Can a Hydra Ever Be a Good Pet? Federal Information Technology Modernization's Likely Failure

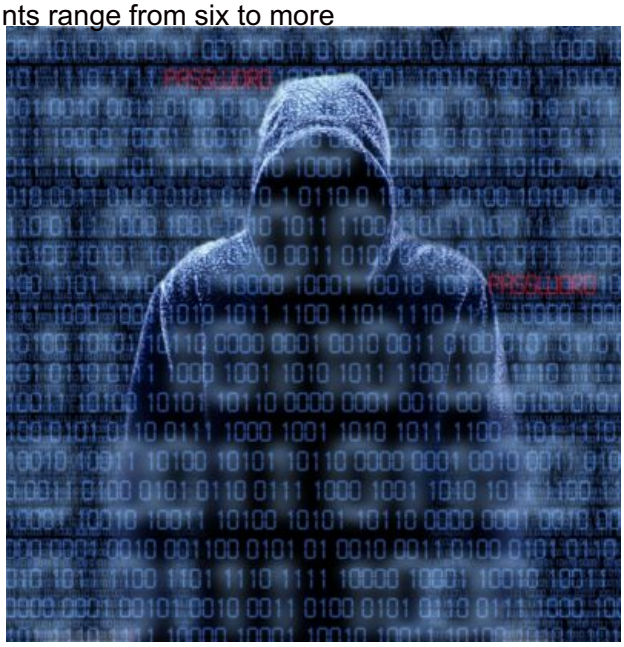
fpri.org/article/2017/04/can-hydra-ever-good-pet-federal-information-technology-modernizations-likely-failure/

April 24, 2017

E-Notes

Lawrence Husick

Lawrence Husick is Co-Chairman of the Foreign Policy Research Institute's Center for the Study of Terrorism. He is also co-director of the FPRI Wachman Center's Program on Teaching Innovation and a faculty member at the Whiting Graduate School of Engineering and the Krieger School of Arts and Sciences Graduate Biotechnology Program of the Johns Hopkins University.Read More



In Greek mythology, the Hydra was a many-headed serpent (accounts range from six to more than 50 heads) which grew back at least two heads for each one lopped off. The Hydra had poisonous breath and blood so virulent that even its scent was deadly. It took Heracles to vanquish the beast in his second labor. It's a pity then that the less-than-heroic Jared Kushner now has the task of modernizing and reforming the federal government's information technology (IT) and cybersecurity infrastructure—a hydra-like beast if ever there was one.

Emblematic of the magnitude of Mr. Kushner's labors, the department of Health and Human Services under Dr. Tom Price is now establishing its own version of the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC). The new Health Cybersecurity and Communications Integration Center (HCCIC) will become operational in June 2017 and will educate health organizations and consumers about the risks of using mobile applications and data. The Centers for Medicare and Medicaid are looking into a similar concept, but have not announced specific plans as of April 2017. Other federal agencies already host similar operations. Almost none of these are directly connected to either military or intelligence units tasked with defensive cyber operations.

Under President Obama, various cybersecurity bills died on Capitol Hill, prompting the Executive Branch to promulgate several frameworks for cybersecurity developed by the National Institute for Standards and Technology (NIST). These voluntary "best practices" documents were to have served as a blueprint for government and the private sector, but primarily due to a lack of funding, have mostly been relegated to occupying bookshelf space. Even within the federal government, the most notable cybersecurity actions have comprised strongly slamming barn doors at agencies ranging from the Department of State to the Office of Personnel Management after the livestock has been taken by foreign rustlers.

Federal agencies as diverse as NORAD and the IRS use outdated technology that would embarrass any private-sector CIO. According to a May 25, 2016 Government Accounting Office (GAO) Report, some federal agencies are today still using Windows 3.1 (last supported on December 31, 2001), the decades-old COBOL and Fortran programming languages, and computers purchased in 1970s for which spare parts must now be found on eBay. A backup nuclear control messaging system at the Department of Defense runs on an IBM Series 1 computer from

1976 that uses eight-inch floppy disks, while the Internal Revenue Service's master file of taxpayer data is written in assembly language code that's more than fifty years old. Many other agencies run systems of similar venerable age using ancient technologies. Meanwhile, Congress has cut over $7.3 billion from the federal IT modernization budget since 2010, and the government now spends the vast majority of its budget on operations and maintenance. A January 2013 report from the Defense Science Board concluded that the United States could not even ensure that the IT systems involved in our nuclear triad were safe from hackers.

Enter Mr. Kushner and his new "White House Office of American Innovation." Among a host of other initiatives (personnel policies and workforce development, combating opiate abuse, and providing universal broadband internet access), the Office will work on "modernizing the technology and data infrastructure of every federal department and agency." What is not clear, however, is whether such agencies and departments are either able or willing to engage in modernization.

For example, the private sector has largely determined that cloud-based infrastructure and services are more efficient and cost-effective than older client-server or host-based systems. Front-ended by mobile and desktop "apps," cloud services from Amazon to iTunes to TurboTax show the way, and yet, few government services show even the slightest movement in this direction. It is understandable that we may not want to have the nuclear "football" give way to an Android App that could be activated by a mistake, but the clear benefits of making personal tax return filing as easy as the TurboTax 1040EZ app make such innovations a clear path forward for government. Secure "two-factor" and biometric authentication make this path an even better option for government systems still stuck in the username and password hell of older generation systems that have been retrofitted for marginally better security at the expense of usability.

The GAO estimates that there are approximately 7,000 information technology programs in the federal government (and clearly there are at least an order of magnitude more in the state and local governments around the nation that are beyond both the scope of the GAO report and of Mr. Kushner's mission.) More than 5,200 IT efforts in the federal government now spend 100% of their funding on operations and maintenance, and have no budget to even think about modernization. There simply is nobody at each of these offices for Mr. Kushner and his team to engage.

President Trump, in appointing his son-in-law to this task, told the nation that, "As a former leader in the private sector, I am proud to officially announce the White House Office of American Innovation, which will develop innovative solutions to many problems our country faces." For a small office working on multiple simultaneous priorities from a thinly staffed White House, and without an immediate and gigantic budgetary allocation from Congress that reverses the decades-long slide into obsolescence to even attempt to catalog, let alone modernize the federal IT infrastructural hydra is, at best, a pipe dream.

We should expect more "go-it-alone" solutions from executive agencies like HHS, more balkanization, more IT systems held together with "spit and baling wire," and more exposure of hacked systems until the magnitude of the problem becomes painfully evident on Capitol Hill. We can only hope (because we do not actually know) that it is not already too late for some critical systems.