Cyber Update
27 March 2019
By Michael Kans

Budget Request Trims IT Funding and Boosts Cyber Funding

Last week, the Trump White House released more detailed information on its FY 2020 budget request, particularly about cybersecurity, information technology, and related policy areas. In terms of top-line funding, the Trump Administration identified $87.79 billion requested for FY 2020 IT programs ($36.749 billion for the Department of Defense (DOD) with the balance of the government accounting for $51.041 billion), a slight cut from the current year's funding of $87.792 billion ($50.048 billion for non-DOD agencies and $37.924 billion for the DOD). The White House requested "additional Technology Modernization Fund (TMF) funding ($150 million) to meet the demand generated by agencies and to invest strategically in modernizing agency systems" even though it noted that more than 50 requests totaling more than $500 million have been submitted to date. Overall, "cybersecurity-related" programs would be funded at $17.435 billion, "an $790 million (5 percent) increase above the FY 2019 estimate." The Trump Administration is proposing a funding cut for the new Cybersecurity and Infrastructure Security Agency (CISA). In FY 2019, Congress appropriated $1.346 billion for CISA, and the Administration is asking for $1.279 billion for FY 2020. Further, the Administration asserted that "approximately $850 million at the Department of Energy (DOE), National Institutes of Health (NIH), National Institute of Standards and Technology (NIST), and National Science Foundation (NSF)" is being dedicated to the President's Artificial Intelligence (AI) Initiative.

In terms of programmatic announcements, the budget request was largely a recitation of steps and initiatives announced in the previous two calendar years, including Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Executive Order 13859, *Maintaining American Leadership in Artificial Intelligence*, a draft Federal identity policy: *Strengthening the Cybersecurity of Federal Agencies through Improved Identity, Credential, and Access Management, Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements (M-19-02)*, *2018 Federal Cloud Computing Strategy — Cloud Smart*, *Update to the Trusted Internet Connections (TIC) Initiative*, and the *Data Center Optimization Initiative*.

The Office of Management and Budget (OMB) broke out its IT funding requests by non-defense agency:

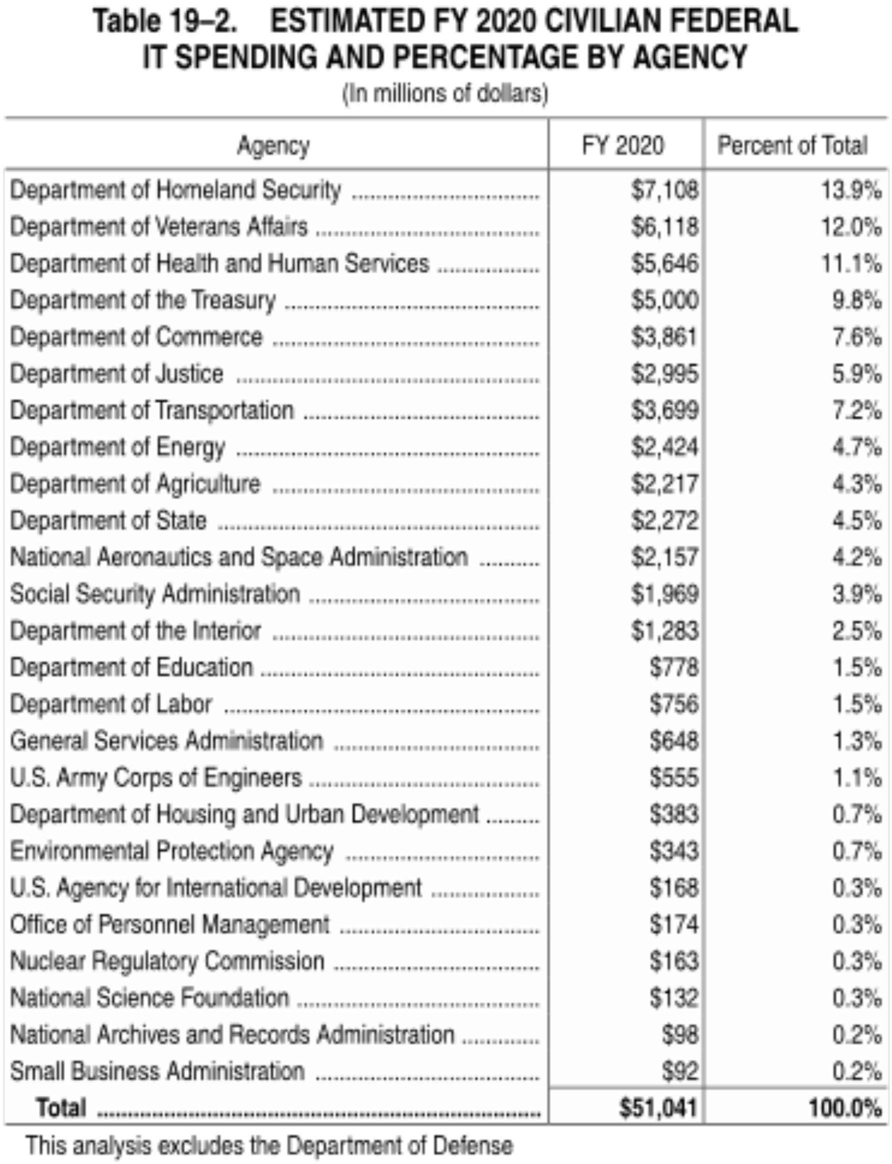

Table 19–2. ESTIMATED FY 2020 CIVILIAN FEDERAL IT SPENDING AND PERCENTAGE BY AGENCY

(In millions of dollars)

Agency	FY 2020	Percent of Total
Department of Homeland Security	$7,108	13.9%
Department of Veterans Affairs	$6,118	12.0%
Department of Health and Human Services	$5,646	11.1%
Department of the Treasury	$5,000	9.8%
Department of Commerce	$3,861	7.6%
Department of Justice	$2,995	5.9%
Department of Transportation	$3,699	7.2%
Department of Energy	$2,424	4.7%
Department of Agriculture	$2,217	4.3%
Department of State	$2,272	4.5%
National Aeronautics and Space Administration	$2,157	4.2%
Social Security Administration	$1,969	3.9%
Department of the Interior	$1,283	2.5%
Department of Education	$778	1.5%
Department of Labor	$756	1.5%
General Services Administration	$648	1.3%
U.S. Army Corps of Engineers	$555	1.1%
Department of Housing and Urban Development	$383	0.7%
Environmental Protection Agency	$343	0.7%
U.S. Agency for International Development	$168	0.3%
Office of Personnel Management	$174	0.3%
Nuclear Regulatory Commission	$163	0.3%
National Science Foundation	$132	0.3%
National Archives and Records Administration	$98	0.2%
Small Business Administration	$92	0.2%
Total	**$51,041**	**100.0%**

This analysis excludes the Department of Defense

In the DHS Budget In Brief, the Department of Homeland Security provided a summary of its CISA request:

> Securing Cyberspace
> We continue to improve our collective efforts in cybersecurity with the recent creation of the Cybersecurity and Infrastructure Security Agency (CISA). CISA is charged with protecting the Nation's critical infrastructure from physical and cyber threats, requiring collaboration between both government and private

sector organizations. DHS is focused on stepping up our digital defense as cybersecurity threats grow in scope and severity. To assess evolving cybersecurity risks, protect Federal Government information systems, and protect critical infrastructure, the FY 2020 President's Budget continues investments in federal network protection, proactive cyber protection, and infrastructure security.

- $694.1 million for federal network protection, which includes Continuous Diagnostics and Mitigations (CDM), National Cybersecurity Protection System, (NCPS), and Federal Network Resilience. These programs provide the technological foundation to secure and defend the Federal civilian Government's IT infrastructure against advanced cyber threats.
- $371.4 million for proactive cyber protection. Requested funds support the National Cybersecurity and Communications Integration Center (NCCIC), the civilian hub for sharing cyber threat indicators and defensive measures with Federal and non-Federal entities, and the private sector as well as supporting election infrastructure.

Nielsen Previews DHS Strategic Plan and Details Cyber Worries

Last week, Secretary of Homeland Security Kirstjen Nielsen delivered her 2019 State of Homeland Security Address in which she wanted to "preview our bold, new strategic plan by walking you through a few of the Department's overarching goals." However, Nielsen was careful not to discuss a homeland security theme President Donald Trump often raises during his public appearances and on Twitter: the U.S.-Mexico border and immigration. This Congressionally-required strategic plan follows last May's "Cybersecurity Strategy" (Strategy) that "provides the Department with a framework to execute our cybersecurity responsibilities during the next five years to keep pace with the evolving cyber risk landscape by reducing vulnerabilities and building resilience; countering malicious actors in cyberspace; responding to incidents; and making the cyber ecosystem more secure and resilient."

Nielsen noted that DHS was founded "to fight one primary, generation-defining struggle: the war on terror…[b]ut we now find ourselves defending against emerging threats on new battlegrounds." She contended that "[n]ot only are we still facing the insidious threat from global jihadists, but we are under siege from transnational criminals…faceless cyber thugs and hackers…and resurgent nation-state rivals." Nielsen said that "[t]oday, I am more worried about the ability of bad guys to hijack our networks than their ability to hijack our flights…[a]nd I am concerned about them holding our infrastructure hostage…stealing our money and secrets…exploiting children online…and even hacking our democracy."
Nielsen asserted that "[t]he idea that we can prevail with so-called "Whole of Government" efforts is now an outdated concept." She claimed that "[w]e need a

"Whole of Society" approach to overcome today's threats." Nielsen noted that "President Trump has made homeland security his number-one priority…[and] [i]t's Pillar One of the U.S. national security strategy." She added that "as Secretary of Homeland Security, I am running with that mandate to obtain the resources, to secure the authorities, and to execute the changes we need to fully transform homeland security and give the American people the protection they deserve."

Nielsen said that "[o]n the top of my list of threats—the word CYBER is circled, highlighted, and underlined…[and] [t]he cyber domain is a target, a weapon, and a threat vector—all at the same time." She said "[t]hat is why another goal in our strategic plan is Secure Cyberspace and Critical Infrastructure." Nielsen said that "[w]hat worries me, though, is not what these threat actors have done, but what they have the capability to do: stealing our most sensitive secrets…deceiving us about our own data… distracting us during a crisis…launching physical attacks on infrastructure with a few keystrokes…or planting false flags to embroil us in conflict with other nations."

Nielsen said that "[t]o get ahead of our adversaries, we released the first DHS Cybersecurity Strategy last May…[which] was Step One." She said that "Step Two was partnership…[s]o DHS held a first-of-its-kind National Cybersecurity Summit in New York City…[that] produced real results." Nielsen claimed that "[p]articipants took action to deepen partnerships, break down barriers, and better integrate collective risk-management efforts." She added that DHS "announced the formation of the National Risk Management Center (NRMC), a premier forum for government and industry to collaborate against evolving digital dangers." Nielsen noted the authorization and founding of the Cybersecurity and Infrastructure Security Agency—CISA—at DHS."

Nielsen stated that "strategies, partnerships, and organizational change will still only get us partway…[s]o we have ramped up operations to keep intruders out of our networks:

- First and foremost, we have driven a change in U.S. policy to replace complacency with consequences. We have made clear we will no longer accept malicious cyber interference. We are fighting back in both "seen and unseen" ways, including publicly attributing cyber attacks to the perpetrators, levying sanctions, and delivering other consequences.
- We have also instituted a next generation risk management approach to identify and assess critical functions—not only specific assets and systems. We are wielding DHS authorities to get dangerous software, such as Kaspersky-branded products, out of federal systems…and taking swift action to patch newly discovered vulnerabilities.

- Alarmingly, our adversaries are using state-owned companies as a "forward-deployed" force to attack us from within our supply chain. So we are working with industry partners to identify and delete these bugs and defects from our systems.
- But of all the digital threats, the ones we must take most seriously are those aimed at the very heart of our democracy. In 2016, at the direction of Vladimir Putin, Russia launched a concerted effort to undermine our elections and our democratic process using cyber-enabled means. Unfortunately, other nation-state rivals appear to be following suit and are—in various ways—working to virtually influence U.S. policy and discourse.

Nielsen said "let me just send one last message to our cyber adversaries: you cannot hide behind your keyboards and computer screens…we are watching you…and no matter what malware you develop, I promise you, the engines of our democracy are far stronger and far more resilient than any code you can write." She contended that "[l]ast year we applied our "lessons learned" from 2016 to prevent hacking in the 2018 elections…[and] [w]e worked to support all 50 states in a variety of ways, including technical assistance, security assessments, planning, exercises, sharing of threat data, and incident response."

Nielsen said that "[n]ow we have our eyes on the next election and are launching "Protect 2020," a new initiative designed to get all States to a baseline level of election infrastructure cybersecurity well before the next vote." She added that "[m]ore broadly, DHS is in the process of bolstering its approach to countering foreign influence to ensure we are prepared to "zoom out" and see the full scope of adversary attempts to undermine our networks, our nation's critical infrastructure, and our homeland security."

Top State Cyber Official Fleshes Out Cyber Deterrence Initiative

At a cybersecurity conference last week, Deputy Assistant Secretary for Cyber and International Communications and Information Policy Robert Strayer provided additional detail on the elements of a "Cyber Deterrence Initiative." Strayer said that that the first element is determining the types of cyber conduct the U.S. wants to deter. The second element would streamline the process by which the U.S. and like-minded nations could issue joint attributions. To date, a number of joint attributions have been issued, including the 2018 U.S.-United Kingdom statement on malicious cyber activity carried out by Russian government and the 2018 report on "five publicly available tools, which have been used for malicious purposes in recent cyber incidents" released by Australia, Canada, New Zealand, the U.K., and the U.S. The third element centers on how to make bad cyber actors feel consequences, which Strayer noted would require the development of "a broader range of tools that we can bring to bear to change the calculus of the adversaries." The fourth element is effective deterrence arising from advance warning that malicious activity directed at the U.S. will result in retaliation. Strayer noted that "[f]or it to truly be deterrence-based, we need to signal that we will act this way in advance of the deterrent to deter the adversaries rather than just respond to them."

Last year's "National Cyber Strategy" sketched out a new "Cyber Deterrence Initiative:"

> The imposition of consequences will be more impactful and send a stronger message if it is carried out in concert with a broader coalition of like-minded states. The United States will launch an international Cyber Deterrence Initiative to build such a coalition and develop tailored strategies to ensure adversaries understand the consequences of their malicious cyber behavior. The United States will work with like-minded states to coordinate and support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors.

OMB Refines and Refocuses Category Management

Last week, the Office of Management and Budget (OMB) released a new memorandum to alter the government's program to leverage its size and collective spending across categories of services and goods to drive down the prices of these purchases. While the Category Management initiative was started on a more modest scale two administrations ago, it was much enlarged during the Obama Administration and continued by the Trump Administration. The central thrust of the program is that the federal government buy these common goods and services as one entity instead of many current practices of agencies and components within agencies buying separately.

OMB explained that:

> Each year, the Federal Government spends hundreds of billions of dollars–over $325 billion in FY 2018–for common goods and services, such as software, mobile devices and professional services. The lack of mechanisms to support agency collaboration on common contract solutions has resulted in billions of dollars in lost cost avoidance, inappropriate contract duplication, and missed opportunities to adopt Government and industry best practices. These missteps have also unnecessarily added to the workload of the acquisition workforce, whose talents and time could produce greater return if they could focus more on mission critical acquisitions.

OMB defined the term “category management” as “the business practice of buying common goods and services as an enterprise to eliminate redundancies, increase efficiency, and deliver more value and savings from the Government's acquisition programs.” OMB stated that “[t]eams of experts in each category of spending help agencies increase their use of common contract solutions and practices and bring decentralized spending into alignment with organized agency-and Government-level spending strategies by sharing market intelligence, Government and industry best practices, prices paid data, and other information to facilitate informed buying decisions.”

OMB explained the memorandum is “designed to build on [previously started Category Management] activities in order to help the Government buy as a coordinated enterprise and avoid the waste associated with duplicative contract actions.” OMB added that “a number of activities in this Memorandum emphasize robust communications, consistent with law and acquisition best practices, between contractors who sell common goods and services and all levels of the Federal Government that have responsibility for category management – namely, category managers, Federal organizations that manage Government-wide smart solutions (BIC solution owners), and agency officials who are responsible for determining the best way to meet their everyday requirements.”

OMB stated that “[a]gencies shall undertake the following five key category management actions to better position themselves to bring spending under management and leverage common contract solutions and practices:

1. Annually establish plans to reduce unaligned spend and increase the use of BIC solutions for common goods and services, consistent with small business and other statutory socioeconomic responsibilities;
2. Develop effective vendor management strategies to improve communications with contractors, especially those that support mission-critical functions;
3. Implement demand management strategies to eliminate inefficient purchasing and consumption behaviors;
4. Share data across the Federal Government to differentiate quality and value of products and services in making buying decisions; and
5. Train and develop the workforce in category management principles and practices.

The notion of buying like items across the federal government has been a focus of OMB’s since the George W. Bush Administration when the Federal Strategic Sourcing Initiative (FSSI) program was launched. In 2016, the Government Accountability Office (GAO) explained

> From fiscal year 2011 through 2015, federal agencies reported spending almost $2 billion through the Federal Strategic Sourcing Initiatives (FSSI) GAO reviewed and reported an estimated total of $470 million in savings. Federal agencies' low use of the FSSIs, however, diminished the potential savings that could have been achieved. For example, in fiscal year 2015, federal agencies spent an estimated $6.9 billion on the types of goods and services available through these FSSIs. Of this amount, $4.5 billion was considered "addressable" and could have been spent through the FSSIs, but just $462 million was. While total savings reported for fiscal year 2015 came in at $129 million—a savings rate of 28 percent—had all of the agencies directed their addressable spending through FSSIs, up to $1.3 billion in savings could have been achieved, assuming the same savings rate.

GAO found that OMB's "Office of Federal Procurement Policy's (OFFP) category management initiative largely incorporates key lessons learned from the FSSIs into guidance, such as addressing small business concerns and obtaining data on prices paid." GAO stated that "OFPP, however, has not yet ensured that agency-specific targets and performance measures for adoption of FSSI and category management solutions are set…[and] [u]ntil OFPP takes action to do so, it is at risk of agencies underutilizing existing FSSI and category management solutions and, in turn, of diminished cost savings."

In its most recent "Goal Action Plan & Progress Update" on the Category Management portion of its Performance Management Agenda, the Administration claimed that

> To date, $301 billion in common spend has been obligated with $136 billion under management (97% of $140 billion goal) and $29 billion going to Best In Class (BIC) solutions (exceeding the goal by $9 billion) generating $9.3 billion in cost avoidance in FY 2018.

OMB further explained that "[b]y the end of FY 2020, the government will achieve $18 billion in savings for taxpayers by applying category management principles or smart decision-making where agencies buy the same kinds of goods and services through best value contract solutions to 60% of common spend."

EU Fines Google "for abusive advertising practices"

The European Union (EU) explained in a press release that the European Commission "fined Google €1.49 billion for breaching EU antitrust rules…[because the company] has abused its market dominance by imposing a number of restrictive clauses in contracts with third-party websites which prevented Google's rivals from placing their search adverts on these websites." The EU stated that "Google's practices amount to an abuse of Google's dominant position in the online search advertising intermediation market by preventing competition on the merits."

The EU explained that it has previously fined Google:

- In June 2017, the Commission fined Google €2.42 billion for abusing its dominance as a search engine by giving an illegal advantage to Google's own comparison shopping service.
- In July 2018, the Commission fined Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen the dominance of Google's search engine.

The EU stated that "[i]t is not possible for competitors in online search advertising such as Microsoft and Yahoo to sell advertising space in Google's own search engine results pages...[and] [t]herefore, third-party websites represent an important entry point for these other suppliers of online search advertising intermediation services to grow their business and try to compete with Google."

The EU stated

> Google's provision of online search advertising intermediation services to the most commercially important publishers took place via agreements that were individually negotiated. The Commission has reviewed hundreds of such agreements in the course of its investigation and found that:
>
> - Starting in 2006, Google included exclusivity clauses in its contracts. This meant that publishers were prohibited from placing any search adverts from competitors on their search results pages. The decision concerns publishers whose agreements with Google required such exclusivity for all their websites.
> - As of March 2009, Google gradually began replacing the exclusivity clauses with so-called "Premium Placement" clauses. These required publishers to reserve the most profitable space on their search results pages for Google's adverts and request a minimum number of Google adverts. As a result, Google's competitors were prevented from placing their search adverts in the most visible and clicked on parts of the websites' search results pages.
> - As of March 2009, Google also included clauses requiring publishers to seek written approval from Google before making changes to the way in which any rival adverts were displayed. This meant that Google could control how attractive, and therefore clicked on, competing search adverts could be.

Further Reading

"Desperate to get through to executives, some cybersecurity vendors are resorting to lies and blackmail" – *CNBC*
"Why Metro is trying to hack into its own railcars" – *WTOP*
"An Android Vulnerability Went Unfixed For Over Five Years" – *Wired*
"Google bans VPN ads in China" – *ZDNet*
"Vietnam 'State-Aligned' Hackers Are Targeting Auto Firms, FireEye Says" – *Bloomberg*
"Leaker, Liar, Hacker, Hoaxer: The Russian contractor who infiltrated Anonymous" – *Emma Best*
"Domestic abusers 'sewing GPS trackers into teddy bears'" – *BBC*
"A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments" – *The New York Times*
"Finland to investigate Nokia-branded phones after data breach report" – *Reuters*
"Security flaw in Medtronic heart defibrillators is serious, DHS says, but don't panic" – *cyberscoop*