the CCD database system. Similarly, passports could not be issued without CCD approval.

Once the system was returned to service, there was a massive backlog of visa and passport applications to clear up, a process that took several weeks and delayed travelers even further.

The One-Week Outage of the U.S. Patent and Trademark Office System

When Anthrax was mailed to several Capitol Hill offices in the fall of 2001, the United States Patent and Trademark Office (USPTO) set out to become a paperless agency. It now has achieved that goal. Patent applications are filed via their new Electronic Filing System (EFS). The EFS also provides communication services between the patent examiners and the patent practitioners.

On December 22, 2015, the USPTO experienced a catastrophic major power outage at its headquarters in Alexandria, Virginia, U.S.A. In a statement that it issued, the USPTO explained:

"Power that comes into the USPTO's main building feeds two power filtration systems that provide steady, "filtered" power so systems don't suffer from damaging surges or drops in power supply. A malfunction in the power supply lines feeding these two systems caused significant damage to both systems. This is what we believe caused our systems to go down on Tuesday night.

"Because of their size, these large and highly complex power filtration systems cannot be easily replaced. We are working with service providers to obtain a source of uninterrupted conditioned power to the data center as soon as possible."

It took the USPTO a week to replace the damaged power filtration systems so that it could get its EFS system back online and work through the backlog of patent applications that had formed during the outage.

Summary

The U.S. government faces the same problems as such other industries as financial-services and health-care.² It is saddled with legacy IT systems that are decades old. These systems are fragile and often unmaintainable. The availability of the software skills required to correct or modify legacy applications are disappearing rapidly.

The government spends the majority of its IT budget on maintaining its old applications. However, replacing the applications would be even more costly. Fortunately for the U.S. government, the “Federal Information Technology And Acquisition Reform Act” recently passed by the U.S Congress may be the salvation of these systems if it motivates Congress to provide the funds necessary to upgrade at least the mission-critical systems upon which the nation depends.³

Acknowledgements

Material for this article was taken from the following sources:

IT outages are an ongoing problem for the U.S. government, *Computerworld*; August 19, 2014.

The Crisis in Federal IT That’s Scarier Than Y2K, *Nextgov*; November 20, 2015.

Lawmakers Take On Federal IT Fossils, *Nextgov*; December 29, 2015.

U.S. Immigration Court System Outage Enters Week Six, *IEEE Spectrum*; May 19, 2014.

State’s passport and visa system crashes, *FCW*; July 24, 2014.

US State Department database used to process passports and visas still hasn’t recovered from a crash last week – leaving tens of thousands of people stranded overseas, *Information Week*; July 30, 2014.

USPTO experiences catastrophic failure of electronic patent and trademark systems, *IP Watchdog*; December 28, 2015.

² RBS – A Poster Child for Outages, *Availability Digest*; January 2016.

http://www.availabilitydigest.com/public_articles/1101/rbs.pdf

³ As a side note, President Obama has included such funds in his proposed budget for the next fiscal year, but the Republican-dominated Congress has declared that it will ignore his budget.