10th Annual Carahsoft Budget and IT/Cyber Policy Update

Robert G. Efrus
Founder and CEO
Efrus Federal Advisors LLC

December 13, 2019

Overview

Fiscal 2020 Budget/Continuing Resolution Update

Federal IT Legislative Update

Fiscal 2020 IT/Cyber/AI Spending Outlook

IT/Cyber Policy Trends

2020 Sales Plays

Tech Lobbying Update

Summary

Fiscal 2020 Appropriations Update

Status

House has approved 10 of 12 spending bills

(all but Homeland and Leg. Branch)

Senate has approved 4 of 12 spending bills

(USDA, CJS, THUD, Interior/EPA)

Bipartisan Budget Act of 2019—Set Fiscal 2020-2021 Discretionary Spending Caps (July, 2019)

	2019	2020	2021
Defense	$716B	$738B	$740.5B
Civilian	$620B	$632B	$634.5B

The BBA increased discretionary spending by $320 Billion over two years as compared with the levels set by Balance Budget Act of 2011

Fiscal 2019 Appropriations Update

Entire government has been operating under a Continuing Resolution since October 1st

The second CR expires on December 20th

Sixteenth year since 2001 that Congress has required CR's to keep the government running

Best case: Hill passage of several less controversial Fiscal 2020 spending bills by December 20th with the remaining spending bills requiring a third CR that will run until at least mid-February.

Worst Case: Third CR for all twelve Fiscal 2020 spending bills that will run until at least mid-February.

A government shutdown on or about December 20th is still a possibility especially if President Trump throws down the gauntlet if Congress refuses to approve any funding for the President's Wall.

Fiscal 2020 Appropriations Items of Interest

	House	Senate
Defense	JAIC ($166M) Cybercom ($323M)	JAIC ($208M) Cybercom ($348M)
Energy	IDEA Act ($250K) +$10M for SwA in Energy Infras.	IDEA Act ($4M) +$71M for AI
FSGG	TMF ($35M) Election Security ($600M)	TMF ($0) Election Security ($250M)

Fiscal 2020 Appropriations Items of Interest

		House	Senate
DHS	Total Cyber	$927M	$1B
	CDM	$272M (+$135M) +$17M for CDM Dashboard +$3M for Endpoint Protection +$3.6M for agency CDM +$14M for mobile device protection	$137.6M
Labor-HHS		Find commercial solutions that can enable data interoperability between HHS and DHS +$37M for HHS IT Modernization + $45M for SSA IT Modernization	
State		$+310M for IT Modernization	

Fiscal 2020 National Defense Authorization Act

	House	Senate
Cloud	Multi-Cloud	Cloud Migration Policy
JAIC	More reporting	Use commercial solutions
Software	New SW Acq. Pathways	New SW Acq. Pathways
	SW Testing Pilots	
Cyber	Emulate DHS Shared Cyber pgm	
	Support CMMC	
	Consider SCRM during Req’ts definition	

Fiscal 2020 NDAA Conference Report

- DOD CIO Cyber Responsibilities
- Cloud Migration Policy for Applications and Data
- NSA responsibility to evaluate commercial cyber solutions
- Weapons Systems Vulnerabilities
- Software Development
- AI and JAIC Reporting
- Space Force

  The Senate recedes with an amendment that would enact the United States Space Force Act. The amendment would modify title 10, United States Code, to establish the United States Space Force as an Armed Force within the Department of the Air Force.

Pending Federal IT/Cyber-related Legislation

Federal Risk and Authorization Management Program Authorization Act of 2019
https://www.congress.gov/116/bills/hr3941/BILLS-116hr3941ih.pdf

Advancing Cybersecurity Diagnostics and Mitigation Act
https://www.congress.gov/116/bills/hr4237/BILLS-116hr4237ih.pdf

Federal CIO Authorization Act of 2019
https://www.congress.gov/116/bills/hr247/BILLS-116hr247rfs.pdf

AI in Government Act of 2019
https://www.congress.gov/116/bills/hr2575/BILLS-116hr2575ih.pdf

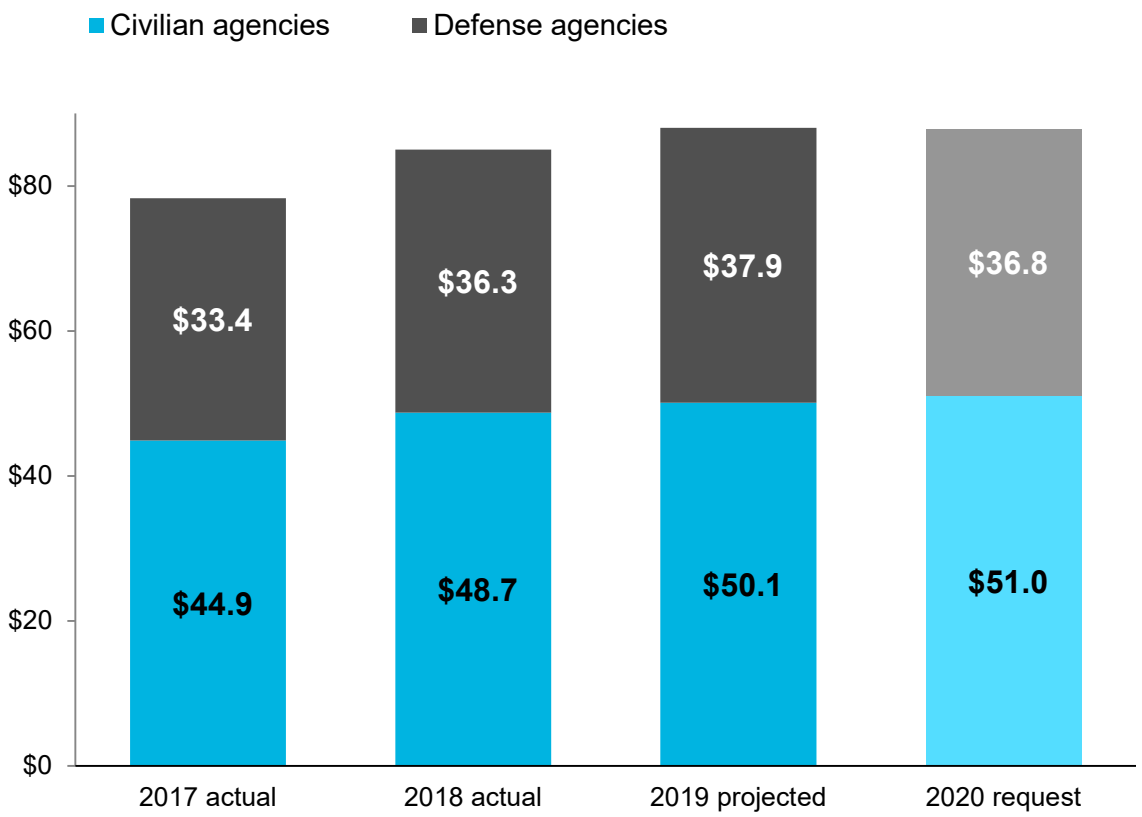
IoT Cybersecurity Improvements Act
https://www.congress.gov/116/bills/s734/BILLS-116s734rs.pdf

Cybersecurity Vulnerability Remediation Act
https://www.congress.gov/116/bills/hr3710/BILLS-116hr3710rfs.pdf

Fiscal 2020 IT Budget Topline

White House proposes $87.8 billion in unclassified IT budget authority

Unclassified IT budget request by fiscal year; dollars in billions



Notes: Figures do not include classified IT spending by defense and intelligence agencies.

Sources: Fiscal 2019 and 2020 Budget Request, Analytical Perspectives: Information Technology; BGOV Cyber, Tech Upgrades, R&D Dominate FY 2020 IT Budget Request

Administration's top priorities:

- Technology Modernization Fund
- Cloud adoption
- Improving the IT and cybersecurity workforce
- Reducing cybersecurity risks
- IT talent management

Sizeable jump in civilian IT spending between fiscal 2017 and 2018

Budget request would shrink Pentagon unclassified IT budget

BGOV Cloud Spending Analysis

BGOV projects that civilian agencies will obligate $4.3 billion on cloud services in FY 2020, while defense agencies are projected to obligate $1.7 billion.

Agencies will invest a combined $3.2 billion on IaaS/PaaS and $3.3 billion on SaaS in fiscal 2020.

Since fiscal 2015, the Centers for Medicare and Medicaid Services, the Department of Veterans Affairs, and the U.S. Air Force have been the top spenders on cloud computing.

Perspecta Inc. has been the top recipient of IaaS/PaaS contract spending since fiscal 2015, while Carahsoft Technology Corp. has generated the most SaaS obligations.

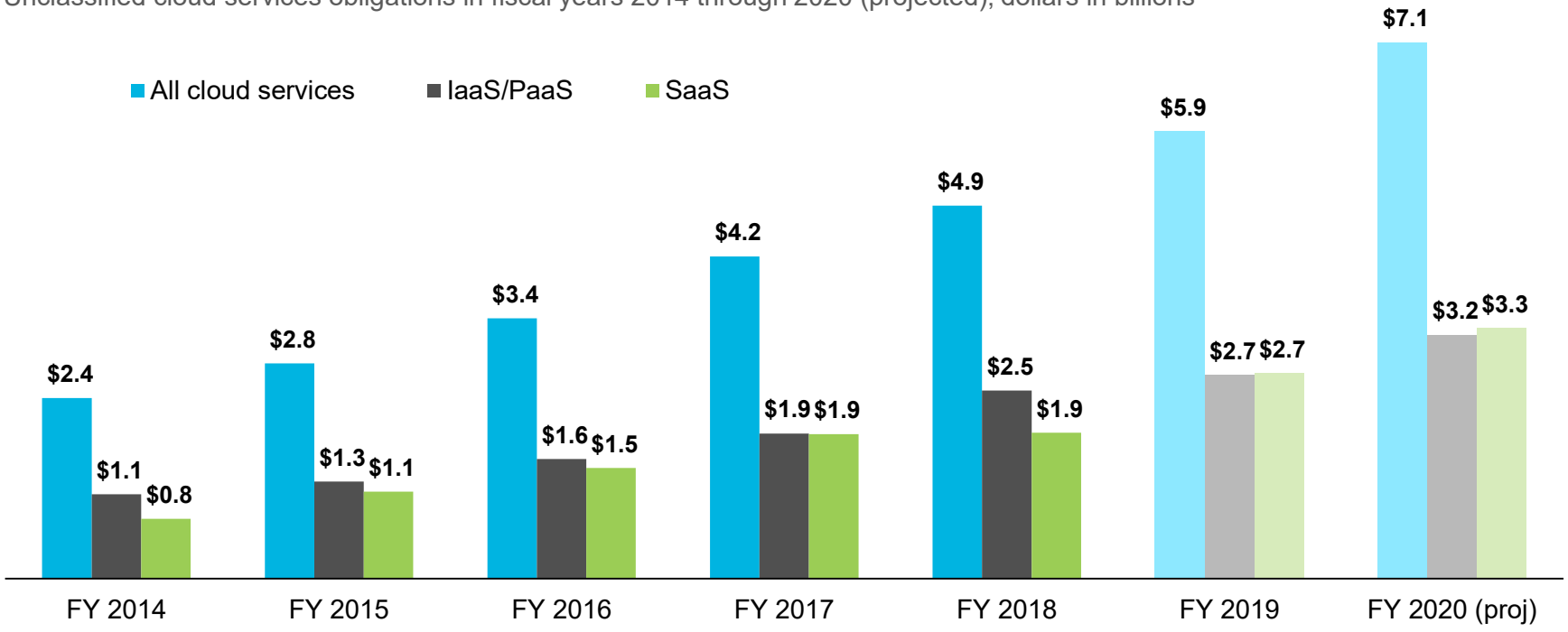
Federal cloud-adjacent spending on digital services will reach $5.2 billion in fiscal 2020, while contracting spending on artificial intelligence and machine learning will reach $1.6 billion.

Federal Cloud Contract Spending

The federal cloud market will reach $7.1 billion by FY 2020

Cloud spending is expected to accelerate as agencies prioritize modernizing aging infrastructure, reforms streamline the security authorization process, and software vendors shift to an as-a-service model

Unclassified cloud services obligations in fiscal years 2014 through 2020 (projected); dollars in billions



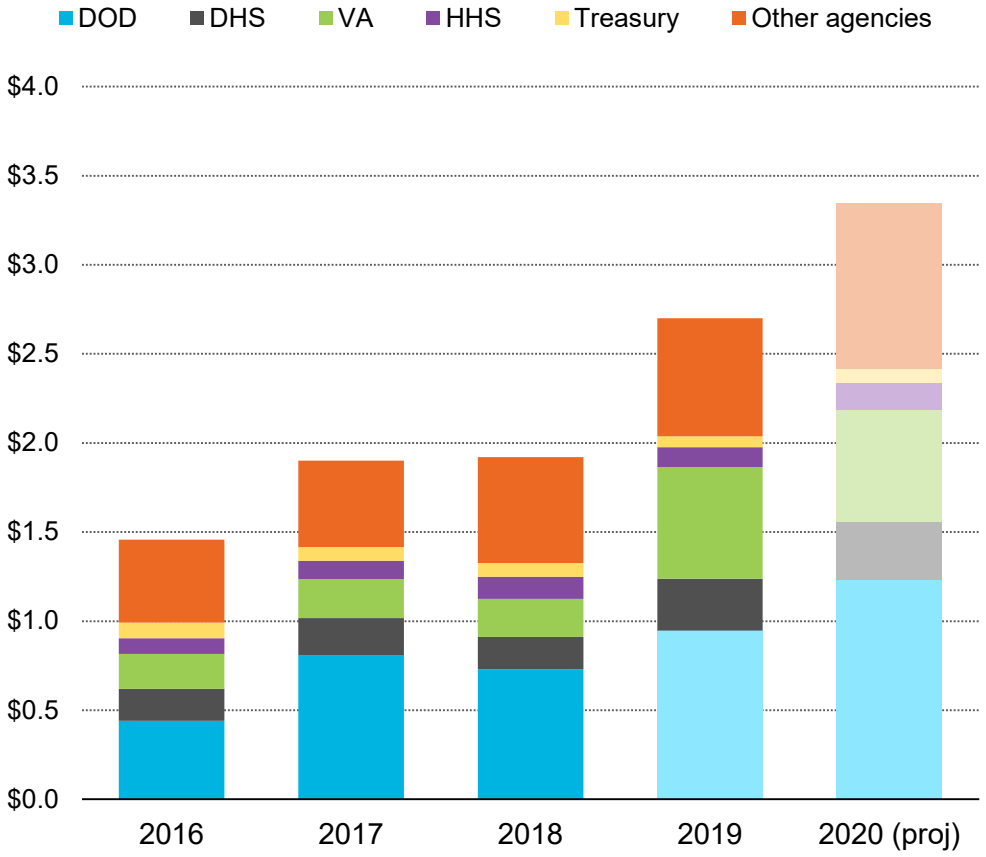
Note: Cloud Services, IaaS/PaaS, and SaaS are BGOV analyst-defined markets. Data for FY 2019 and 2020 are incomplete due to the Pentagon's 90-day reporting lag. BGOV used a five-year CAGR to project spending.

Sources: Bloomberg Government data

Spending on Software as a Service

SaaS spending to reach $3.3 billion; SEWP is the top contracting vehicle

Unclassified SaaS obligations in fiscal years 2016 through 2020 (projected); dollars in billions



Sources: Bloomberg Government data

SEWP V was the largest SaaS contract in FY 2019, generating $1.1 billion in SaaS obligations

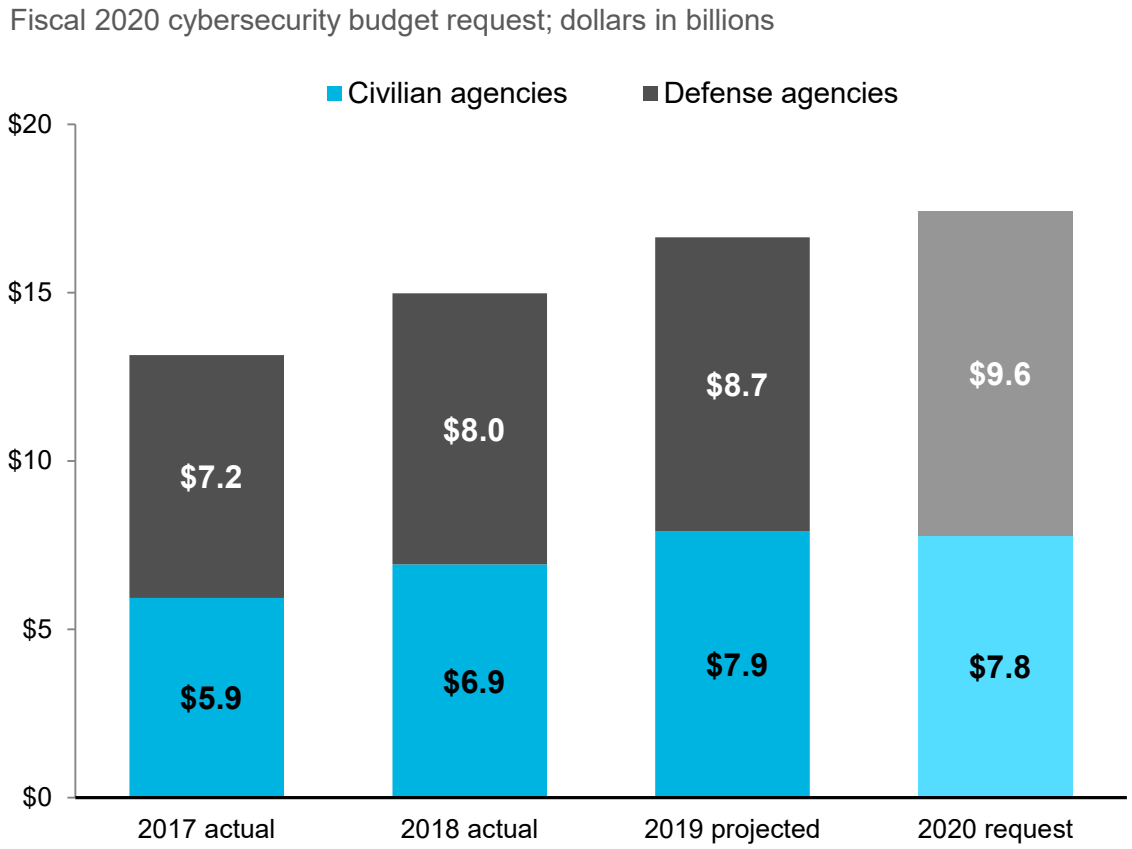
The largest recipients of SaaS obligations in FY 2019 were Dell Inc. ($412 million), Carahsoft Technology Corp. ($358 million), and V3Gate LLC ($195 million)

The largest recipients of SaaS obligations are resellers/distributors of commercial software, including products from Microsoft, Oracle, SAP, and Salesforce

Palantir Technologies generated over $80 million in SaaS obligations from the DOD, DOJ, and SEC

Fiscal 2020 Cybersecurity Budget

White House proposes $17.4 billion in unclassified cybersecurity funding



Pentagon would receive $800 million cybersecurity funding bump compared with fiscal 2019

Top civilian agency recipients of cybersecurity funding:

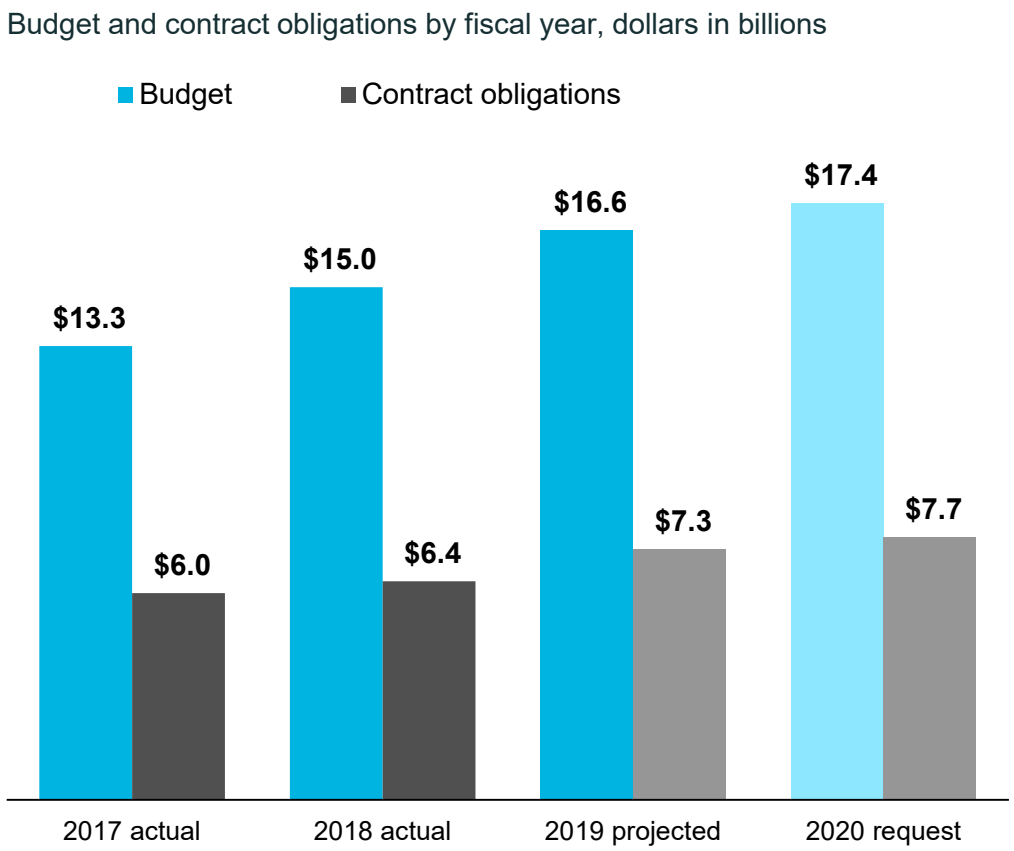
- NPPD ($1.0 billion)
- FBI ($732 million)
- IRS ($349 million)
- National Nuclear Security Administration ($216 million)
- NIST ($104 million)
- Office of Federal Student Aid ($103 million)

Notes: Figures do not include classified IT spending by defense and intelligence agencies. NPPD – National Protection and Programs Directorate; FBI – Federal Bureau of Investigation; IRS – Internal Revenue Service; NIST – National Institute of Science and Technology

Sources: Fiscal 2019 and 2020 Budget Request, Analytical Perspectives: Cybersecurity

Cybersecurity Contracting Projection

BGOV estimates billions in cyber contract obligations in fiscals 2019 and 2020



Contractors are likely to see increased cyber contract obligations in fiscal 2019 and 2020 with increased budget

An average of 44 percent of the cybersecurity budget in fiscal 2017 and 2018 went to contract obligations

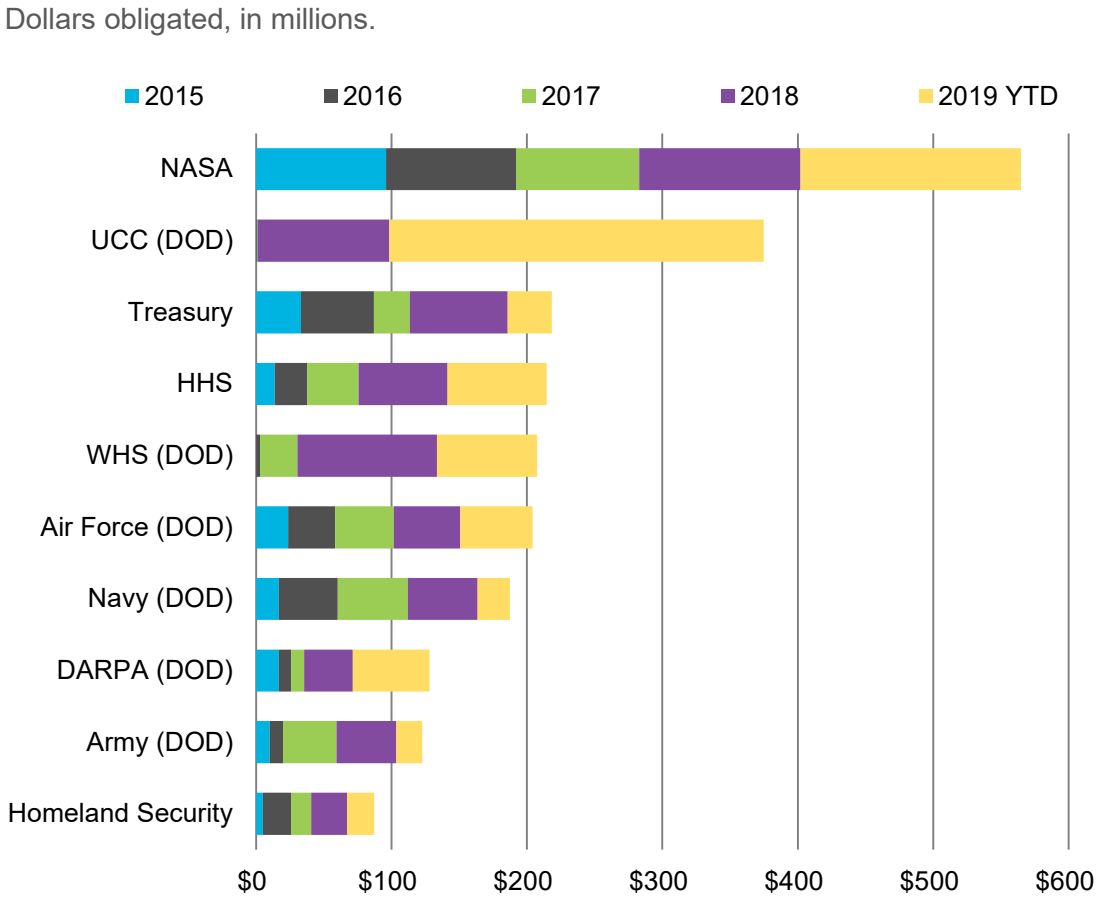
BGOV expects at least an additional $5.1 billion to be spent on cybersecurity in fiscal 2019 and $7.7 billion in fiscal 2020

Note: Darker contract obligations are actuals and lighter bars are estimates

Source: Bloomberg Government data

A.I. Contract Spending by Agency

Spending obligations since fiscal 2015 total nearly $2.7 billion



NASA, Unified Combatant Command, and Treasury account for the majority of AI spending obligations since fiscal 2015

Efforts at NASA include basic R&D at Jet Propulsion Laboratory which stood up a division known as the Artificial Intelligence Group

Much of UCC spending is concentrated in SOCOM which is developing decision making processes around AI

UCC – Unified Combatant Command, HHS – Health and Human Services, WHS – Washington Headquarters Service, DARPA – Defense Advanced Research Projects Agency;

Supply Chain Risk Management

Federal Acquisition Supply Chain Security Act of 2018

Federal Acquisition Security Council

Executive Order on Securing the Information and Communications Technology and Services Supply Chain (5/19)

The rules establish a framework for the Secretary of Commerce to assess ICT product and services (ICTS) transactions that pose an undue risk to critical infrastructure or national security. Transactions are described as activities involving the acquisition, importation, transfer, installation, dealing in, or use of ICTS. A transaction that meets the following conditions will be subject to review by the Secretary and may require ***mitigation, prohibition, or an unwinding*** *of the transaction if determined to be prohibited.*

Supply Chain Risk Management

Cyber Security Maturity Model Certification

Remarks by Katie Arrington, DOD CISO

$600B Annually lost on IP Theft

Self attestation not working

CMMC Impact within 300,000 Company DOD Ecosystem

- *80% CMMC Level 1&2*
- *10-15% CMMC Level 3 (70K Companies)*
- *5% CMMC Levels 4&5 (12K Companies)*

CMMC Certifiers will be drawn from FedRAMP 3PAO Community

CMMC compliance will be an allowable cost

CMMC compliance as a go/no go in DOD contract negotiations

CMMC compliance not needed to sell products to DOD

CMMC—Putting Teeth in NIST SP 800-171

Software Assurance

Derived Security Requirements 3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. 3.11.3 Remediate vulnerabilities in accordance with risk assessments

Data Security

3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

Federal IT Trends

Software Acquisition Reform

DOD's Ellen Lord rewriting the rules pertaining to software acquisition to "enable contracting at the speed of relevance."

Category Management

"The category management cross-agency priority goal team is keeping the government on track to achieve $36 billion in savings by the end of FY 2020 by helping agencies reduce duplicative contracts and leverage the government's huge buying power. The team recently released several tools, trainings, and dashboards to help agencies implement category management strategies."

Federal IT Trends

DevSecOps/Open Source Open Source Software

DevSecOps is a tech industry term for the front-end and continuous integration of development, security and operations teams in the building of software (FedScoop)

In DevSecOps, testing and security are shifted to the left through automated unit, functional, integration, and security testing - this is a key DevSecOps differentiator since security and functional capabilities are tested and built simultaneously.

Cloud native computing uses an open source software stack to deploy applications as microservices, packaging each part into its own container, and dynamically orchestrating those containers to optimize resource utilization. Cloud native technologies enable software developers to build great products faster." (DoD Enterprise DevSecOps Reference Design 8/19)

"Everything we do is open source," he said. "The entire code and the entire infrastructure as code is open to the public." Nicolas Chaillan, Special Advisor for Cloud Security and DevSecOps

Federal IT Trends

Legacy Modernization/Cloud Migration

GAO identified a number risk factors of government mainframe systems include outdated programming languages, unsupported hardware and software by vendors, operating with known security vulnerabilities, and shortages of qualified staff (GAO-19-471).

Legacy system modernization is not a new challenge and several alternative approaches have been tried and tested up to this point, but with highly variable degrees of success. In fact, industry analyst Gartner Inc. defined five legacy modernization alternatives back in 2011; replace, rewrite, rehost, retain, and retire respectively.

The five examples that GAO selected of successful information technology (IT) modernization initiatives included transforming legacy code into a more modern programming language and moving legacy software to the cloud. Doing so allowed the agencies to reportedly leverage IT to successfully address their missions and achieve a wide range of benefits, including cost savings.

Federal IT Trends

Cloud Smart and Multi-Cloud

Industries that are leading in technology innovation have also demonstrated that hybrid and multi-cloud environments can be effective and efficient for managing workloads. As a result, the Cloud Smart Strategy encourages agencies to think of cloud as an array of solutions that offer many capabilities and management options to enhance mission and service delivery. (Cloud Smart)

Agencies are increasingly requesting hybrid/multi -cloud solutions

The market for hybrid/multi-cloud management technologies is becoming more mature, while agencies are reluctant to get locked into a single provider. DHS, Treasury, and the CIA are embarking on multibillion dollar cloud migration programs; each requested hybrid/multi-cloud solutions and participation by multiple hyperscale cloud providers (BGOV)

Congress and Multi-Cloud

Therefore, the Committee directs that no funds may be obligated or expended to migrate data and applications to the JEDI cloud until the Chief Information Officer of the Department of Defense provides a report to the congressional defense committees on how the Department plans to eventually transition to a multi-cloud environment, as described in its January 2019 Cloud Initiative Re-port to Congress. (HAC-D Report 116-84)

FITARA Update

12/11/19 FITARA 9.0 House O&R/Gov Ops Hearing

Updated OMB Data Center Optimization Metrics creating Hill concerns that the Trump Administration is slow rolling data center consolidation

IDEA Act progress cited by NASA and DHS CIO's

Scorecard tracking agency progress on Megabyte Act, Modernizing Government Technology Act and FISMA

Statute and Policy-Driven Sales Plays

Software Security

Section 932 of Fiscal 2013 National Defense Authorization Act
Draft 2019 OMB Memo: Improving Vulnerability Identification, Management, and Remediation
DHS' Binding Operational Directive (BOD) 19-02 (https://cyber.dhs.gov/bod/19-02/)

Software Asset Management

Megabyte Act and Federal IT Acquisition Reform Act

Digital Services (web-based forms, web-based applications)

The 21st Century Integrated Digital Experience Act/Agency reports due 12/20/19:

A list of the websites and digital services maintained by the executive agency that are most viewed or utilized by the public or are otherwise important for public engagement; a prioritization of websites and digital services that require modernization to meet the requirements under subsection and an estimate of the cost and schedule of modernizing the websites and digital services

Cyber Solutions (Sell To)

12,000 DOD Vendors with CMMC Levels 4-5 Status

2019 Lobbying Expenditures (as of 9/30/19)

Firm	Lobbying Spend 2019	2018
Alphabet	$9.7M	$16.7M
Amazon	$12.3M	$10.6M
Facebook	$12.2M	$9.8M
Microsoft	$7.8M	$7.2M
Oracle	$5.9M	$5.4M
IBM	$5.3M	$4M
Dell	$4.8M	$2.8M

Summary

Fiscal 2020 Appropriations End Game

Cyber and Tech Modernization continue to drive IT spending priorities

Cloud spending continues to rise on a year over year basis with expenditures on SaaS soon to eclipse overall USG spending on software acquisition

Supply Chain Risk Management laws and policies will directly or indirectly impact all companies doing business with DOD and civilian agencies

Software acquisition reform in general and DevSecOps in particular will transform how the government buys and uses software

Look for more value added from Carahsoft on creating sales plays that leverage relevant laws, polices and directives

Thanks for your time…

Robert G. Efrus

Founder and CEO

Efrus Federal Advisors LLC

rge@efrusfederal.com

703.307.3156