GovWin
from Deltek

Federal Cloud Computing Market, 2021-2023

Copyright Statement

Published by:

Deltek

2291 Wood Oak Drive

Herndon, VA 20171

About This Report

Deltek's Federal Cloud Computing Market, 2021-2023 report examines key trends shaping the federal cloud computing market.

The report provides:

» Insight into the factors, policies and strategies shaping the cloud market.

» Analysis of the dynamics influencing agency spending on cloud computing.

» Identification of opportunities for cloud business development.

» Spending profiles and forecasts for the top 18 agencies using cloud computing solutions.

» Recommendations to help contractors evaluate the impact of market trends on their business.

Report Deliverables

» 127 Slide PowerPoint® Report

» 37 Slide PowerPoint® Executive Summary

» Excel® Workbook

GovWin *Federal Market Analysis*
from Deltek

Full Report
Table of Contents

To purchase the full report visit GovWin.com

Understanding and Using Deltek's Cloud Data

Obligations (Spending)	Total Awarded Contract Value (TCV)

Obligations (Spending)

» Deltek collects the previous 3 fiscal years of federal spending data using the numbers of contracts awarded for efforts we have verified as cloud work. Verification is done by reading the relevant documentation, through independent research and/or keyword searches for verified cloud solutions (e.g., Microsoft 365).

» Large IT support and data center management contracts with specific cloud Contract Line Item Numbers (CLINs) are included **only** when specific task or delivery orders for cloud-related work can be confirmed.

» **Past obligations are an indicator of trends already in place.** They verify the strength and evolution of the market that Deltek uses as a data point in developing its cloud market forecast.

Total Awarded Contract Value (TCV)

» Deltek collects contract value data upon award and organizes it by federal fiscal year, including quarter awarded.

» TCV provides the ceiling value of contracts awarded in any given fiscal year for cloud work. It is not the same as cloud obligations (i.e., spending) because a contract may never reach its ceiling value before re-competition or completion of the work.

» The data may or may not include contract numbers based on the information source. Some awards are only announced in media releases, meaning some specific data like the exact date of award could be missing.

» **TCV may indicate potential spending to come.** Spikes in TCV suggest increased spending in the following fiscal years since a contract is in place. Deltek uses TCV as a data point in developing its cloud market forecast.

To purchase the full report visit GovWin.com

Key Findings

» Identifiable federal spending on cloud reached a new high of $8B in FY 2020, but the rate of growth slowed compared to previous years due to disruption caused by the COVID-19 public health crisis.

» The move to full-time telework did not cause an exceptionally high spike in cloud spending due to the fact that many agencies had already invested in network infrastructure and collaboration capabilities.

» Cloud activity at highly-federated civilian agencies remains concentrated in components that are heavy users while other components have hardly any use at all.

» The Military Departments (MILDEPs) are all taking a centralized approach to cloud adoption by leveraging a small number of enterprise commercial IaaS and PaaS providers. This development has created a de facto dual-cloud ecosystem independent of the Joint Enterprise Defense Infrastructure (JEDI).

» Agencies are spending more on community/public cloud than on any other deployment model.

» Spending on IaaS is slowing across all of government due to the dominance of a small number of large commercial providers. Investment in SaaS and PaaS is picking up speed.

» Agencies continue to favor FedRAMP Moderate solutions above all others.

» Customers in both the Defense and Civilian sectors prefer using Government-Wide Acquisition Contracts (GWACs) and GSA's Multiple-Award Schedule (MAS) to acquire cloud services more than any other procurement method.

» Agencies with science missions still struggle to leverage cloud for federal R&D.

Total IT Budget Request*

$95.7B

FY 2022 vs. 2021*

+0.9%

Defense*

$37.3B

(-1.2%)?

Civilian*

$58.4B

(+2.4%)

*Excludes S&L grants and classified programs.

FY 2022 IT Budget Overview

» The total FY 2022 IT budget request for civilian agencies is $58.4B, up from $57.1B enacted for FY 2021.

» Funds 4,531 investments at 25 civilian agencies, 546 of which are considered major IT investments.

» Focuses on *securing data and systems, delivering citizen services* and furthering the vision of *digital government*. The IT budget promotes:

  » Reducing cybersecurity risk.
  » Laws to enable technology planning, oversight, funding, and accountability.
  » Strategic use of IT to enable missions.
  » Modernizing legacy systems.
  » Migrating to commercial cloud solutions and shared services.
  » Recruiting, retaining, and reskilling the federal technology workforce.

*Notes on the data

» *Defense: DOD's FY 2022 IT budget was not publicly available at the time of publishing of this report. This figure represents DOD's FY 2022 unclassified IT budget estimate from its FY 2021 request.*

» *Civilian: The figure reported in the "Information Technology and Cybersecurity Funding" chapter of the Analytical Perspectives budget document ($58.4B) DOES NOT align with the total of $57.4B reported in the IT Portfolio Summary.*

FY 2022 IT Budget Request By Department

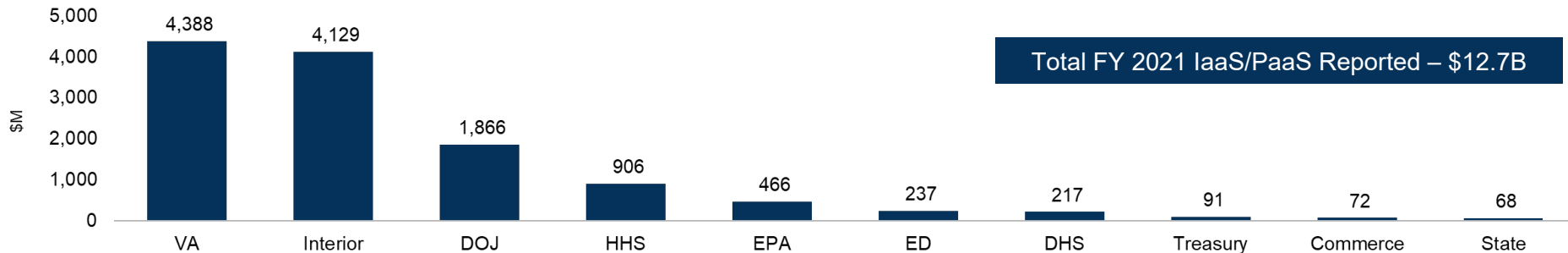| $M	2020 Actual	FY 2021 Estimate	FY 2022 Request	%Change FY 2021-22
Defense*	36,597	37,719	37,274	-1.2%
Defense Agencies	10,280	10,614	10,646	0.3%
Army	12,068	12,342	12,192	-1.2%
Navy	8,366	9,260	9,084	-1.9%
Air Force	5,883	5,503	5,352	-2.7%
VA	7,204	9,102	8,495	-6.7%
DHS	7,567	7,423	8,150	9.8%
HHS	6,916	6,955	6,956	0.0%
TREAS	4,936	5,363	5,916	10.3%
DOJ	3,388	3,328	3,471	4.3%
DOT	3,057	3,082	3,413	10.7%
STATE/USAID	2,886	2,813	3,019	7.3%
DOC	4,012	2,827	2,596	-8.1%
USDA	2,588	2,705	2,749	1.6%
DOE	2,360	2,460	2,564	4.2%
NASA	2,381	2,229	2,145	-3.8%
SSA	2,395	1,991	2,157	8.4%
DOI	1,379	1,474	1,502	1.9%
EDUC	843	1,026	982	-4.3%
Other	3,210	3,300	3,264	-1.1%

Source: OMB, Deltek

Excludes S&L grants and classified budgets.

OMB-Reported Federal Cloud Investment, FY 2021*

Top 10 Agencies by Reported IaaS/PaaS Budgets, FY 2021

$M

Agency	Value
VA	4,388
Interior	4,129
DOJ	1,866
HHS	906
EPA	466
ED	237
DHS	217
Treasury	91
Commerce	72
State	68

Total FY 2021 IaaS/PaaS Reported – $12.7B

Top 10 Agencies by Reported SaaS Budgets, FY 2021

$M

Agency	Value
DOE	428
Interior	395
VA	261
ED	196
DHS	121
HHS	116
State	78
USDA	73
GSA	42
Commerce	32

Total FY 2021 SaaS Reported – $1.7B
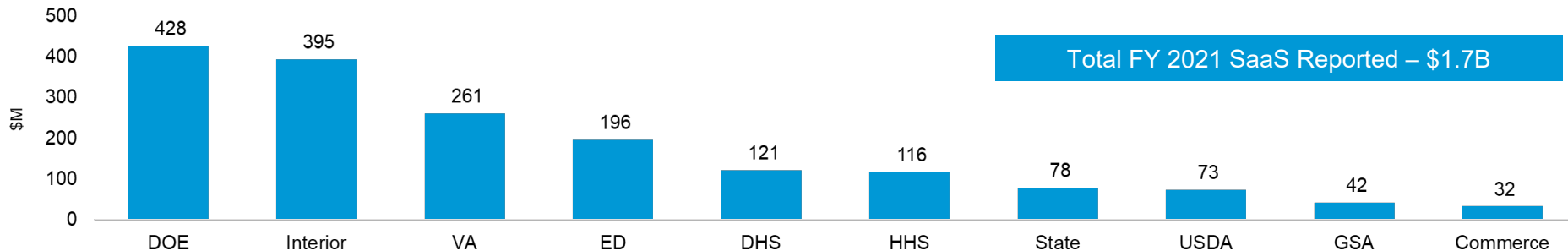
OMB guidance requires civilian agencies to report their cloud investments for the previous fiscal year in each year's IT budget request. Platform-as-a-Service and Infrastructure-as-a-Service investments are reported together. Software-as-a-Service is reported separately. Agencies reported this data for FY 2021 in their FY 2022 budget requests. DOD data is not included. *Source: OMB*

Cloud Smart Progress Update

The Cloud Smart strategy issued by the Federal Chief Information Officer in June 2019 listed 22 action items to be completed before December 2020. These items are divided into four topic areas: General, Security, Procurement and Workforce. As of this writing, five action items in three topic areas are still in progress.

Security

» Action 4 – Update Trusted Internet Connection Policy to ensure objectives can be achieved. Policy goals will be updated using security architectures that are scalable and allow for the efficient use of cloud.

Procurement

» Action 13 – Task the Cloud Solutions Category Team (CSCT) with evaluating the best Government-Wide Acquisition Contract (GWAC) vehicles best to use for cloud services acquisitions.
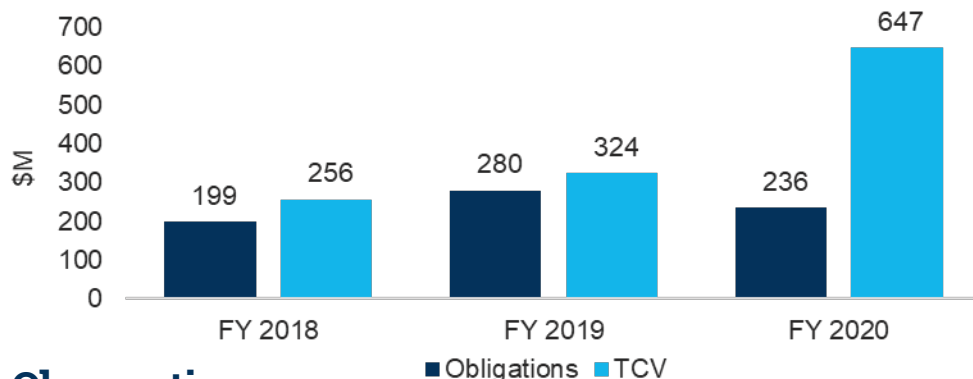
Workforce

» Action 19 – Conduct acquisition workforce competency survey to identify skill and talent gaps.

» Action 21 – Collect employee communication, engagement and transition best practices for ensuring successful cloud migration efforts.

» Action 22 – Develop market-informed pay and compensation strategy for new employees.

Market Implications
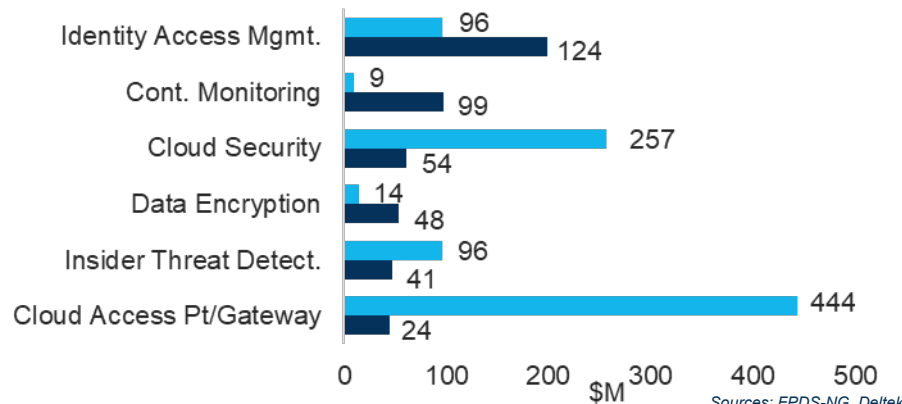
» Even the partial implementation of Cloud Smart is credited with accelerating cloud adoption across civilian agencies.

» Full implementation of Cloud Smart will result in a list of GSA-recommended GWACs that agencies should use for cloud procurement.

» Workforce training should ensure government contracting personnel become smarter about purchasing cloud services.

Use of Cloud-Based Cybersecurity Solutions, FY 2018-2020

**Total Cloud-Based Cybersecurity Solutions, FY 2018-2020**

- FY 2018: Obligations 199, TCV 256
- FY 2019: Obligations 280, TCV 324
- FY 2020: Obligations 236, TCV 647

■ Obligations ■ TCV

Cyber Solutions by Type, FY 2018-2020

Type	TCV	Obligations
Identity Access Mgmt.	96	124
Cont. Monitoring	9	99
Cloud Security	257	54
Data Encryption	14	48
Insider Threat Detect.	96	41
Cloud Access Pt/Gateway	444	24

Observations

» Federal spending on cloud-based cybersecurity solutions fell for the first time in FY 2020. The decline tracks with a general fall-off in spending likely caused by the shift to full-time telework in response to the COVID-19 crisis.

» The surge in contracting for Cloud Access Points (CAPs) reflects expanding use of cloud by federal agencies. Multi-cloud environments require more secure access points. The DOD in particular is seeing exploding demand for CAPs.

» Civilian agencies spent $471M on cloud-based cybersecurity from FY 2018-2020, more than double the DOD's $264M.

» Top spending Civilian agencies: SSA ($105M), DHS ($98M), Commerce ($48M), DOJ ($43M) and HHS ($42M).

» Top spending Defense organizations: DISA ($123M), Air Force ($46M), Army ($22M) and Navy ($22M).

» Top 3 commercial cloud-cyber solutions by spending: Forcepoint ($66M), Virtru ($46M) and EnTrust ($32M).

FedRAMP Adoption Trends

Contracted Solutions by FedRAMP Compliance Level, FY 2018-2020

Compliance Level	# of Contracted Solutions
Moderate	1,688
Low	1,205
Moderate/High	798
No Detail	698
High	66

# of Contracted Solutions
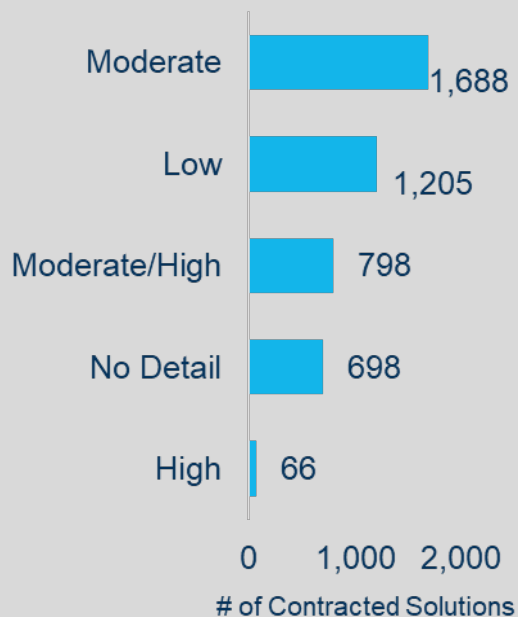
Solutions identified as Moderate/High indicate agency acceptance of proposed solutions at either level (See Notes).

Program Growth. The FedRAMP PMO reported a 50% increase in agencies reusing authorized cloud products in FY 2020. Agencies also made 3,000 requests to evaluate cloud security products already in use.

Container Vulnerability Compliance: Recognizing a risk posed by container technology, the FedRAMP PMO issued rules in March 2021 requiring all cloud solutions to incorporate scanning capabilities that harden container images, per NIST SP 800-70 guidelines.

Civilian Sector Outpaces DOD: Civilian agencies issued contracts for 1,170 instances of FedRAMP-compliant solutions in FY 2020. DOD awarded 434, led by Navy with 122 awards. State led the Civilian space, awarding 213 contracts in FY 2020, followed by HHS (130), DHS (121), Interior (88) and Justice (84).

FedRAMP Low Surges, Moderate Still Leads: Agencies procured a new high of 607 FedRAMP Low solutions in FY 2020, up from 198 in FY 2019. They still preferred FedRAMP Moderate solutions, however, buying 677 in FY 2020 compared to 509 in FY 2019.

FedRAMP at a Glance

218 Authorized Solutions
(+29 in FY 2020 vs. FY 2019)
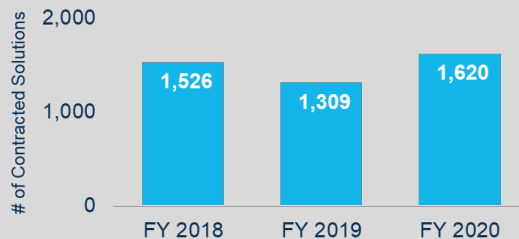
55 Solutions in Process

35 FedRAMP Ready Solutions pending authorization

Total Spending on FedRAMP Authorized Solutions in FY 2020

$4.2B

+$395M vs. FY 2019

Agency Procurement of FedRAMP Compliant Solutions

Fiscal Year	# of Contracted Solutions
FY 2018	1,526
FY 2019	1,309
FY 2020	1,620

Sources: FedRAMP PMO, Deltek

Cybersecurity Executive Order: Cloud Market Impact

On May 12, 2021, the White House published an "Executive Order on Improving the Nation's Cybersecurity" in response to a series of high-profile cyber attacks. The EO suggests regulatory reforms that will have an impact on Cloud Service Providers (CSPs) and the federal cloud market in general. The Cyber EO calls for:

Modifying Contract Language

» Changes will be made to the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS) that *require CSPs to collect and share data on cyber incidents* with their agency customers and federal law enforcement.

Accelerating Cloud Adoption

» Agencies must develop Zero Trust architectures and accelerate the migration of data to secure CSPs.

» By July 12, agencies must develop plans to prioritize the adoption and use of cloud technology.

» *Agencies must ensure that cloud services adopted are compatible with Zero Trust architecture*.

Updating Federal Cloud Security Strategy

» By July 12, the CISA at DHS must produce a cloud service governance framework that identifies services and protections available to agencies based on incident severity.

» By July 12, the FedRAMP PMO must:

  » Establish a training program to ensure agency personnel are equipped to manage FedRAMP requests.

  » Improve communication with CSPs by automating and standardizing messages at each stage of authorization.

  » Automate compliance processes throughout the FedRAMP lifecycle.

  » Digitize and streamline documentation that CSPs are required to complete.

  » Map relevant compliance frameworks to the FedRAMP authorization process and allow those frameworks to substitute for relevant portions of the FedRAMP process where applicable.

Trusted Internet Connections (TIC) 3.0 Update

Following the release of final TIC 3.0 core guidance in July 2020, the Cybersecurity and Infrastructure Security Agency (CISA) at DHS published a series of use cases outlining how agencies can securely connect to commercial cloud services. **Use cases are considered key documents supporting cloud adoption.** Three use cases have been published to date, with another five slated to appear in FY 2022.

Core Guidance *(as of June 2021)*

TIC 3.0 Program Guidebook
Outlines the modernized TIC program.

»**TIC 3.0 Reference Architecture**
»*Defines program concepts to guide security capability implementations.*

TIC 3.0 Security Capabilities Handbook
Indexes security capabilities relevant to TIC.

TIC 3.0 Service Provider Overlay Handbook
Maps service provider security functions to TIC capabilities.

🟢 = Published   ## Use Cases *(as of June 2021)*   🔴 = Not Published

Remote User Use Case
Defines network and multi-boundary security when an agency user can access agency resources in agency-hosted or commercial cloud environments from outside agency network boundaries. 🟢

Traditional TIC Use Case
Defines network security when agency personnel are in a physical location that uses a TIC Access Point, a TIC Access Provider or Managed Trusted Internet Protocol Services (MTIPS) to access the web. 🟢

Branch Office Use Case
Defines network and multi-boundary security when an agency conducts work in more than one physical location, but most of IT services are provided by another branch office rather than the agency campus. 🟢

Planned Use Cases
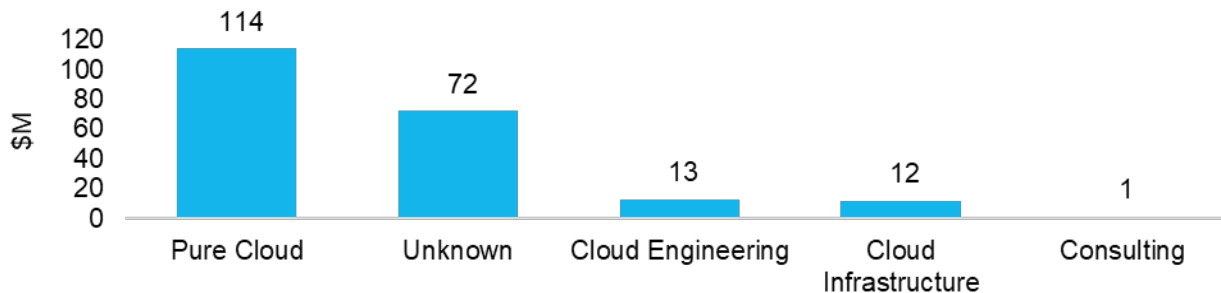Zero Trust, Research and Development, Infrastructure, Software and Platform-as-a-Service. 🔴

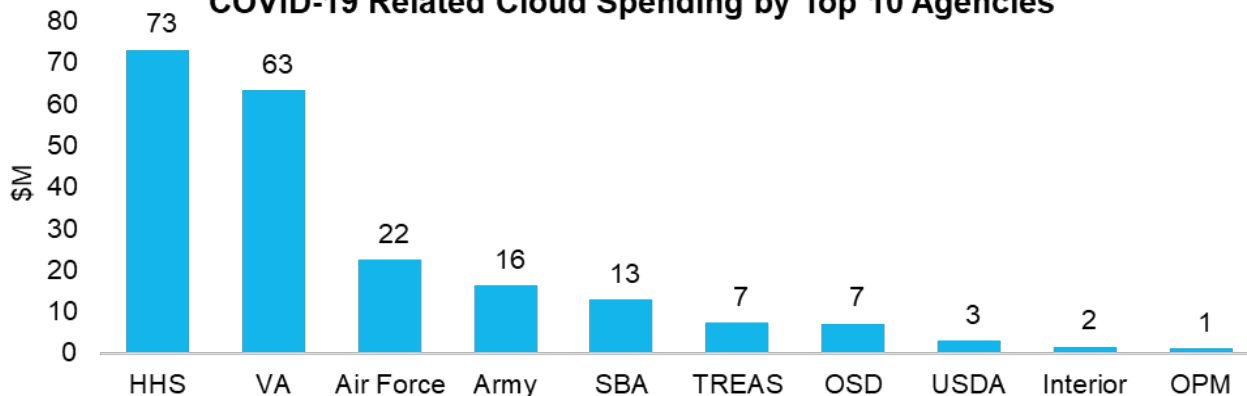# COVID-19 and Federal Cloud Computing Investment

Observations

» Identifiable cloud spending related to COVID-19 totaled $211M.

» Civilian agencies spent $165M. The DOD spent $46M.

» Agencies spent $111M on applications, including $32M on advanced analytics and $29M on email/bundled communications and messaging. They spent another $9M on communications infrastructure.

Bottom Line: Although the COVID-19 crisis forced an unprecedented number of federal employees to telework, it did not cause an exceptionally high spike in cloud spending due to the fact that many agencies had already invested in network infrastructure and collaboration capabilities.

COVID-19 Related Cloud Spending by Market Category

Market Category	$M
Pure Cloud	114
Unknown	72
Cloud Engineering	13
Cloud Infrastructure	12
Consulting	1

COVID-19 Related Cloud Spending by Top 10 Agencies

Agency	$M
HHS	73
VA	63
Air Force	22
Army	16
SBA	13
TREAS	7
OSD	7
USDA	3
Interior	2
OPM	1

Sources: Deltek, FPDS-NG

To purchase the full report visit GovWin.com

Technology Modernization Fund Update

American Rescue Plan Act TMF Funding **$1B** (Avail. until 09/30/25)	» The Modernizing Government Technology Act established a Technology Modernization Fund (TMF) Board for evaluating agency proposals, awarding funding and providing assistance and oversight during project implementation. » Agencies submit Initial Project Proposals (IPPs) in Phase 1 of the TMF funding application. » If the Board approves the IPP, the agency project team submits a Full Project Proposal (FPP) in Phase 2. » Final approved funding allows agencies to compete and award contracts for accepted projects.

TMF Board Project Selection Criteria

» **User Impact:** How the project improves agency mission effectiveness or user/public benefit.

» **Risk Reduction:** The current system deficiencies, record of previous incidents or technology audits that support the case for modernization; modernization of hardware or software that relies on outdated skillsets; and impact of technological dependencies on other systems.

» **Opportunity Enablement:** Potential or known savings, long-term financial impact, criticality of modernization timing, reduction of vendor lock-in, and government-wide added value.

» **Common Solutions:** Reuse, cross-agency collaboration, and shared tool potential.

» **Team Strength:** Previous successes, leadership, technical and subject matter expertise in agency modernization.

» **Project Strategy Strength:** Strength of project and acquisition plans, readiness of project team to execute, and alignment with ongoing modernization strategies.

Technology Modernization Fund Update (Cont)

The administration released updated guidance in May 2021 concerning how it will prioritize the funding of new projects using the TMF account. It produced the guidance to ensure that agency needs are balanced with Congress' intent for providing the additional $1B of TMF funding in the American Rescue Plan. ***The TMF Board will prioritize legacy IT projects that cut across agencies, address immediate security gaps and improve the public's access to government services, such as:***

Modernizing High Priority Systems. Modernize and support priority agency assets and services. May include systems designated as High Value Assets that have significant importance or long-standing security issues, ***such as the 10 systems listed (but not named) on page 15 of GAO's June 2019 report GAO-19-471 (see notes).***

Cybersecurity. Address gaps uncovered in the recent SolarWinds incident. This may include identity, credential and access management, as well as moving toward a Zero Trust architecture.

Public-Facing Digital Services. Creation or modernization of digital services that increase access, reduce fraud and improve service delivery.

Cross-Government Collaboration and Scalable Services. Public- or agency-facing shared services, including technical infrastructure that can offer a scalable, secure foundation for the rapid creation and modernization of digital services.

Repayment Terms. The new guidance offers ***flexible repayment terms***, even including an option where agencies may repay only a portion of the investment.

Market Implications: Boon for cloud vendors! Flexible repayment is designed to increase agency applications for TMF investment, providing more business opportunities, particularly for cloud migration services. High-Value Asset targeting, building out Zero Trust architecture and scalable services should also drive higher spending on cloud.

Schedule Consolidation and Cloud Spending on GSA Schedule 70, FY 2018-2020

GSA's News Multiple Award Schedule Takes Over. After consolidating 24 Multiple Award Schedules (MAS) into a single Schedule for products, services and solutions, cloud spending on the MAS (as defined by use of cloud SIN 132-40) surpassed Schedule 70 starting in FY 2019 and accounted for practically all cloud spending in FY 2020.

Use of Schedule 70 Stops. Following consolidation into the new MAS, cloud spending on GSA's Schedule 70 fell to only $3M in FY 2020.

COVID-19 Slows Cloud Spending in FY 2020. Spending on the new GSA MAS fell in FY 2020, likely due to the disruption caused by the federal government's transition to full-time telework in response to the COVID-19 public health crisis.

Reforming Cloud Pricing. The Coalition for Government Procurement (CGP) is calling on GSA to reform the cloud pricing methodology used by the new MAS. Instead of using the antiquated Price Reduction Clause and Commercial Sales Practices Clause that are currently the basis for MAS price negotiations, the CGP is urging GSA to adopt a flexible model for pricing cloud services per customer use. GSA is evaluating options.

Cloud Spending on SIN 132-40, FY 2018-2020
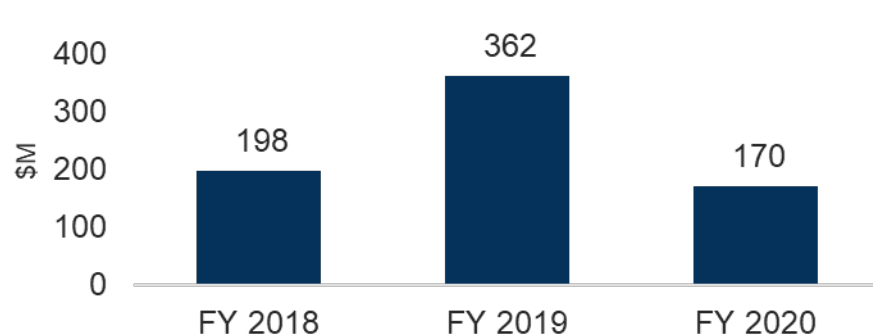
Cloud SIN Spending by GSA Schedule, FY 2018-2020

Source: GSA

To purchase the full report visit GovWin.com
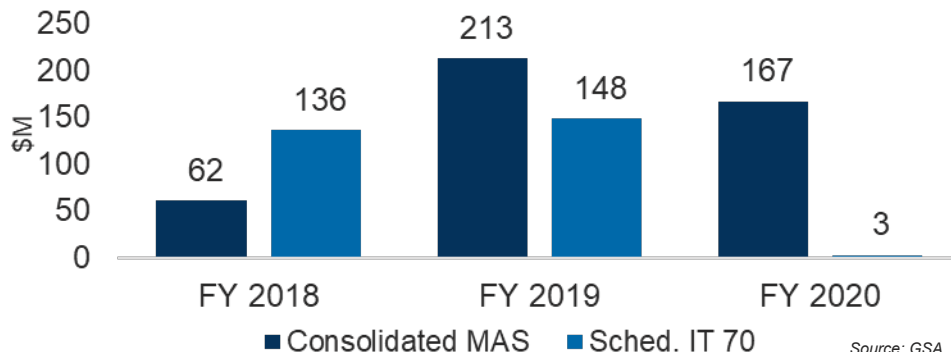
DOD's Use of OTAs for Cloud

Total Spending on Cloud OTAs Fell in FY 2020. After rising to a new high of $383M in FY 2019, spending on cloud OTAs dropped to $315M in FY 2020. The onset of the COVID-19 crisis likely caused the drop in spending, as OTAs are typically for engineering prototypes and the transition to full-time telework kept personnel away from work sites.

» At $169M, the Army led all organizations in cloud-related OTA spending. Army spent $77M on the Enterprise IT-as-a-Service (EITaaS) effort, $48M on the cloud-based Persistent Cyber Training Environment Cyber Innovation Challenge and another $29M on the Army Accessions Information Environment.

» The Air Force spent $90M on cloud-related OTAs, including $36M on the compute and store portion of the EITaaS effort.

Total Value of Cloud-Related OTA Contracts Fell. Similar to spending, the total value of OTAs awarded for cloud prototypes fell to $845M in FY 2020, after reaching a high of $982M in FY 2019.

New OTA Requirements in FY 2020: Despite falling spending and awarded contract values, several new cloud OTA efforts got underway in FY 2020. These include the Air Force's prototyping and production of the MilMove capability ($15M in FY 2020) and the Navy's Maintenance, Repair and Overhaul Solution ($22M in FY 2020). The Army also spent $5M on a new cyber defensive tools kit.
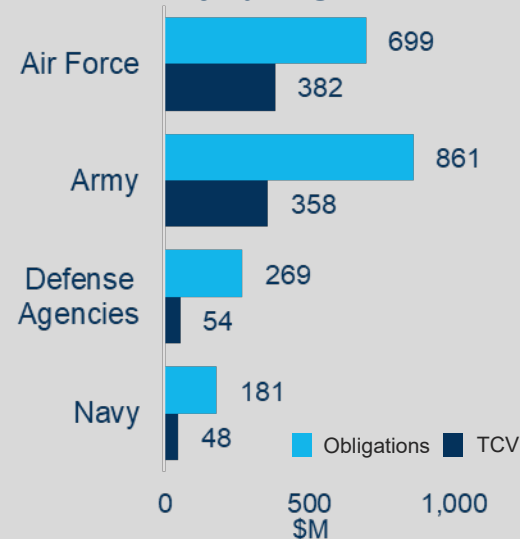
OTA Cloud Procurement at a Glance

$845M in Total Award Value
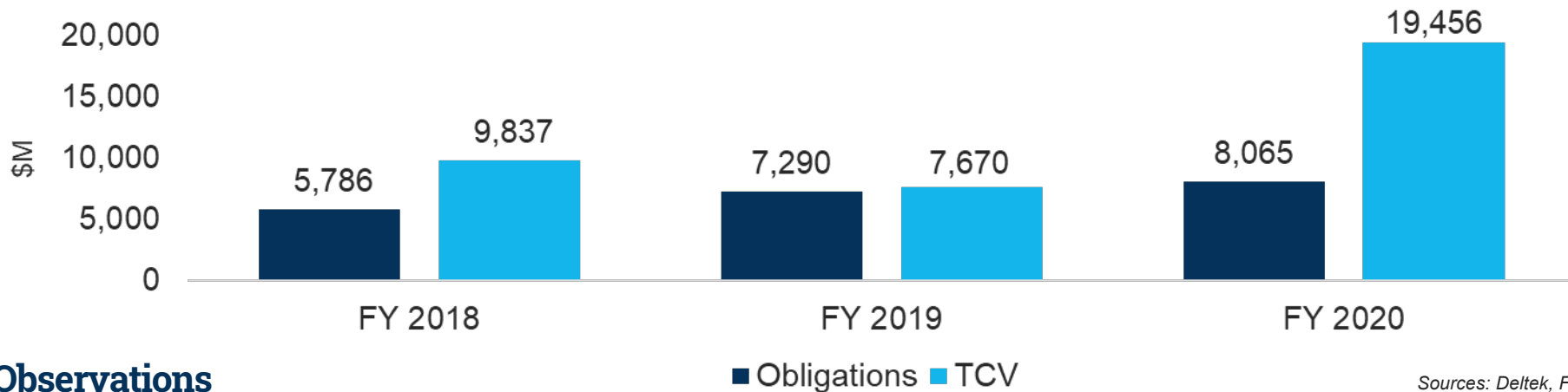
18 Awards in FY 2020

6 Awards by Army

2 Awards by Air Force

2 Awards each by DHA, OSD and DISA

Sources: FPDS, Deltek

To purchase the full report visit GovWin.com

Cloud Computing Obligations and Total Contract Value (TCV), FY 2018-2020
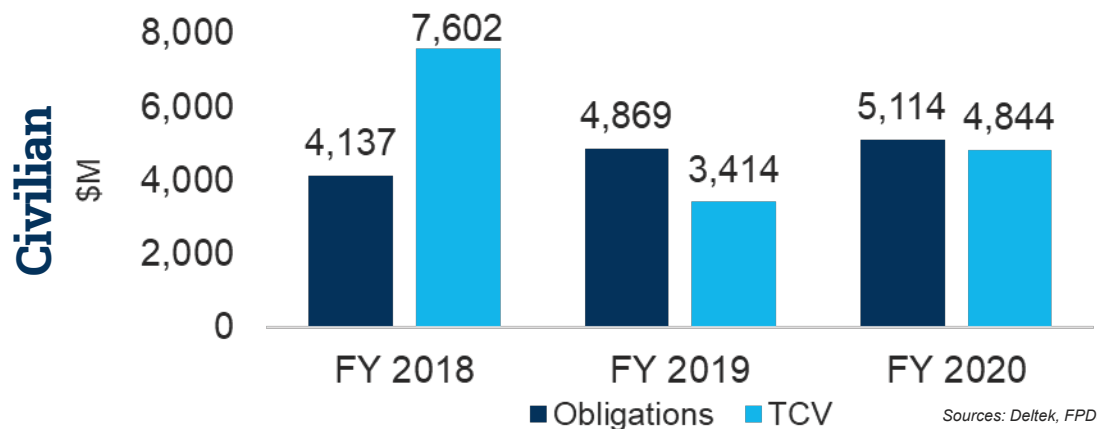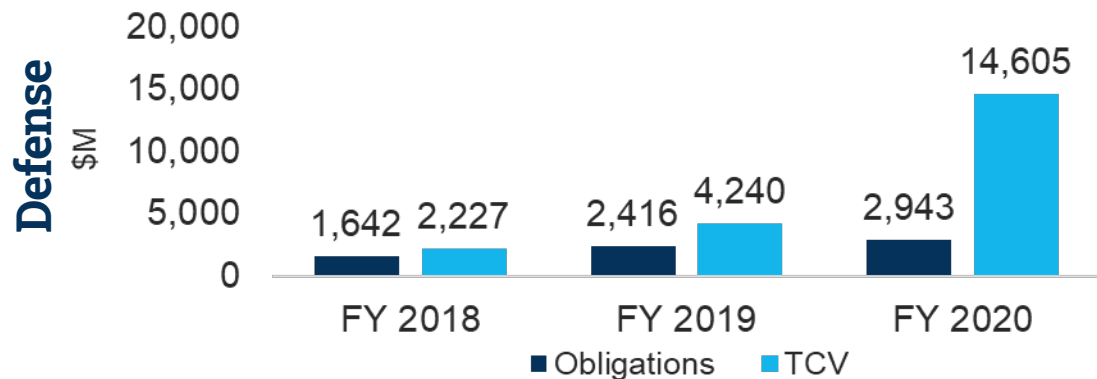

Sources: Deltek, FPDS

Observations

» Verifiable federal cloud spending topped $8B for the first time in FY 2020.

» Federal cloud spending grew by $775M from FY 2019 to 2020, well below the $1.5B increase from FY 2018 to 2019.

» The government's move to full-time telework in response to the COVID-19 public health crisis significantly slowed cloud investments that require on-site work.

» The total value of awarded cloud contracts (TCV) rose to an all-time high FY 2020, adding $1.8B (even when excluding the $10B JEDI award to Microsoft).

» VA, Commerce and HUD reported the largest gains in TCV gains (+$903M, +$731M and +$206M respectively).

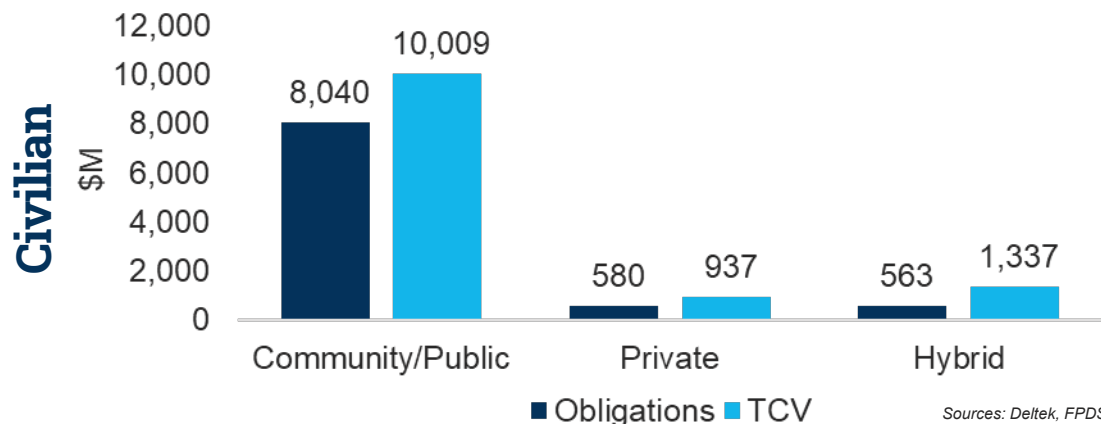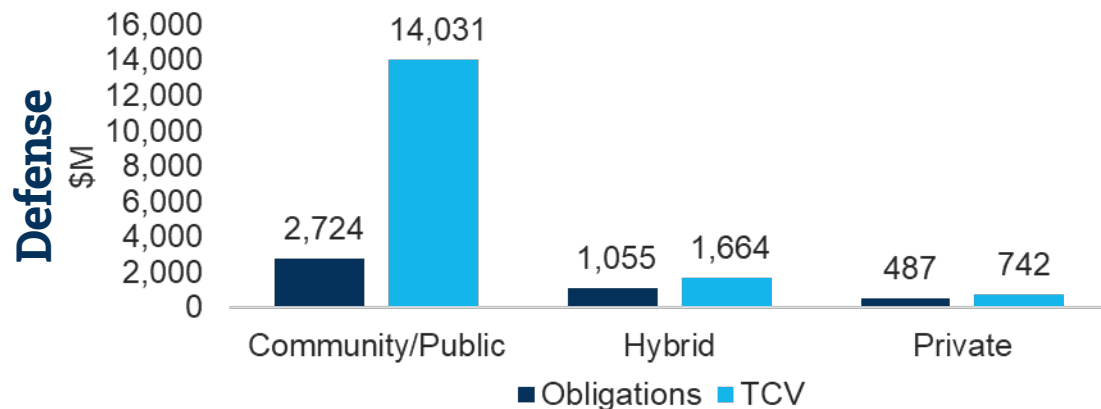» The DOD reported no decline in either cloud spending or TCV from FY 2018 to 2020.

Cloud Obligations and TCV, FY 2018-2020: Buyer Segment

Defense ($M)

	FY 2018	FY 2019	FY 2020
Obligations	1,642	2,416	2,943
TCV	2,227	4,240	14,605

Civilian ($M)

	FY 2018	FY 2019	FY 2020
Obligations	4,137	4,869	5,114
TCV	7,602	3,414	4,844

Sources: Deltek, FPDS

» **Defense** cloud spending slowed from FY 2019 to 2020 due to COVID-19, growing only $527M compared to $774M from FY 2018 to 2019.

» **Cloud TCV grew 8.6%** over the same period (excluding the $10B JEDI award), which was also a significant slow-down compared to the transition from FY 2018 to 2019.

» **Both cloud spending and TCV rose** across the Defense Department.

» **Rising $245M** from FY 2019 to 2020, cloud spending across the Civilian sector also slowed due to the impact of COVID-19.

» **Cloud TCV rose 42%** over the same period, recovering from a dip from FY 2018 to 2019.

» **Cloud spending surpassed TCV** in the Civilian sector for the second year in a row, suggesting that agencies are leveraging contracts they have already put into place (particularly for IaaS).
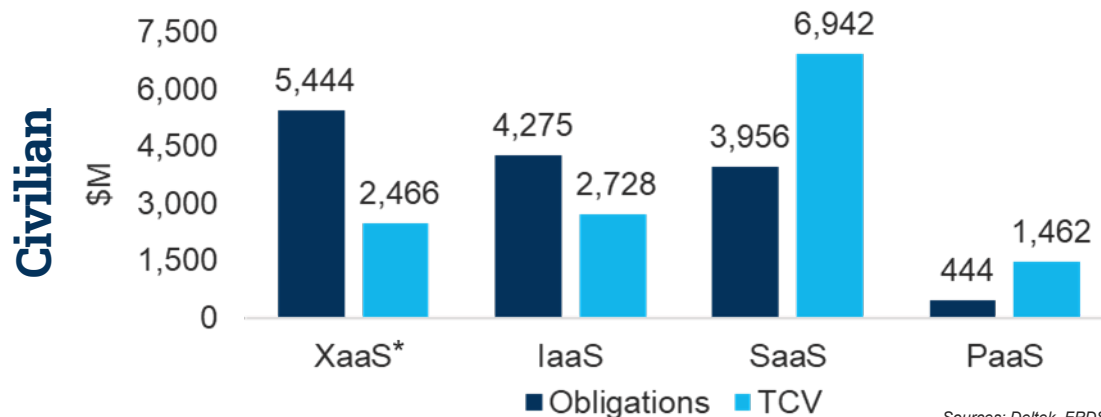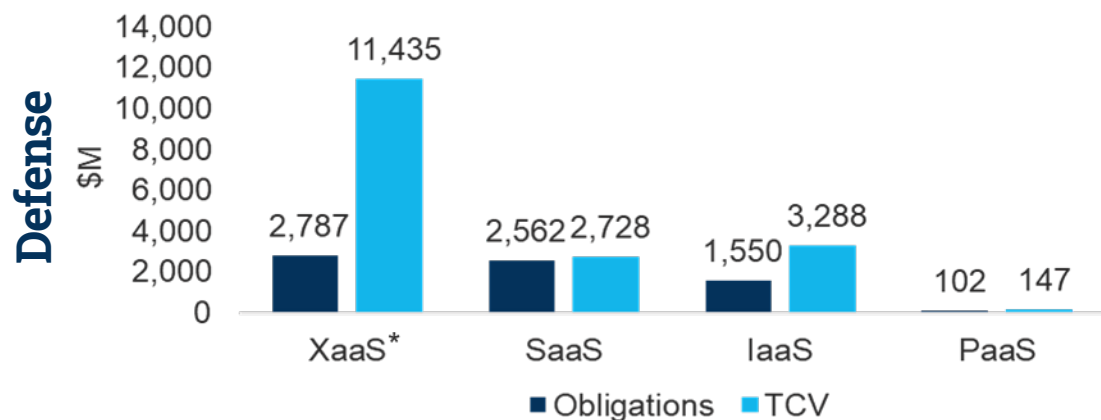
Cloud Obligations and TCV, FY 2018-2020: Deployment Model

Defense $M

- Community/Public: Obligations 2,724 / TCV 14,031
- Hybrid: Obligations 1,055 / TCV 1,664
- Private: Obligations 487 / TCV 742

■ Obligations ■ TCV

Civilian $M

- Community/Public: Obligations 8,040 / TCV 10,009
- Private: Obligations 580 / TCV 937
- Hybrid: Obligations 563 / TCV 1,337

■ Obligations ■ TCV

Sources: Deltek, FPDS

» **Air Force led DOD** in spending on community / public cloud with $1.45B from FY 2018 to 2020. Defense Agencies spent $528M, Army spent $386M and Navy spent $356M.

» **Spending $782M on hybrid cloud**, Defense Agencies led the DOD, followed by Army ($114M), Air Force ($89M) and Navy ($71M). Spending on hybrid cloud also grew every year since FY 2018.

» **Private cloud spending fell** behind all other models for the first time led by OSD ($374M).

» **VA led all agencies** in community/public cloud use, spending $1.7B from FY 2018 to 2020. Commerce, DHS, HHS and Education spent $1.6B, $886M, $801M and $655M, respectively.

» **Private cloud spending fell** to its lowest level yet. Commerce led all agencies, spending $108M.

» **Three-year spending on hybrid cloud** by the Civilian sector more than tripled from $103M to $326M. VA spent $194M, DOT $103M and DHS $43M.

Cloud Obligations and TCV, FY 2018-2020: Service Delivery

Defense chart (\$M):

	Obligations	TCV
XaaS*	2,787	11,435
SaaS	2,562	2,728
IaaS	1,550	3,288
PaaS	102	147

Civilian chart (\$M):

	Obligations	TCV
XaaS*	5,444	2,466
IaaS	4,275	2,728
SaaS	3,956	6,942
PaaS	444	1,462

Sources: Deltek, FPDS

» **Defense spending on SaaS rose** from \$646M in FY 2018 to \$1.1B in FY 2020. Air Force's 3-year spending totaled \$1.3B, followed by Army at \$592M and Defense Agencies at \$440M.

» **Obligations for IaaS rose** from \$353M to \$713M over 3 years. Defense Agencies spent \$808M of that, followed by Army (\$296M), Navy (\$243M) and Air Force (\$153M).

» **Defense PaaS spending** rose from \$21M to \$44M. Air Force spent \$60M over 3-years, Defense Agencies spent \$27M and Navy \$13M.

» **Civilian spending on IaaS fell** from \$1.5B in FY 2018 to \$1.4B in FY 2020. VA spent \$1.2B of that total, followed by HHS (\$824M) and GSA (\$486M).

» **Spending on SaaS** rose from \$1B to \$1.5B over 3 years. VA saw the highest growth, spending \$718M altogether. HHS, Education and DHS spent \$505M, \$460M and \$425M, respectively.

» **PaaS spending rose** from \$115M to \$198M. DHS accounted for \$259M of that total, followed by HHS (\$33M), DOJ (\$33M), Labor (\$29M) and VA (\$28M).

Top Federal Cloud Computing Solution Areas, FY 2018-2020

1
Engineering and Technical Support
$5.6B

» Civilian sector spending on cloud-related technical support rose from $1B in FY 2018 to $1.2B in FY 2020.

» Defense spending on engineering support more than doubled from $432M in FY 2018 to $924M in FY 2020.

2
Applications
$5.5B

» Civilian agency spending on SaaS-based solutions continues to rise, up from $973M in FY 2018 to $1.5B in FY 2020.

» Growing from $482M in FY 2018 to $759M in FY 2020, the DOD is using more cloud-based capabilities.

3
Data Center Services
$4.4B

» Civilian sector spending on these services declined for the first time, dropping from $1.1B in FY 2018 to $936M in FY 2020.

» DOD's use of commercial IaaS grew significantly, from $359M in FY 2018 to $559M in FY 2020.

4
Testing, Design and Development
$1.7B

» Civilian sector development operations spending rose from $270M in FY 2018 to $498M in FY 2020.

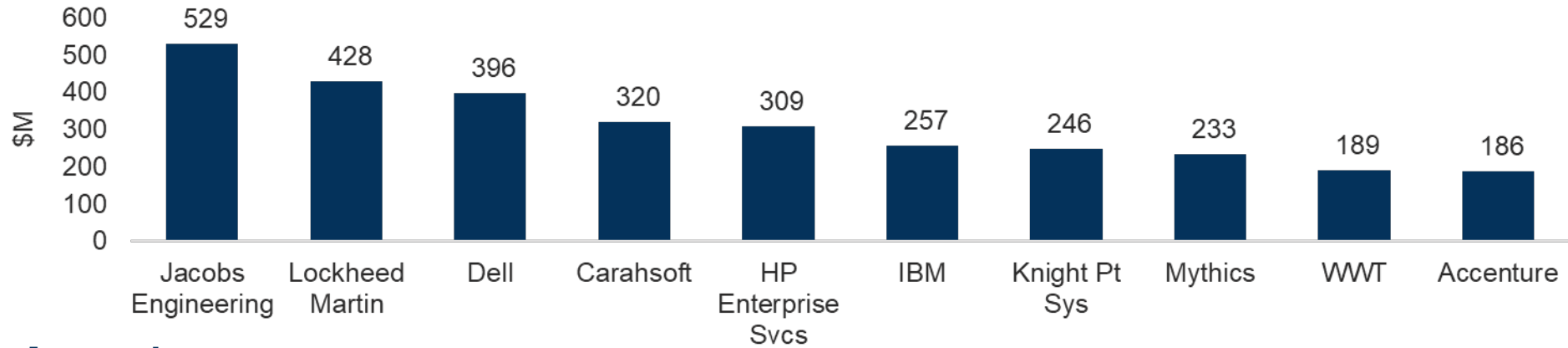» Defense spending on development services accelerated from $114M in FY 2018 to $216M in FY 2020.

5
Professional Services
$1B

» Civilian agency use of contracted services remained flat from $198M in FY 2018 to $201M in FY 2020.

» Spending $34M in FY 2018 and $127M in FY 2020, DOD lags in the use of contracted services related to cloud.

Source: Deltek

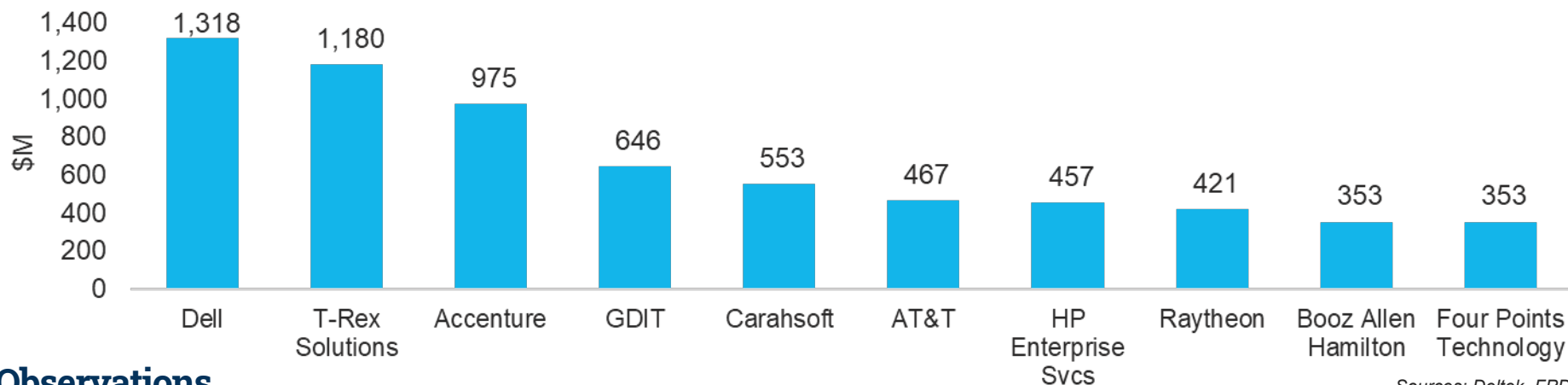# Top Defense Cloud Contractors by Obligations, FY 2018-2020

Chart: Obligations in $M

- Jacobs Engineering: 529
- Lockheed Martin: 428
- Dell: 396
- Carahsoft: 320
- HP Enterprise Svcs: 309
- IBM: 257
- Knight Pt Sys: 246
- Mythics: 233
- WWT: 189
- Accenture: 186

Y-axis: $M (0, 100, 200, 300, 400, 500, 600)

Sources: Deltek, FPDS

Observations

» **Jacobs'** obligations: U.S. Special Operations Command ($513M) and the Defense Information Systems Agency ($4M).

» **Lockheed Martin's** obligations: Air Force Life Cycle Management Center ($408M) and the Defense Logistics Agency ($15M).

» **Dell's** obligations: Air Force Space Command ($322M) and Naval Warfare Information Systems Command ($65M).

» **Carahsoft's** obligations: Army Program Executive Office Enterprise Information Systems ($128M) and the Defense Logistics Agency ($80M).

» **HP Enterprise Services'** obligations: Air Force ($272M) and DISA ($30M).

» **IBM's** obligations: Army Program Executive Office Enterprise Information Systems ($137M) and at Army NETCOM ($12M).

» **Knight Point Systems'** obligations: DISA ($246M).

» **Mythics'** obligations: Air Force ($228M).

» **World Wide Technology's** obligations: DISA ($181M).

# Top Civilian Cloud Contractors by Obligations, FY 2018-2020

Bar chart ($M):
- Dell: 1,318
- T-Rex Solutions: 1,180
- Accenture: 975
- GDIT: 646
- Carahsoft: 553
- AT&T: 467
- HP Enterprise Svcs: 457
- Raytheon: 421
- Booz Allen Hamilton: 353
- Four Points Technology: 353

Sources: Deltek, FPDS

Observations

» **Dell's** obligations: VA ($989M), DHS ($160M), SSA ($106M).

» **T-Rex Solutions'** obligations: Commerce ($1.2B), DHS ($2M).

» **Accenture's** obligations: Education ($416M), DHS ($346M), GSA ($77M).

» **General Dynamics IT's** obligations: HHS ($377M), DOT ($77M), Commerce ($58M). DOT and Commerce are CSRA, a part of GDIT.

» **Carahsoft's** obligations: USDA ($166M), HHS ($129M).

» **AT&T's** obligations: GSA ($454M), Treasury ($9M), Interior ($3M).

» **HP Enterprise Services'** obligations: HHS ($438M), DHS ($13M), VA ($5M).

» **Raytheon's** obligations: Commerce ($415M), DOJ ($7M).

» **Booz Allen Hamilton's** obligations: VA ($317M), GSA ($26M), HHS ($9M).

» **Four Points Technology's** obligations: VA ($178M), DHS ($82M).

Total Addressable Cloud Computing Market, FY 2021-2023

CAGR: 10.9%

Year	$B
2021	9.2
2022	10.3
2023	11.4
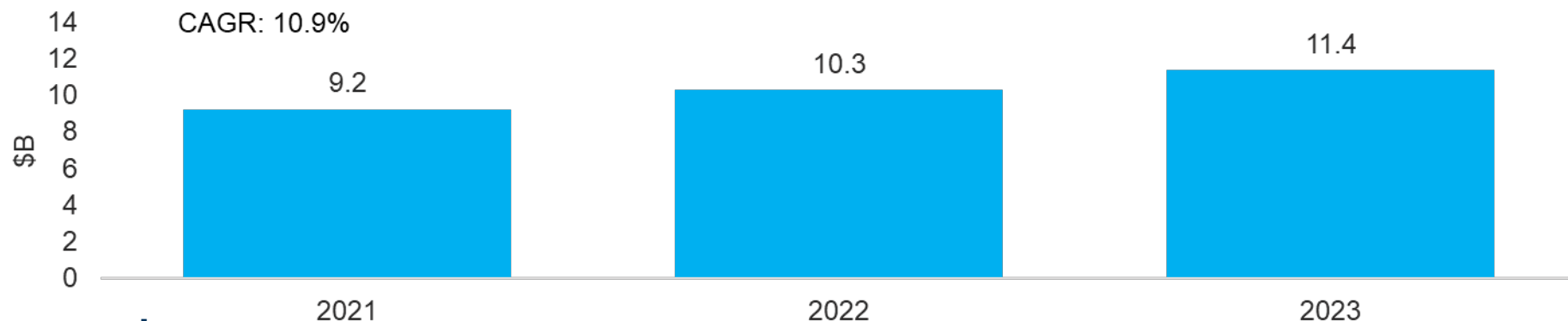
Source: Deltek

Assumptions

» Federal cloud spending grew an average of $1.8B annually between FY 2016 and FY 2019 before slowing to $900M from FY 2019 to FY 2020. After FY 2020's slowdown, cloud spending will begin rising faster in FY 2021 and accelerate from FY 2022 on.

» Telework will remain a part of the federal IT landscape even after the end of the COVID crisis, reinforcing the need for agencies to provide readily-accessible cloud services.

» The number of secure, FedRAMP-certified cloud solutions continues to grow, offering agencies easy access to more choices.

» Agencies have come to accept that commercial cloud services are more secure than on-premise government systems.

» Revised Trusted Internet Connection (TIC) policy is providing agencies with greater flexibility for securely connecting to cloud providers.

» Significant appropriations and relaxed repayment options for the Technology Modernization Fund will encourage agencies to begin cloud projects that modernize important legacy IT systems.

Conclusions

Cloud Budget Trends

» Data center and cloud investment reported by OMB totaled $3.4B for FY 2022, rising $200M from the estimate of $3.2B reported in FY 2021.

> » The total investment reported rose despite the fact that OMB provided no data for the Department of Defense.

» OMB reported total combined IaaS/PaaS spending of $12.7B for FY 2021, which is a significant increase from the $1.6B reported for FY 2020. This increase is likely more the result of agencies complying fully with the TBM reporting methodology than an actual rise in investment of almost 700%.

> » The increase in reported IaaS/PaaS spending occurred despite OMB not reporting data for the DOD.

» FY 2021, SaaS spending reported by OMB totaled $1.7B, an increase of $1B from the $700M reported for FY 2020. Like IaaS/PaaS, this increase is also probably a result of stricter agency compliance with mandated TBM guidelines.

Market Trends and Drivers

» Civilian agencies credit the Cloud Smart policy with accelerating adoption even though implementation of it remains incomplete.

» The full implementation of Cloud Smart will result in a list of GSA-recommended Government-Wide Acquisition Contracts (GWACs) that agencies should use for cloud procurement.

» Workforce training should ensure government contracting personnel become smarter about purchasing cloud services.

Conclusions

Market Trends and Drivers (Cont)

» The value of contracts awarded for Cloud Access Point/Gateway capabilities is surging, indicating adoption strength in the market.

» Cloud spending from FY 2019 to FY 2020 grew at a slower pace than expected due to disruption caused by the COVID-19 public health crisis.

  » The federal government's move to full-time telework in response to the COVID-19 crisis did not cause an exceptionally high spike in cloud spending due to the fact that many agencies had already invested in network infrastructure and collaboration capabilities.

» The Military Departments (MILDEPs) are all taking a centralized approach to cloud adoption by leveraging a small number of enterprise, commercial IaaS and PaaS providers. SaaS adoption remains more dispersed.

» MILDEPS using the same enterprise IaaS providers has created a de facto dual-cloud ecosystem independent of the Joint Enterprise Defense Infrastructure (JEDI).

» As of Q1 FY 2021, the FedRAMP PMO has approved 218 solutions for use by federal agencies.

  » The number of FedRAMP approved solutions rose by 50% in FY 2020, providing agencies with a larger number of choices.

  » The number of FedRAMP-Low authorized solutions procured by agencies surged in FY 2020, but FedRAMP-Moderate solutions still remain the preferred option. The procurement of FedRAMP-High solutions continues to trail the acquisition of both Moderate and Low solutions.

To purchase the full report visit GovWin.com

Conclusions

Market Trends and Drivers (Cont)

» Implementing CMMC/FedRAMP reciprocity could drive SaaS adoption across the DOD in future years.

» Cloud adoption is enabling agencies to introduce Zero Trust security capabilities.

» Challenges identified by the National Science and Technology Council (NSTC) – including inconsistent access to cloud services and a lack of understanding of the technology by researchers – are limiting the use of cloud for federal R&D programs.

» The $1B allocated to the Technology Modernization Fund (TMF) will remain available to federal agencies until used or until the end of September 2025, whichever comes first.

   » The TMF Board will prioritize projects that cut across agencies, address immediate security gaps and improve the public's ability to access government services.

   » The GSA is considering flexible TMF repayment options, making it more likely that agencies will apply for cloud-oriented IT modernization projects, particularly those for high-valued legacy systems.

» Cloud spending on the old GSA schedule IT 70 fell to practically nothing in FY 2020 due to the roll-out of the new Multiple Award Schedule (MAS).

   » The GSA is currently evaluating ways to reform the cloud pricing methodology used by the new MAS in order to introduce a flexible model for pricing cloud services per customer use.

» Moving to the cloud is now considered the key method of modernizing agency IT environments.

Conclusions

Cloud Computing Spending Trends

» Identifiable federal spending on cloud reached a new high of $8B in FY 2020, but the rate of spending growth slowed compared to previous years.

   » Civilian agencies as a whole continue to spend more than the DOD, but the gap is narrowing.

   » Cloud spending surpassed total awarded contract value in the Civilian sector for the second year in a row, suggesting that agencies are leveraging contracts they have already put into place (especially for IaaS) rather than awarding new agreements.

   » With 3-year spending totals nearing or exceeding $2B, VA, Commerce, HHS and DHS have now clearly separated from the rest of the Civilian sector in the scale of their cloud usage.

   » The DOD reported no decline in spending or total awarded contract value from FY 2018 to FY 2020.

» Cloud activity at highly-federated civilian agencies remains concentrated in a small number of components, with limited use in other parts of the organization.

» Both the Defense and Civilian sectors of government spend heavily on cloud engineering services.

» Agencies are spending more on community/public cloud than on any other deployment model.

» Spending on hybrid cloud is growing fast, rising nearly 3x in the Civilian sector from FY 2018 to 2020 and overtaking spending on private cloud at the DOD.

Conclusions

Cloud Computing Spending Trends (Cont)

» Defense spending on SaaS nearly doubled from FY 2018 to FY 2020. Civilian sector spending on SaaS rose 50% over that same period.

» Spending on IaaS is slowing across all of government compared to spending on SaaS.

» PaaS spending is rising as well just not as fast as SaaS and IaaS.

» Although cloud engineering remains one of the most robust areas of federal investment, spending slowed in FY 2020 due to the COVID-19 crisis.

  » Total spending on cloud engineering by civilian agencies fell by $500M in FY 2020 compared to FY 2019. Defense cloud engineering spending rose by $360M.

  » Agencies across government continue to spend the most on migration services, a subset of cloud engineering work, although that spending declined 50% in the Civilian sector from FY 2019 to FY 2020 while nearly doubling at the DOD.

Competitive Landscape

» Traditional contractors continue to dominate the Defense cloud market.

» Spending on AWS and Microsoft Azure outpaces all other IaaS providers at the DOD, but traditional resellers remain the primary way that DOD customers procure those services.

Conclusions

Competitive Landscape (Cont)

» Microsoft Azure remains the most used IaaS solution by Civilian agencies, with total spending from FY 2018 to 2020 more than double that of AWS.

» Defense organizations spent the most on Adobe, Microsoft 365 and Oracle Cloud SaaS solutions from FY 2018-2020, while Civilian agencies preferred Adobe, Tableau and AWS.

» Pivotal and a combination of AWS and Microsoft Azure made up the top PaaS solutions used across the DOD. Civilian agencies also used AWS and Microsoft Azure as their preferred PaaS solutions, with Appian rounding out the top three.

» Customers in both the Defense and Civilian sectors prefer using Government-Wide Acquisition Contracts (GWACs) to acquire cloud services more than any other method.

» Both the Civilian and Defense sectors also tend to use GSA Schedules for cloud procurement. This preference is stronger at the DOD than it is across the Civilian sector.

» Defense spending on cloud prototype OTA contracts fell for the first time in FY 2020, likely due to the impact of the COVID-19 crisis. The total value of cloud-related OTA contracts fell as well.

» The use of Other Transaction Authority by the DOD to acquire cloud prototypes fell in FY 2020 vs. FY 2019. OTA agreements are typically for cloud engineering efforts, work that was disrupted by federal work-from-home orders.

Recommendations

» Look for cloud business primarily on GWACs and GSA's MAS Schedule, as these are now the preferred acquisition avenues for both Civilian and Defense customers.

» Focus more on delivering SaaS capabilities to the DOD as the IaaS portion of the market is presently locked up by a small number of large commercial providers.

» Contractors are advised to have cloud solutions certified at the FedRAMP-Moderate impact level to increase competitiveness in both DOD and civilian agencies.

» Expect the PaaS business opportunity to be more robust across the Civilian sector than at the DOD; the latter is now dominated by large commercial providers.

» Help educate researchers within agencies with science missions on the possibilities of using cloud services for R&D.

» Position your company to take advantage of TMF funding by identifying requirements that cut across agencies, address immediate security gaps and improve the public's ability to access government services.

» Discuss flexible pricing with the GSA to help shape the possible addition of that methodology to the GSA MAS.

» Providing cloud engineering services remains the market play that offers the most business opportunity.

Gov**Win**
from Deltek

GovWin is the leader in market intelligence for businesses selling to the public sector. We provide enterprise, mid-market and small business customers with the most comprehensive set of federal, state, and local government contracting leads. Clients grow their sales pipelines with access to expiring term contracts, pre-RFP information, and planned, funded projects, along with government contacts, competitor information, and market analytics – all backed by our holistic integration and expert support. Learn more about how GovWin IQ can help equip your organization for success in public sector sales.

Learn More About GovWin IQ Today at **info.deltek.com/GovWin-IQ-Request-Demo**

US & Canada 800.456.2009 • **UK** +44 (0) 20 7518 5010 • **EMEA** + 45 70 20 33 18 • **APAC/AUNZ** +61 2 9911 7740